

The Continuing Evolution of Effective IT Security Practices

By John Voloudakis

The art of living lies less in eliminating our troubles than in growing with them.
—Bernard Baruch

Key to the importance of and focus on IT security over the past ten to fifteen years is the change in information technology itself. Previously a specialized tool used by a relatively small subset of higher education institutions, information technology today represents a critical system in the organism that is a modern college or university. In the past, IT security was an afterthought on many campuses. Administrators chose to protect “critical” systems with encryption or other advanced techniques or to provide minimal protection, such as anti-virus 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.

John Voloudakis is Regional Practice Leader for Higher Education at BearingPoint. This article is based on a chapter written for the forthcoming EDUCAUSE Center for Applied Research (ECAR) study “Safeguarding the Tower: IT Security in Higher Education, 2006.”



As use of the Internet grew beyond academia in the mid-1990s, the demand for connectivity grew as well. Colleges and universities, along with the rest of society, became ever more interconnected via the World Wide Web. And 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 and through a new vehicle: worms that automatically propagated themselves through all unprotected systems. These worms either blocked network access by overloading the network or gave their creators access to the infected system, which the hackers could then use as part of a *botnet* (a collection of compromised systems) to send spam or launch additional attacks.

This was the scenario when the EDUCAUSE Center for Applied Research (ECAR) conducted its initial study of

information security in higher education in the spring and summer of 2003: “Information Technology Security: Governance, Strategy, and Practice in Higher Education.”¹ At that time, higher education was just starting to awaken to the paradigm shift caused by these new, automated attacks. When the survey research was conducted, in early spring of 2003, there had not yet been many instances of automated attacks causing large-scale shutdowns of institutional and corporate systems. This was reflected in the survey results, which showed a purposefully limited use of protective technologies such as perimeter firewalls and a relatively low use of “soft” measures such as policies, awareness, and planning. But by the time ECAR conducted detailed interviews in mid-summer of that year, the SQL Slammer worm had spotlighted these emerging threats, shutting down a number of campus networks by exploiting a known application vulnerability that many administrators had never

patched. And by the time ECAR had completed its research and presented the results at the EDUCAUSE annual conference and the ECAR Symposium, both in the fall of 2003, 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 temporary network outages. As a result, many of the individuals who had earlier told us about the need to limit enterprise-wide IT security measures indicated that they were currently rethinking their approaches in this new environment.

Now, three years later, ECAR has conducted a follow-up study of information security in higher education.² In the time between the 2003 study and this follow-up study, we have indeed witnessed a marked change in the tools and techniques used by colleges and universities to combat the ever-increasing wave of security threats. Driven by the increasing

frequency and virulence of attacks on their networks and systems, higher education institutions have made a number of moves to secure their critical systems and protect their users. The degree of change in this relatively short time span is one of the key findings of the 2006 study.

In several areas, the 2006 study paints a brighter landscape. The use of many information security technologies has grown by double digits. Likewise, and even more encouraging, the adoption of “soft” IT security approaches has risen dramatically. However, there is still much room for improvement. Many important technologies and practices are still not in use at 25 percent or more of the institutions responding to the ECAR survey. Moreover, respondents indicated that although 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 nature of the threats that must be countered. If, as described above, information technology is viewed as a critical system within the institutional organism—as the circulatory system that moves the information that is increasingly becoming the lifeblood of many institutions—then the nature of the attacks that this system faces is changing for the worse. In the early days of computing, attacks primarily centered on the organs composing this system—the servers and computers connected to the network—most often to destroy them, to use them to launch a subsequent attack on another machine, or occasionally to target the data housed on them. Fighting off attacks against these organs was the primary information security goal of colleges and universities at the time of the 2003 study. Later, attacks targeted the arteries and veins connecting the organs: the network itself. Denial-of-service at-

tacks—launched either from outside the network or from within, by overloading the network using compromised machines—became a primary threat.

Although both of these threats remain today, information security administrators have become adept at protecting key host systems and keeping the network

In the early days of computing, attacks primarily centered on the organs composing the system—the servers and computers connected to the network—most often to destroy them [or] to use them to launch a subsequent attack on another machine.

running—hence the increased perception of success in protecting centrally controlled assets. However, the new threat is targeting not the organs or the veins of the system but the blood itself: the data flowing through and housed on networks and computers, particularly personal data about constituents of the institution. These attacks can come in many forms: keyboard sniffers installed to ferret out passwords; “phishing” attacks in which users are tricked into giving up personal data; compromises of improperly designed applications; or

actual thefts of physical assets such as laptops or backup tapes housing valuable data. These types of attacks are different in a couple of ways. First, they often hit targets of opportunity—lightly protected systems or ignorant users outside the highly fortified areas of the institution. Second, and perhaps more important, 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 information security game.

