**EDUCAUSE Center for Applied Research**

Research Bulletin

Volume 2003, Issue 23

November 11, 2003

# Information Technology Security Policy: Keys to Success

Judith Borreson Caruso, University of
Wisconsin–Madison and ECAR

4772 Walnut Street, Suite 206 ◆ Boulder, Colorado 80301-2538 ◆ www.educause.edu/ecar/

# Overview

When computer use hit the mainstream in the early 1980s, personal computers and open networks held great promise not only for enriching communication but also for enabling society to become more self-aware. In the early days, keeping networks open for academic pursuits was a natural match for the Zen of high technology. Founded on principles of good faith, open access, and a self-governing “netiquette,” the Internet fit naturally and comfortably into the culture of higher education. Even before the World Wide Web was a glimmer in the eye of Tim Berners-Lee, computing and network tools enabled scholars to explore their disciplines in exciting and new ways.

Awed by the ever-increasing possibilities of the new technologies, and busy learning how to apply them, academics, administrators, computer engineers, and even technology vendors focused more on information sharing than on information security. To be sure, those most closely connected to the technologies were keenly aware of how vulnerable the computer systems were to malicious attackers. There were, of course, ways to keep computers secure, but closing the loopholes that prevented “bad guys” from getting in also meant closing off access for legitimate and important scholarly exchange.

From the start, information security was a priority for military and corporate computers as well as for networks and applications serving health and other specialized industries. Computers on major university campuses often had connections to these secure computers. By exploiting the open access policies of higher education, malicious hackers could use university-based computers to gain access to otherwise impenetrable resources.

In 1986 Clifford Stoll, a relaxed astronomer-turned-programmer who had recently started work at the Lawrence Berkeley Laboratory near San Francisco, noticed a 75-cent discrepancy between the amounts recorded by two different accounting programs used to charge people for computer use. What he first thought was a software bug turned out to be a lead in a chase to catch dangerous computer hackers. The chase led from university computers in California to West Germany and, at Stoll’s instigation, included investigators from the FBI, the CIA, the NSA’s National Computer Security Center, and the Air Force Office of Special Investigation. It resulted in the arrest of a group of German hackers who had been scouring American military systems for material to sell to the KGB. Stoll memorialized his story in *The Cuckoo’s Egg: Tracking a Spy through the Maze of Computer Espionage*.[1] The epilogue to the book discusses Robert T. Morris Jr.’s famous 1988 Internet worm program, one of the many nails that have now been driven into the coffin of the open computer society.

As evidenced by several recent breaches at U.S. colleges and universities,[2] the stakes for IT security have risen quite high. Likewise, the breadth and sophistication of information security incidents have increased. Such incidents, along with the impacts of increased federal and state legislation regulating computer and network security, have raised the topic of IT security to the level of the executive agenda. In large part, higher education institutions choose to address issues of IT security through policies designed to describe acceptable use of the institution’s computer and network resources. Such policies, some of which have been in place for decades, are being revisited and strengthened as institutions become increasingly accountable for demonstrating that they protect individual privacy (student records, health records, and so on), that they are responsible Internet service providers, that they respect and protect online intellectual property, that their online banking transactions are secure, and that they support antiterrorist programs and legislation. It seems that no sooner do institutions recover from one virus, security breach, or legislative compliance initiative than another is knocking at the door.

For the purposes of this research, the U.S. General Accounting Office (GAO) definition of information technology security policy is used: “The framework within which an organization strives to meet its need for information security is codified as security policy. A security policy is a concise statement, by those responsible for a system (such as senior management), of information values, protection responsibilities and organizational commitment.”[3]

## Highlights of IT Security Policy

Information technology security policies currently in place or under development at higher education institutions vary in scope, breadth, and depth. This is not only understandable but also appropriate. Because each higher education institution varies in size, complexity, and culture, IT security policies are most effective when they map to the individual institution’s needs. These security policies often include guidance directed at ensuring legislative compliance, protecting university assets, and ensuring confidentiality and privacy.

Many federal and state laws have been enacted over the past few years in response to the explosion of electronic information. These laws have greatly increased the rules under which higher education institutions must operate, presenting a challenge for institutions to keep their security policies current. In *IT Security for Higher Education: A Legal Perspective*, published in 2003 by the EDUCAUSE/Internet2 Computer and Network Security Task Force, Salomon, Cassat, and Thibeaus note that these new laws

> … have failed to keep pace with technological innovations. The result has been an atmosphere of uncertainty, placing further strain on already scarce institutional resources and leading in some cases to inaction as a result of concerns over 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.[4]

The potential legal exposure and liability are significant, and IT security policies must be shaped to ensure compliance while reflecting the institutional persona.

