

# 2

## Introduction

*We must strive for a sensitive balance between openness and security, between access and control. We need both.*

—James Wright, President, Dartmouth College

**P**roviding secure information technology (IT) services to colleges and universities is a special, if not unique, challenge. Unfettered and timely access for all to enormous quantities of information is higher education's lifeblood and is key to its success in educating its students and generating new ideas and know-how. Insensitive, political, or casual attempts to check and control this dynamic transmission and consumption of information are problematic at best, and potentially deleterious to the academic mission. On the other hand, thoughtful and mission-minded implementation of IT security can and will ensure, protect, and facilitate the requisite flow of information so necessary for higher education's continued success.

James Wright, president of Dartmouth College, captures higher education's dilemma and posits on its future. "The new environment of higher education will require increased security, and new procedures may mandate changes in practices that have been used for many years."<sup>1</sup> Indeed, much has changed since the early and mid-1990s when information security was more a local problem for selected institutional business and research units and the IT organization. With the advent of the World Wide Web in 1993 and the commercialization and globalization of the Web in the mid-

1990s, the campus community's attention to information security began to change, both rapidly and radically. Risks and threats to institutional information assets grew suddenly and exponentially as educational institutions were subjected to both accidental and malicious acts that exploited inherent network, operating system, and software vulnerabilities and low levels of security awareness and security-conscious behavior.<sup>2</sup> Noteworthy, too, was the change in federal and state legal environments, which mandate ever-stronger IT security practices. And public expectations of IT security for higher education—and all industries for that matter—are growing as well.

More than ever, higher education's information assets, whether they support core missions or business administration, are essential to enhancing reputation, competitiveness, client satisfaction, revenue, and accountability, so they must be protected. And despite occasional academic and cultural resistance (or apathy), most institutions are investing substantial financial and human resources to protect their information infrastructure and valuable intellectual assets and, not least, the privacy and interests of the people they serve.

Indeed, we can compare IT security to fiduciary responsibility on the part of higher

education institutions. Just as institutions are held to standards regarding the accounting of their funds, so they are and will be increasingly held to standards of data protection. It is not surprising that auditors, both internal and external, are addressing these matters on a regular basis. How institutions will achieve acceptable levels of IT security, and by what means—technologies, policies, software, personnel, budgets—currently varies widely, as this study will demonstrate. But whether security is achieved and satisfactorily reported becomes less and less of an alternative. Indeed, higher education now faces the reality of providing robust IT security.

In a recent article in the *Chronicle of Higher Education*, Dan Carnevale elaborates on the implications of the Gramm-Leach-Bliley Act of 1999 for higher education.<sup>3</sup> First thought applicable to financial institutions only, the legislation was largely ignored by higher education until the Federal Trade Commission ruled in 2002 that it also applied to colleges' and universities' financial relationships. Higher education institutions therefore must notify people they deal with of their right to keep their financial information confidential and must protect their financial data. Protection also involves having a plan or security policy that includes designating an employee to coordinate information security, identify and repair computer system weaknesses, continually monitor systems, provide security training for employees, and ensure that service providers comply with the law through contract language requiring compliance.

As this study shows, institutions have proposed and implemented numerous IT security technologies and strategies. In many cases the investments haven't proven sufficiently effective, however, especially as threats to institutions' systems become commonplace and public scrutiny and press cov-

erage become harsh and often unforgiving. Awareness training and other interventions that address behavior and institutional values also haven't had the anticipated positive impact on internal security, largely because too few institutions have put them in place and many that have fail to deploy them regularly. Even where IT security measures are robust, failures abound.

The task appears daunting. Perhaps what most frustrates higher education's senior administrators is coming to grips with the reality that IT security is an ongoing process of continual refinement and investment. They can never know whether the institution is really secure despite their best efforts, and there is no end point.

## What Do We Mean by Information Security?

By far the most commonly used meaning for information security in the literature is the preservation of

- ◆ *confidentiality*, or protection from unauthorized use or disclosure of information;
- ◆ *integrity*, ensuring data accuracy and completeness through protection from unauthorized, unanticipated, or unintentional modification, and including *authenticity* (the ability of a third party to verify that a message's content has not been modified in transit), *nonrepudiation* (the origin or receipt of a specific message must be verifiable by a third party), and *accountability* (an action can be traced uniquely to an entity); and
- ◆ *availability*, making data available to authorized users on a timely basis and when needed.