State of the Practice Today

A comparison of the 2003 and 2006 studies shows not only the progress that higher education has made in advancing the practice of information security but also those areas where improvement is still needed.

Technology

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 in 2006 was the 22 percent growth in the use of perimeter firewalls in research universities, since in 2003 many respondents at research institutions ardently stated that perimeter firewalls would not be an effective solution in their environment. Also significant was the growth in the use of interior firewalls, with an increase of more than 27 percent across all Carnegie classes. Other rapidly growing technologies include virtual private networks, up more than 65 percent, and intrusion-detection and intrusion-prevention systems, each up more than 30 percent. The use of enterprise directories jumped 55 percent, and the use of active filtering technologies increased nearly 100 percent. These statistics show that institutions are seriously considering the threat of attack and have taken steps to protect themselves.

Still, despite the high growth rates, less than half of the respondents to the 2006 survey were using intrusion-detection systems, 35 percent were not using 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 respondents since 2003. Fully 95 percent of institutions reported still using traditional, weak username-and-password combinations. Although almost 60 percent indicated they also used strong passwords within their organizations, only 27 percent were using Kerberos, and fewer than 10 percent reported using 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, respondents were, as a whole, focused more on technical solutions and less on the “softer” IT security aspects such as planning, training, auditing, and codifying policies and procedures. The study thus recommended that institutions seek out a more balanced approach, combining the effective use of technologies with cultural solutions to more effectively combat threats. Significant progress has been made on this front. The 2006 study shows tremendous

growth rates in the cultural aspects of information security. Over 32 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, institutions reporting that either a partial or a complete security plan was in place jumped 128 percent, and the number of institutions that had conducted a risk assessment increased 77 percent. In addition, senior management's interest in IT security issues increased substantially.

But despite the quantum leap forward in many of the cultural aspects of security, 68 percent of institutions have not appointed a chief information security officer, and 38 percent do not have a centralized security function. These

numbers may reflect limited resources or conscious policy decisions, but this topic bears further study. Although most respondents had some security policies and procedures in place, their coverage was not uniform. For example, 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 cover 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 do not test new applications for security, and nearly 70 percent had not established security standards for application or system development. Respondents who indicated that no plan of any type was in place for IT security totaled 20 percent. Less than 10 percent of respondents indicated they had undergone a comprehensive risk assessment in the last two years, and over 40

percent still had not performed any type of risk assessment.

Outcomes

On the whole, institutions rated the success of their IT security programs lower in 2006 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 2006. There was a much higher assessment of the security of central applications, networks, and data than of the security of applications, networks, and data that are locally controlled.

This lower rating of overall success likely stems from several factors. First, as described earlier, is the changing nature of threats. As attacks target data, rather than systems and networks, the defenses that have been put in place to date are not adequate, since they generally are not as strong

in the decentralized areas of the organization, where many new attacks are targeted. A second factor is that institutions may have a greater awareness of the complexity of developing a comprehensive IT security program to combat these changing threats. Added to this is the difficulty of managing information 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 counter IT security threats. The 2006 study shows that higher education has certainly 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, along with the other areas highlighted as possibilities for improvement, now put the spotlight on a new need: the development of enterprise IT security programs that are designed to protect the entire institution—not just the central systems—and to do so in a coordinated, flexible manner. Several additional data points from the study support this need: there was no change in the number of respondents (a low 34 percent) who said that security practices were woven into the fabric of their institution; and only 25 percent of respondents agreed that security was part of the institutional employee culture. These findings show that even though 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 IT security program encompassing the protection of both central and local assets is a large undertaking, particularly in the 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.

The 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 earlier, the target of many new attacks is no longer the operating system, the network, or control of the machine but rather is the personal data about the users of these systems and the constituents of the organization. The driver of these hacking attempts is simple: profit. And the easiest way for a hacker to profit is not by stealing top-secret research

The target of many new attacks is no longer the operating system, the network, or control of the machine but rather is the personal data about the users of these systems and the constituents of the organization.

housed in a secure system or accessing an organization's financial system and rerouting funds. The easiest way for a hacker to profit is to discover a weak link in the organization's security and use that weak link to find personal data. With only a relatively small set of information on an individual, a competent identify 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 a 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 Symantec Corporation, a security vendor. 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."³

More than 89 million records containing personal data have been compromised since the ChoicePoint incident in February 2005, according to the nonprofit consumer information and advocacy organization Privacy Rights Clearinghouse. This organization maintains a list of the incidents on its Web site.⁴ Of the 237 incidents that occurred between February 2005 and July 2006, 83 of them, or 35 percent, were at colleges and universities. Only a well-thought-out, enterprise IT security program that restricts the distribution of sensitive data and that makes users aware of the risks can significantly reduce the risk to the college or university from these types of threats.