Most importantly, IT security policies provide higher education community members with guidance about what is expected of them. Glenn Hill, information security officer of Northeastern University, described policy development at his institution:

> Information technology policies here are a statement of our values. They uphold the mission of the institution. They're designed to protect the rights of individuals and the organization. At a minimum, they help influence use of technology in ways the community expects and respects. They are our public persona—what we will be measured on. They have a direct impact on our public image and form the very foundation on which all our information security efforts are built.[5]

All of an institution's IT security policies together provide a framework in which to place security standards, processes, and procedures.

## Shaping Information Technology Security Policies

Institutions of higher education can create IT security policies through a formal policy program or through informal processes. These efforts are typically shaped by the institution's culture. Over the past five years, many institutions have created formal programs for IT security policy development, dissemination, and monitoring. These programs not only include a description of the processes for creating and disseminating policies but also a definition of the roles and responsibilities for university faculty, staff, and students. Other institutions have used a less formal approach, using best practices and security procedures to frame the institutional response.

Before embarking on development of an IT security program, an institution should consider what benefits it expects to achieve and whether a formal IT security policy program is a good fit for the institution. For example, the Indiana University (IU) Information Technology Policy Office, which provides a formal program of information technology policy development, dissemination, and education at IU, has been described as providing the following benefits:

- Function dedicated to developing and maintaining consistent IT appropriate use policies
- Education on common issues, appropriate use, and university IT policy
- Assistance in reviewing specific situations and analyzing and determining appropriate IT policy
- Assistance in coordinating appropriate technical investigation for violations of law or policy
- Assistance in packaging technical information for IU governance agencies, IU legal counsel, law enforcement, prosecutors, university administration, etc.
- Common and consistent incident response
- Incident statistics collection and reporting

- Assistance in determining incident cost, valuable in determining appropriate safeguards
- Formal online incident tracking and archiving[6]

While these benefits fit appropriately within the Indiana University framework, each institution must decide for itself what benefits it hopes to achieve and structure its IT security policy program or process for development and dissemination accordingly.

## IT Security Policy in the Context of Risk

One often thinks of IT security in terms of managing incidents that involve unauthorized access to systems, compromised data, or the spread of malicious computer viruses. In fact, institutional IT security risks span a much larger landscape. McMillan and Sitko outline the breadth of this domain in “Managing University Business Continuity.”[7] Among other questions, they invite higher education officials to ask, “What would result from the partial or complete destruction of key buildings and the records they contain? What if the systems that control fire alarms and security systems in residence halls, classroom buildings, or administrative facilities are compromised? … How does an institution operate in the face of long-term inaccessibility to communication infrastructure? Who has the authority to declare a campus emergency, and where are emergency protocols maintained? … How does an institution determine how much risk is acceptable?”

Within this context, shaping a formal or informal process for IT security policy development requires knowing the priorities of the institution and the best way to structure policy programs to support them. For example, at some institutions a university-level policy office is responsible for overseeing policy development and dissemination in all areas, including human resources, academic freedom, copyright, finance, and information technology. Other institutions with more decentralized structures ask responsible functional offices to determine the best way to develop and communicate policies from their areas across the institution. In “Resolving Information Technology Policy Issues on the Networked Campus,” Tracy Mitrano, director of information technology policy and computer law and policy at Cornell University, identified three models for policy development and management: the central policy development office model, the decentralized model, and the hybrid model.

> In the centralized model, the highest leaders of the institution—that is, the president or provost—authorize a specific policy office to be the central repository of campus policy and to deploy its personnel in the service of executing a uniform procedure for formulating and issuing policy. … Policy development in the decentralized model is instead left to the individual departments or units, with the underlying understanding that should a conflict between them emerge, a robust and authoritative administration will act as the arbiter of the dispute. … Most institutions use a hybrid model in which some aspects of policy development are centralized and others are not. Some colleges and universities may employ a select group of administrators or constituent representatives to vet policy, but may not have formalized either that membership or the process by which the vetting occurs. … The

> ubiquitous role that information technologies play in higher education makes these distinctions among models for policy development significant.[8]

It is wise for institutions with a formal institutional policy-development process to include IT security policies among the areas covered. Policy development is often deeply embedded in the institution's values and assumptions, and roles and responsibilities are clearly delineated. IT security policy, however, is the new kid on the block. New governance structures, approval mechanisms, and dissemination procedures must be established. According to 435 higher education respondents to an April 2003 IT security survey conducted by ECAR,[9] many institutions are just getting started—beginning with the central IT organization.