We can, in turn, characterize each of these six protection categories—confidentiality, integrity, authenticity, nonrepudiation, accountability, and availability—by level of sensitivity: high (grave injury to an institution), medium (serious injury), and

low (minor injury).<sup>4</sup> (See the sidebar “ISO Standards” for information about ISO/IEC 17799:2000 standards.)

The above nuances are significant for higher education, where much information used for teaching and research requires the highest level of integrity and availability but a low level of confidentiality. For public institutions, this also holds true for much of their financial information. However, in areas protected by FERPA (Family Education Rights and Privacy Act), HIPAA (Health Insurance Portability and Accountability Act), and the Gramm-Leach-Bliley Act, and for sensitive research data, all six of the protection categories must be at the highest level. A compromise in any one area potentially puts the institution at significant risk.

College and university administrators thus face the dilemma of how to build information systems that can support the institution's public and open missions and academia's intellectual curiosity while protecting the privacy and intellectual property of the institution and its community. Higher education's information systems must be both open and closed, depending on what kind of information is being viewed and its intended use. Flexibility is essential, and it must accommodate campus security needs and cultural values alike.

According to Gordon Wishon, CIO, associate vice president, and associate provost at Notre Dame University, finding the balance is the \$64,000 question. “I don't know if we can guarantee that we can strike a precise balance, partially because the requirements and threats are always changing and the legislative landscape and technology are changing. Whether we achieve this is something that I think we will always be questioning.” For Philip Long, CIO at Yale University, “the overall strategy is that we want a controlled, open network. It is not completely open by default; it is opened by request. That is the

punch line to our strategy—finding ways to run networks and network segments that are opened by request.”

Diana Oblinger, executive director of higher education, Microsoft, and former ECAR senior fellow, eloquently addressed this dilemma.<sup>5</sup> For higher education, “intellectual freedom provides for free and open scholarly inquiry, freedom of information, and creative expression, including the right to express ideas and receive information in the networked world. One possible interpretation of intellectual freedom is that individuals have the right to open and unfiltered access to the Internet.” She further noted that “the academic culture tends to favor experimentation, tolerance, and anonymity—all characteristics that make it more difficult to create a culture of computer and network security.” The challenge is to appropriately balance values, risk, and realistic safeguards.

The legal and regulatory environment also poses many challenges for higher education. According to Kenneth Salomon and colleagues, “Federal laws have failed to keep pace with technological innovations. The result has been an atmosphere of uncertainty, in which already scarce university resources are increasingly strained by policy considerations and constrained by fears of legal exposure. The absence of a single set of standards further complicates the issue, leaving administrators and IT directors struggling to decide how best to protect their institutions, while at the same time not interfering with their educational mission. Navigating this maze is made even more difficult due to the fact that many of the laws are overlapping or apply differently to different institutional activities.”<sup>6</sup>

HIPAA is a particular force at this time. In the 14th annual Healthcare Information and Management Systems Society (HIMSS) Leadership Survey (2003) of leaders in hos-

## ISO Standards

ISO/IEC 17799:2000 uses an elaborate set of standards that includes

### System Access Control

- 1) To control access to information
- 2) To prevent unauthorized access to information systems
- 3) To ensure the protection of networked services
- 4) To prevent unauthorized computer access
- 5) To detect unauthorized activities
- 6) To ensure information security when using mobile computing and telenetworking facilities

### System Development and Maintenance

- 1) To ensure security is built into operational systems
- 2) To prevent loss, modification, or misuse of user data in application systems
- 3) To protect the confidentiality, authenticity, and integrity of information
- 4) To ensure IT projects and support activities are conducted in a secure manner
- 5) To maintain the security of application system software and data

### Compliance

- 1) To avoid breaches of any criminal or civil law; statutory, regulatory, or contractual obligations; and of any security requirements
- 2) To ensure compliance of systems with organizational security policies and standards
- 3) To maximize the effectiveness of and to minimize interference to/from the system audit process

### Personnel Security

To reduce risks of human error, theft, fraud, or misuse of facilities; to ensure that users are aware of information security threats and concerns and are equipped to support the corporate security policy in the course of their normal work; to minimize the damage from security incidents and malfunctions and learn from such incidents.