Influence of Federal Mandates

Pressure to improve security is coming not only from inside the institution, in response to more malevolent threats. Compliance with a growing list of existing and emerging federal and state laws and regulations is certain to be another, external driver of change. Examples of these laws and regulations include the federal Family Educational Rights and Privacy Act (FERPA), the FTC safeguard regulations of the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), state laws on notification of security breach, the FDA rule on electronic records and electronic signatures (21 C.F.R. Part 11), and the Payment Card Industry Data Security Standard (PCIDSS).⁵

In addition, higher education information security administrators should be aware of the Federal Information Security Management Act (FISMA), part of the eGovernment Act of 2002. This legislation mandates compliance with a set of standards established by the federal government to ensure the consistent application of effective security standards and practices.⁶ 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-123,⁷ which holds federal executives responsible for instituting accountability and controls for assets under their

management, some federal agencies are beginning to apply the FISMA standards to the recipients of their funds. For example, the U.S. Department of Labor has been auditing state agencies receiving funds, such as unemployment insurance agencies, to ensure that they have properly complied with FISMA. It is easy to see that the Department of Education, the National Science Foundation, and the National Institutes of Health could hold institutions receiving their funds for financial aid and/or research grants similarly responsible in the future. Given this possibility, it may make sense for higher education institutions to become familiar with the standards that FISMA requires and to consider using these as a guide when developing their own information security programs.

Another federal mandate that could have a similar impact is Homeland Security Presidential Directive 12 (HSPD-12),⁸ which requires the use of more uniform, secure standards for issuing govern-

ment identity credentials. The Federal Information Processing Standards (FIPS) Publication 201-1,⁹ issued by the National Institute for Standards and Technology (NIST), describes standards for the proposed Personal Identity Verification, or PIV, system. HSPD-12 calls for these standards to be implemented both by federal offices and by “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 want to use this standard as a guide when looking at their own systems.

Finally, the Communications Assistance for Law Enforcement Act (CALEA) is another piece of federal legislation that may affect the technologies that colleges and universities deploy. CALEA requires facilities-based broadband Internet access providers, interpreted to include colleges and universities, to deploy standardized equipment and

procedures to enable surveillance by law enforcement agencies. Although 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 and could pose particular difficulties for institutions utilizing VoIP (Voice-over Internet Protocols) on their networks.¹⁰

Implementing an Enterprise IT Security Program

Managing IT security in higher education presents a number of unique challenges, especially at larger institutions that operate in a decentralized fashion. Although the central IT department is expected to ensure the security of the institution’s IT assets, many of these assets are not managed by the central IT department. These assets may be controlled by relatively autonomous faculty members, schools, or departments or may not be owned by the institution at all—as in the case

of students' personal equipment. This makes it difficult to implement a "one size fits all" solution for many aspects of security. Thus, approaches to creating an enterprise IT security program in higher education need to reflect this element of the institution's organization and culture.

An enterprise IT security program for higher education should include the following elements:

- *The program should be standards-based:* The program should define common standards that the institutional community will utilize. These include not only technical standards but also a set of policies and procedures that are accessible, understandable, actionable, and up-to-date.
- *The program should be flexible:* The program must be able to allow for the diverse needs of the institution's distributed departments and user population.
- *The program should be mission-driven:* The

program should be aligned to the risk profile of the institution and should be developed through the participation of a broad governance body.

- *The program should be adaptable:* The program should be designed around principles and risk profiles—not specific threats or systems. This will allow the program to adapt as the institution changes and as new threats emerge.
- *The program should be simple:* The program needs to be as simple as possible for individuals and departments to implement in order to gain their willing participation. This may require significant work by the IT department.
- *The program should be measurable:* Metrics should be established to gauge the performance of the program so that it can continue to be improved in a meaningful way.