The depth and breadth of the IT security policies developed at an institution are largely a reflection of the culture of an institution. In a highly decentralized institution, there are likely very few institutional-level policies. Instead, such institutions might establish guidelines, procedures, incentives, and recommendations that schools, colleges, and departments can use to create their own policies and procedures. In these cases, it is the responsibility of individual units to develop and disseminate their own IT security policies, procedures, and processes. Centralized initiatives, however, such as a site license for anti-virus software, can provide incentives for schools, colleges, and departments to adopt policies and procedures that result in tightened network security, both locally and across the institution. Even in a very centralized institution, certain policies must likely be created primarily within the confines of part of the institution, such as HIPAA policies to protect the privacy of individual health records in the medical school, dental school, or student health service. At the same time, the HIPAA-related IT security implications for the campus network and centrally supported systems and applications are institution-wide risks that must be addressed.

Another consideration for an institution in IT security policy development is to review the relationship between security policy and security practices. Mark Bruhn, chief IT security and policy officer and associate director of the Center on Applied Cybersecurity Research of Indiana University, emphasized the importance of policy: "Institutional values drive policy; policy dictates processes, procedures, and standards; and security implements those."[10] Since policy lays the foundation for security, it is important to ensure that the policies developed reflect the institutional priorities and needs. Policies that fit the institution well will be easy for students, faculty, and staff to understand.

As an institution moves to create or refine IT security policies, it important to consider the balance among academic freedom, an open Internet, and the assets that the institution is charged to protect. In a recent article, Kent Wada advised:

> We must ensure that our decisions carefully weigh all arguments, balancing between conflicting needs and viewpoints of our campus communities. Determining how much monitoring is "appropriate," for example, is made even more challenging by ambiguity in, and national controversy over, untested new laws and shifting expectations. Each institution will likely come up with a different answer, as local cultural values will always frame the discussion.[11]

This conflict between academic freedom and freedom of speech and the need to control access, protect assets, and ensure privacy is a challenge best met through a dialogue within the institution about the amount of risk the institution is willing to take and the amount of control it requires. This assessment of risk and possible solutions should include considerations related to

- **Legal obligations.** These obligations span the alphabet soup of FERPA, HIPAA, DMCA, TEACH Act, Gramm-Leach-Bliley, SEVIS, USA PATRIOT Act, and so on. Salomon, Cassat, and Thibeaus recommend that institutions review recent legislation and decide what they should do.[12] They advise the following actions:
  - Analyze applicable state laws and municipal ordinances
  - Assess information security vulnerabilities and risks
  - Review and update information security policies and procedures
  - Review personnel policies and procedures for access to sensitive information
  - Scrutinize relationships with third-party vendors
  - Review the institution's insurance policies
  - Develop a rapid-response plan and incident-response team
  - Work with higher education associations and coalitions to develop standards relating to information security
- **Protection of university information assets.** An institution should review its information assets—not only the centrally maintained student, finance, and human resource data but also, for example, alumni, customer, and health-related data that are not maintained centrally—and determine what policies are needed.
- **Education of students, faculty, and staff.** Since security breaches are often caused by human error, it is important for institutions to increase security-policy and best-practices awareness for students, faculty, and staff. An information and training program on security policy and security best practices tailored to the institution can significantly reduce institutional risk.
- **Protection of privacy.** An institutional privacy policy and appropriate security practices can not only reduce risk but also reassure students, faculty, and staff that their rights are being protected, especially if the institution operates in an open-to-the-Internet environment.
- **Protection of confidential or sensitive data.** In recent years, the risk of exposing confidential data such as Social Security numbers has become an important concern for higher education institutions. An access to data policy, for

example, reduces this risk and informs students, faculty, and staff of their responsibilities regarding access and use of data.

- **Changes in the technological environment.** New technologies, implemented appropriately, can reduce risk and enable automation of policies, thereby ensuring policy adherence.

- **Changes in the institutional culture.** As institutions evolve, IT security policies and institutional risk should be reviewed to ensure that the policies continue to fit the institution's culture and needs. Adjustments to existing information technology security policies are not only necessary but also inevitable. The campus network environment, for example, is constantly changing. Also, changing legal requirements may require policy updates. Additionally, the nature of the threats keeps changing as hacker software becomes more sophisticated, requiring greater diligence in policy and security. Of course, technology is changing as well and may impact how a policy is implemented.

## Developing IT Policy in Higher Education

In the past few years, legislation impacting higher education has grown to such an extent that some institutions that had little or no formal IT policy development processes are now adopting them. Often an IT security officer leads the effort. According to the ECAR IT security survey, the number of IT security officers has greatly increased in the past 10 years.[13] Seventy-five percent of the 435 institutions that responded to the survey reported having such a function.