### Security Organization

- 1) To manage information security within the institution
- 2) To maintain the security of organizational information processing facilities and information assets accessed by third parties
- 3) To maintain the security of information when the responsibility for information processing has been outsourced to another organization

### Computer and Operations Management

- 1) To ensure the correct and secure operation of information processing facilities
- 2) To minimize the risk of systems failures
- 3) To protect the integrity of software and information
- 4) To maintain the integrity and availability of information processing and communication
- 5) To ensure the safeguarding of information in networks and the protection of the supporting infrastructure
- 6) To prevent damage to assets and interruptions to business activities
- 7) To prevent loss, modification, or misuse of information exchanged between organizations

### Asset Classification and Control

To maintain appropriate protection of institutional assets and to ensure that information assets receive an appropriate level of protection. Included here are policies for asset classification, asset protection, asset management, acceptable use, vulnerability assessment and management, threat assessment and monitoring, and security awareness.

### Security Policy and Its Deployment

To provide management direction and support for information security through document version control, difficulty of use—can you read and understand them?—distribution and ease of access, awareness, and compliance.

pitals, sponsored by the Superior Consultant Company, 61 percent of respondents—the second largest group in the survey—noted HIPAA compliance as having the biggest impact on them in the next two years (ranked second). Forty-three percent indicated that they would have to upgrade their IT systems' security as a result.<sup>7</sup>

Finding a correct balance proves extremely difficult in an open milieu with enormous network bandwidth, organizational diversity and autonomy, and a confusing legal environment, and where security breaches are increasing in number and notoriety. Moreover, for some insiders, compromising their institutional systems is a cottage industry—a personal challenge, perhaps just for fun.

### **How Do We Establish Security Requirements?**

According to ISO/IEC 17799:2000, an international standard for information security management, there are three dimensions to establishing an institution's security requirements. The first is through an institutional risk assessment, which is designed to determine the likelihood of internal and external threats to the institution and reveal its vulnerabilities. The second is the legal, statutory, regulatory, and contractual requirements imposed on the organization—for example, by HIPAA and FERPA. The third is the policies, procedures, and practices the institution has created for itself. This study does not focus directly on the legal environment but does try to determine whether higher education institutions have undertaken risk assessments and developed policies that help them establish security requirements.<sup>8</sup>

### **Security Threats and Breaches**

According to the ISO, a breach can be viewed conceptually as a vulnerability, a

threat, or a risk. "A vulnerability is an error or a weakness in the design, implementation, or operation of a system. A threat is an adversary that is motivated to exploit a system's vulnerability and is capable of doing so. Risk refers to the likelihood that a vulnerability will be exploited, or that a threat may become harmful."<sup>9</sup>

The combination of university systems' open nature and the high-powered technology often present on campuses puts academic institutions in a unique position compared with other large enterprises. In addition to being the target of cyber attacks, university networks and systems sometimes serve either as the source of attacks on other entities or as a staging area for attacks on other entities by external hackers. This happened to Yahoo, Amazon, and eBay in February 2000. In this instance, a teenage hacker took control of computers owned by institutions including Stanford University, UCLA, and the University of California at Santa Barbara and used them to block access to these major e-commerce sites. For many institutions, being a good "net citizen" and preventing use of institutional resources for such attacks is nearly as high a priority as protecting their own information.

### **Higher Education's Responses**

Universities are responding to threats creatively by using new technologies and their substantial intellectual resources. At the University of Minnesota, Twin Cities, for example, the Minnesota Intrusion Detection System employs a suite of data-mining techniques to automatically detect novel and emerging attacks against computer networks and systems. The system has successfully detected attacks that are on the CERT (Computer Emergency Response Team) list of recent advisories and incident notes.<sup>10</sup> Summarizing anomalous connections using association pattern analysis has been very

helpful in understanding the nature of cyber attacks and creating new signature rules for intrusion detection systems.