For institutions interested in moving forward with developing an enterprise IT

security program, some critical steps are highlighted below:

1. *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 to the governance structure designed to manage it, as well as to ensure that the controls and enforcement procedures have "teeth." Given the heightened awareness of the consequences of security failures, it should be easier to make this case at most institutions than it may have been in the past.
2. *Implement governance structure:* Since most institutions do not 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 but be diverse enough to incorporate the points of view of different types of campus constituents. A multitiered structure—for example, executive and operational—may help achieve this goal.
3. *Maintain communication:* Clear, frequent communications are essential to any change initiative. Whether through formal training and awareness programs or through informal e-mail updates, members of the campus community should be kept informed of the changes being made and of their roles in the vision.
4. *Develop inventory:* Institutions need to identify and classify the assets that require protection. This is extremely critical for data, since ultimately this is what the institution is trying to protect. Classification can be simple, for example: (1) regulatory compliance—data that needs to be protected due to legislation or other regulation; (2) confidential—data that the institution has determined should be protected; (3) internal—data that is open for use by internal users but not for public consumption; (4) public—data for which no protection is needed. A

more complex classification could be used if deemed necessary.

5. *Perform risk assessment:* Institutional assets should be examined to determine the level of protection they require and to develop a risk-mitigation plan to address risks with an appropriate level of response.
6. *Implement controls:* Based on the risk assessment, institutions should implement needed technical, procedural, and organizational components and develop approaches to accommodate the needs of the broader organization. It may be necessary to provide central support to help some distributed areas with their needs.
7. *Monitor and refine both the assets and the program:* Finally, institutions need to develop and implement monitoring capabilities and procedures for IT assets as well as for the program itself. They should conduct monitoring, on a periodic basis, that aligns to the risk profile of the asset in question and use

the results of this monitoring to improve and tailor the program to more effectively meet their needs.

Conclusion

To meet the security requirements of the college or university in light of the threats and potential compliance challenges described above, institutional leaders should consider the development of an enterprise information security program that addresses the needs not only of the central organizations of the institution but also of the broader campus community. An information security program that consists of technologies, processes, and human components, that is aligned to the institution's risk profile, and that is 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 simply targeting specific threats with specific measures. Yet to get beyond the data center, where the 2006 ECAR IT

security study shows that institutions are already doing a good job, and out to the distributed areas of campus, an institution must have significant political will and capital. Senior-level support will be needed to implement effective and enforceable policies and procedures and to develop effective governance for security efforts. Although instituting such a program will be difficult, this is the step that is needed to take security management to the next level and to continue to provide our institutions with a secure teaching, research, and business environment. The confluence of heightened awareness driven by high-profile incidents and the likelihood of regulatory mandates may make this the ideal time to successfully move such a program forward. *e*

Notes

1. Robert B. Kvavik and John Voloudakis, "Information Technology Security: Governance, Strategy, and Practice in Higher Education," *EDUCAUSE Center for Applied Research (ECAR) Study*, vol. 5 (2003), <<http://www.educause.edu/LibraryDetailPage/666?ID=ERS0305>>.
2. Robert B. Kvavik with John Voloudakis, "Safe-guarding the Tower: IT Security in Higher Education, 2006," *EDUCAUSE Center for Applied Research (ECAR) Study*, forthcoming, fall 2006.
3. Daniel Sieberg, "Hackers Shift Focus to Financial Gain," *CNN.com*, September 26, 2005, <<http://www.cnn.com/2005/TECH/internet/09/26/identity.hacker/index.html>>.
4. "A Chronology of Data Breaches Reported since the ChoicePoint Incident," Privacy Rights Clearinghouse Web site, <<http://www.privacyrights.org/ar/ChronDataBreaches.htm>>, July 25, 2006.
5. For more on each of these, see M. Peter Adler, "A Unified Approach to Information Security Compliance," in this issue of *EDUCAUSE Review*.
6. FISMA standards can be found in the National Institute of Standards and Technology (NIST) publications located at <<http://csrc.nist.gov/publications/index.html>>.
7. Alice M. Rivlin, "Circular No. A-123," June 21, 1995, Office of Management and Budget, <<http://www.whitehouse.gov/OMB/circulars/a123/a123.html>>.
8. President George W. Bush, Homeland Security Presidential Directive (HSPD)-12, August 27, 2004, Office of the Press Secretary, <<http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>>.
9. FIPS Pub 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors," March 2006, National Institute of Standards and Technology, <<http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>>.
10. See the EDUCAUSE resource page: "CALEA (Communications Assistance for Law Enforcement Act)," <http://www.educause.edu/Browse/645?PARENT_ID=698>; Steven Bellovin et al., "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP," Information Technology Association of America (ITAA), June 13, 2006, <<http://www.itaa.org/news/docs/CALEAVOIPreport.pdf>>.