Increasingly, institutions provide education and professional training and are creating centers of academic excellence that undertake basic and applied research and development in information security. For example, in April 2003, Indiana University established the Center for Applied Cybersecurity Research to provide an environment where information security research and practice are intertwined, and Indiana University staff learn from each other. The center's goal is to maximize the speed with which new cyber research is applied and new cyber threats become the subject of research.<sup>11</sup>

EDUCAUSE has long been recognized as a major participant in national efforts to secure higher education's communication and computing infrastructure. It has participated with Internet2 to conceive, develop, and deploy technologies, techniques, and standards to enhance identity services and other middleware elements essential to IT security. A joint EDUCAUSE/Internet2 Computer and Network Security Task Force has identified issues for further study, including how to make IT security a higher and more visible priority in higher education; using existing security tools more effectively; revising institutional policies; and designing, developing, and deploying improved security for future research and education networks. In the spirit of the Bush administration's national security goals, the task force seeks to raise the level of security collaboration among higher education, industry, and government and to integrate higher education work on security into the broader national effort to strengthen critical infrastructure.

The tragic events of September 11, 2001 made protecting the information infrastruc-

ture even more urgent. Securing cyberspace has become one of the pillars of the U.S. Department of Homeland Security's efforts. Especially noteworthy is the release of the Bush administration's cybersecurity plan on 14 February 2003. The national strategy addresses vulnerabilities of higher education institutions and acknowledges higher education's pledge to

- ◆ make IT security a priority;
- ◆ revise institutional security policy and improve the use of existing security tools;
- ◆ improve security for future research and education networks;
- ◆ improve collaboration between higher education, industry, and government; and
- ◆ integrate work in higher education with the national effort to strengthen critical infrastructure.<sup>12</sup>

In partial response to the federal initiative, EDUCAUSE, working with the American Council on Education (ACE) and the Higher Education IT Alliance, has recommended policies and measures necessary to realize greater system security. On 28 February 2003, ACE President David Ward urged university presidents to set the tone for information security on their campuses by insisting on community-wide awareness and accountability and establishing responsibility for campus-wide information security at the cabinet level. Further, presidents should routinely ask for a periodic information security risk assessment, manage risks in the context of institutional planning and budgeting, and regularly request updates to their institutions' information security plans to keep pace with the rapid evolution of the technologies, vulnerabilities, threats, and risks.

To contribute to the information infrastructure's national security, Indiana University partnered with the National

Infrastructure Protection Center (NIPC) in establishing the first higher education Information Sharing and Analysis Center in February 2003. The center's goal is to help protect the nation's colleges and universities from cyber attack and provide incident information to the NIPC.<sup>13</sup>

## **What's Different About IT Security in Higher Education?**

No study of IT security in higher education can ignore the common belief that higher education varies significantly from other industries and that IT security presents a different and extremely difficult challenge for IT security officers and administration. This view pervades the literature we reviewed. Diana Oblinger nicely captures many of the most common arguments.<sup>14</sup> Briefly, many perceive higher education to be less secure in part because of its values such as academic freedom and freedom of expression, its decentralized organization, the *mélange* of hardware and software in use, and its unique mission and user base. As a consequence, the IT security strategies higher education must follow will differ and be more complicated than those in other industries. If higher education is different, do the dissimilarities, if real, make a difference?

### **Decentralization**

In many collegiate environments, particularly larger ones, a decentralized culture is the norm. As a result, individual schools, laboratories, and departments may control a portion of any or all of the previously mentioned IT assets, making the job of the IT security administrator much more difficult. Rather than being able to automatically push new security patches out to all devices on the network or mandate the use of security tools like virus protection software, many

university IT security officers find they must educate and persuade their user community to keep their machines secure.

In most corporate IT departments, centralization is the norm. The central IT organization controls hardware purchases, software loadsets (common sets of software installed on a computer), network infrastructure, user management, and most other aspects of computing within the organization. This enables corporations to centrally set security policies, make secure versions of operating systems and applications available to all users, control access to services being used on their network, and restrict or forbid use of insecure products and protocols.

### **Equipment Diversity**

Even a small higher education institution's technology environment varies significantly from the structure found in the corporate world. One of the biggest differences is that the institution does not actually own a large percentage of the machines on its network; many belong to students connected to the institution's network in a dorm room or classroom. The technologies deployed at a typical college or university tend to be much more diverse than at a corporation. For example, a university network may have desktop machines from many vendors running multiple versions of Windows from 95 to XP, Macintosh PCs running several versions of the MacOS, and Linux workstations running several variants of that operating system. Software loadsets, if they exist at all, are likely created and managed at a departmental level. Server environments can be equally diverse, and many servers are purchased and administrated by semiquified staff or graduate students within schools, departments, or research labs.

For an IT security administrator, this diverse environment makes it difficult to

ensure that all systems are patched with the latest fixes or configured to limit security exposure. It also makes it difficult to provide IT security tools like antivirus software or personal firewalls to the university community because each platform needs a different version or even a completely different application. With so many machines not owned by the institution connected to the network, the security administrator must assume that there will always be insecure systems inside the perimeter and should expect to take additional steps to protect the institution that wouldn't be necessary in the more controlled corporate environment.

In a typical corporate environment, technology standards control the type of equipment connected to the company's network. Even in a large organization, all PCs and servers would be running the same operating system version, all similar hardware types would be purchased from the same vendor, and systems would use standard loadsets certified for security. Additionally, employees would be barred from putting rogue systems on the corporate network.

### **Mission Diversity**

A typical university engages in many diverse business activities as part of its mission. In addition to teaching, many institutions conduct a wide range of research, provide hospitality services (dorms and dining halls), serve as ISPs and phone companies, engage in retail sales (bookstores, food concessions), manage financial accounts, and provide entertainment (athletics, arts), to name just a few. As a result, the IT environment of all but the smallest colleges is necessarily complex and constantly changing. And many institutions leave the selection and maintenance of systems used to support these functions to the individual business units.

For the security administrator, such complexity makes it more difficult to detect

potential intrusions, because network traffic is much more unpredictable. Likewise, the diverse range of network services that must often be deployed, particularly at research institutions, makes it difficult to maintain effective firewalls. And the sheer number and diversity of applications the institution hosts makes it difficult for a central security organization to support each system, thus shifting the burden to the business units, which may not have the skills to maintain these systems.

Except at the largest corporations, IT security administrators in the private sector typically support an organization that conducts a limited range of business activities—for example, selling merchandise, managing financial accounts, or manufacturing products, along with the back-office functions that support this core activity. The IT environment needed to support these business activities is predictable, with relatively standard transaction flows and a limited set of network services required to enable these flows.

### **User Diversity**

Corporate IT security administrators can generally assume that most legitimate connections coming from within their perimeter are being initiated by an employee of their organization. While such users can and do cause intentional security breaches, corporations can screen their employees for criminal backgrounds, mandate training, require the use of certain security technologies, and strongly enforce IT security policies.

However, for university security administrators, high-security-risk individuals are already inside the gates. On campuses with residential housing or wired classrooms, students freely connect insecure systems to the institution's network and, not being employees, cannot easily be made to comply with training, policies, and other tools avail-

able to the corporate security administrator. In Chapter 7 we report that institutions with residence halls were nearly three times more likely to have experienced a significant security incident than those without.

In addition, universities are generally open environments. On many campuses, visitors can plug a laptop into any available data port and gain access to the institution's network. Even in institutions that restrict such access, visitors can often use library machines, public kiosks, or machines in public computer labs, likewise giving them internal access to the network.

To mitigate the risks associated with non-employee network access, some institutions require all systems connected to the campus network to register their hardware address with central IT before they can use DHCP (dynamic host configuration protocol) servers to receive an IP address. This prevents random people from accessing the institution's IP network using network ports in public spaces. Others require authentication to access any machine on campus, including lab and library systems. This is less of an issue for institutions that have chosen an IT security strategy that doesn't rely heavily on perimeter firewalls, because having direct access to the network doesn't provide a potential internal attacker significant advantage over an external attacker.

## Research

Institutions that attract significant research funding have some unique issues of their own. By their nature, research labs encourage experimentation and often have extremely diverse computing environments, as explained by Michail Bletsas, director of computing at the Massachusetts Institute of Technology's (MIT) Media Lab. "The central [IT organization at MIT] follows standards a lot closer than we do. We have no standards by design, because of the research

nature of the facility. People are allowed to use whatever they feel like." In addition, these systems may often store sensitive data, making them important to secure. However, partially because of the culture at many institutions and partially because of the rules governing coverage of institutional support costs from federal research grants, these systems are very often not under the purview of professional IT staff. Instead they reside in individual research facilities, managed on an ad hoc basis by graduate students.

Managing an IT security environment that incorporates a large research community therefore poses some special challenges for administrators. Several research universities we interviewed espouse an IT security philosophy seldom seen in the corporate environment: they make maintaining security on the institution's desktop and server systems the responsibility of each system's "owner." To ensure that such an environment does not descend into chaos, these institutions' central IT organizations provide their communities with common tools, such as antivirus software and operating system patch installers. They also conduct proactive monitoring of the systems connected to the institution's network and alert system owners of any vulnerabilities or security breaches they discover, removing infected systems from the network if the problem is not or cannot be quickly corrected. It then becomes the system owner's responsibility to remediate the problem before the system is allowed back on the network. Such an approach may not work for every institution, but those currently using it find it allows relatively small IT security teams to manage very large environments with few, if any, major incidents.

## What Are We Protecting?

Most of the information stored on the systems of for-profit entities is confidential in

nature. From trade secrets to financial data to customer and employee information, such data is not made public, and corporations face serious financial consequences should such data be compromised. For example, the 2003 CSI/FBI Computer Crime and Security Survey reported that theft of proprietary information caused the highest losses for any type of IT security incident (\$70.2 million, of approximately \$202 million in total losses reported by 251 of their survey respondents). Denial-of-service attacks generated the second-highest losses (\$65 million), as such attacks can quickly disrupt the core business of many enterprises. As a result of this large financial exposure, many for-profit entities strongly emphasize IT security, with the average respondent to *Information Week's* 2002 Global Information Security Survey spending approximately 12.4 percent of their overall IT budget on security. The average salary for information security managers in industry, as reported by *Information Security Magazine* in August 2002, is \$121,000 per year.

By contrast, in higher education much of the data institutions store is not considered sensitive. At many public institutions, financial data and employee salaries are considered public records, making the expenditure of significant time and effort to secure them less important. Some information, of course, such as donor records, research data, and personal information about students and employees, is private. For the most part, universities seem to focus more on providing a trusted technology environment to enable their constituents' work rather than protecting data stored on their systems. John Curry, executive vice president at MIT, said, "I tend to think of security starting first and foremost with people, and their ability to live and work here. This leads in turn to the need for security personnel and technologies, from streetlights to fire protection to data protection. We want to provide [our

community with] a sense that your computer is a safe thing to use. We want to protect their productivity."

Additionally, denial-of-service attacks are less of an issue for most higher education institutions. While a disruption to network services in the middle of a registration cycle, for example, would be a major annoyance, it would not curtail the university's ability to teach courses, conduct research, or otherwise carry out much of its day-to-day business (although this could change if distance learning becomes a larger part of the curriculum).

We feel that this disparity in exposure may be at least partially responsible for much of higher education's perceived underinvestment in IT security, because the financial risks institutions face amount to significantly less than those faced by comparably sized for-profit businesses. For example, results presented in Chapter 5 show that 78 percent of our survey respondents spend 5 percent or less of their central IT budget on security and that only 11 percent of respondents pay their IT security managers more than \$100,000. This may not be an underinvestment at all but rather a decision by senior executives that IT security, as part of the overall portfolio of risks the institution faces, may not warrant as high a level of investment as it does in other industries. However, recent legislation, such as HIPAA and Gramm-Leach-Bliley, that includes IT and data security provisions may change this calculation, as these regulations include significant penalties for noncompliance.

### **Need for More Study: ECAR's Role**

Despite the national attention and ongoing efforts of EDUCAUSE, Internet2, and other organizations to develop and foster a modern and secure IT infrastructure in higher education, our knowledge

of the current state and future plans of colleges and universities vis-à-vis IT security is largely anecdotal. We have little quantitative information with which to benchmark IT security. Security leadership is purported to be reactive rather than proactive, with a lack of clearly defined goals. Similarly, the academic culture is purported to believe that security is antithetical to academic and intellectual freedom.

This ECAR study is designed to provide a first empirical perspective of higher education's security environment, one that we anticipate will lead to information security improvements across the sector. It establishes a security baseline for higher education. It identifies what security policies, products, and procedures are currently in place. College and university administrators will be able to compare their institution's investments and practices with those of similar institutions. This is a necessary first step in determining the security level that needs to be sought. Systematic quantitative data also makes it possible to assess what heretofore has been anecdotal information about IT security in higher education as well as some myths that surround IT security.

This report emphasizes both the benefits and risks of implementing security solutions while considering trade-offs and future trends. We expect this data to contribute to the improvement of information security for higher education. If demonstrating information security to the public becomes as important as demonstrating institutional fiduciary responsibility, then benchmarking what is currently in place will be a critical step toward establishing standards for demonstrating IT security.

One message will become clear as we present the data in this study: higher education is all over the map when it comes to IT security. At the same time, we can discern several trends that suggest increasing

agreement on standards, organization, and practices. The question is, How soon do we reach an agreement?

## Endnotes

1. D. Ward and B. L. Hawkins, "Presidential Leadership for Information Technology," *EDUCAUSE Review*, Vol. 38, No. 3, May/June 2003, p. 45.
2. The CERT Coordination Center (CERT/CC) reported that IT security incidents grew from 252 in 1990 to 82,094 in 2002. In 1995, 171 vulnerabilities were reported compared to 4,129 in 2002. See <<http://www.cert.org/stats/#incidents>>.
3. D. Carnevale, "When is a college like a bank?" *Chronicle of Higher Education*, 11 July 2003, pp. A27–A28.
4. NIST Special Publication 800–26, *Security Self-Assessment Guide for Information Systems*, Nov. 2001, pp. 5–6. The U.S. National Institute of Standards and Technology provides an alternative definition for information infrastructure protection. By information infrastructure they mean "technologies, processes, and activities to protect information infrastructures from hostile threats, to detect unauthorized or potentially damaging behavior, to react to detected or suspected incidents, and to ensure accountability for actions involving information infrastructure components. Legal, policy, and cultural imperatives that constrain or otherwise influence the way technology is used or developed are integral to the concept of an information infrastructure."
5. D. Oblinger, "Computer and Network Security and Higher Education's Core Values," *EDUCAUSE Center for Applied Research Bulletin*, Vol. 2003, Issue 6, 18 Mar. 2003.
6. K. D. Salomon, P. C. Cassat, and B. E. Thibeau, *Electronic Information Security: A Legal Perspective* (Dow, Lohnes & Albertson, PLLC, Feb. 2003). The EDUCAUSE/Internet2 Computer Network Security Task Force commissioned the work, and the authors received a grant from the National Science Foundation. Their work provides an overview of the current legal landscape and factors that foster an atmosphere of confusion and uncertainty as to how to proceed in the current legal environment. The paper summarizes existing federal and state privacy and security-related laws affecting institutions of higher education and explains their implications.
7. HIMSS (Healthcare Information and Management Systems Society) is the healthcare industry's only membership organization exclusively focused on providing leadership for the optimal use of health-

- care information technology and management systems for the betterment of human health. HIMSS is the equivalent of EDUCAUSE for the healthcare provider industry.
8. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), *Information Technology—Code of Practice for Information Security Management*, ISO/IEC 17799:2000, p. ix.
  9. Ibid.
  10. The CERT Coordination Center (CERT/CC) is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.
  11. M. McRobbie, 17 Apr. 2003, <<http://www.indiana.edu/~uits/cpo/cacr041703/>>.
  12. The full report is available from the White House Web site at <[http://www.whitehouse.gov/pcipb/cyberspace\\_strategy.pdf](http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf)>.
  13. See <<http://www.nipc.gov/pressroom/pressrel/NIPCandIU.htm>>.
  14. Oblinger, op. cit.