One challenge for initiating an IT security policy process is ensuring the engagement of all the stakeholders at the institution. For institutions that already have an official formal policy-development process in place, it may be a matter of piggy-backing on what already works with other policies. At institutions with no formal policy process, work on governance, development, and dissemination processes is required. At Cornell University, for example, a formal policy creation process for the institution is defined. In Cornell's "Formulation and Issuance of University Policies," a university policy is defined by all of the following criteria:

- It has broad application throughout the university.

- It helps ensure compliance with applicable laws and regulations, promotes operational efficiencies, enhances the university's mission, or reduces institutional risks.

- It mandates actions or constraints and contains specific procedures for compliance, and articulates desired outcomes.

- The subject matter requires university president and/or executive officer review and approval for policy issuance and major changes.[14]

For institutions with a formal process, like Cornell, the creation of IT security policies will likely be easier to initiate than in those institutions with no defined process.

In the recent ECAR IT security study, 54 percent of the 435 institutions responding to the survey indicated that they had formal institutional IT security policies; another 37 percent had policies in the implementation stage. The status of policy development is shown in Table 1.[15]

**Table 1. IT Security Policies in Place**

| Status of Policies | Number of Institutions | Percentage |
|---|---|---|
| Implemented, interim, and implementing | 45 | 10.3 |
| Implemented and interim policies, not implementing | 13 | 2.9 |
| Implemented, no interim, implementing | 24 | 5.5 |
| Implemented, no interim, not implementing | 153 | 35.2 |
| No formal policy, have interim, are implementing | 39 | 9.0 |
| No formal policy, have interim, not implementing | 62 | 13.7 |
| No formal policy, no interim, are implementing | 64 | 14.7 |
| No formal policy, no interim, not implementing | 35 | 8.0 |

## Participants in Policy Development

It is important to the successful adoption of IT security policies that campus stakeholders be involved in policy development and dissemination. Respondents to the ECAR survey were asked to describe the level of involvement of their senior management in developing their institution's security policies. Researchers calculated the mean and standard deviation for each administrator/office/agency based on a Likert scale of 1 (strongly agree) to 5 (strongly disagree). Table 2 describes the results.[16]

**Table 2. Participants in the Development of IT Security Policy**

| Participation | Mean | Std. Deviation |
|---|---|---|
| IT Organization | 1.74 | 0.726 |
| CIO | 2.06 | 0.977 |
| Campus/Faculty Task Force | 2.89 | 1.262 |
| System Office | 3.10 | 1.245 |
| Internal Auditor | 3.31 | 1.149 |
| Provost | 3.48 | 1.160 |
| External Auditor | 3.58 | 1.094 |
| President | 3.67 | 1.035 |
| Board of Trustees | 3.90 | 0.927 |
| State Agency | 4.03 | 1.012 |

*Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)*

Today, there are many IT security policies in higher education. The policies currently covered are detailed in Table 3, as reported by respondents in the ECAR study.[17]

**Table 3. What Do the Policies Cover? By Carnegie Class**

| What Formal Policies Cover | Positive Response, by Carnegie Class (Percentage of Respondents) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | All | Dr. Ext. | Dr. Int. | MA | BA | AA | Specialized | System | Canada |
| Appropriate use of institutional assets | 99 | 99 | 97 | 99 | 99 | 100 | 90 | 94 | 100 |
| System access control | 89 | 83 | 91 | 90 | 90 | 88 | 88 | 71 | 79 |
| Authority to shut off Internet access | 85 | 89 | 89 | 80 | 90 | 67 | 81 | 82 | 84 |
| Data security | 83 | 80 | 86 | 79 | 86 | 84 | 78 | 71 | 68 |
| Network security | 82 | 78 | 86 | 84 | 83 | 79 | 82 | 71 | 79 |
| Enforcement of institutional policies | 82 | 75 | 88 | 78 | 80 | 86 | 81 | 65 | 79 |
| Desktop security | 80 | 70 | 71 | 72 | 91 | 88 | 86 | 52 | 74 |
| Physical security of assets | 71 | 62 | 66 | 67 | 71 | 72 | 76 | 65 | 68 |
| Residence halls | 61 | 75 | 74 | 68 | 70 | 7 | 42 | 44 | 53 |
| Remote devices | 51 | 51 | 54 | 42 | 51 | 45 | 52 | 41 | 53 |
| Application development | 39 | 32 | 40 | 41 | 31 | 35 | 38 | 41 | 29 |

Additionally, the EDUCAUSE policy program[18] solicits examples of IT security policies from higher education institutions.

## Recommendations for Success

A successful IT security policy program or process can be measured by how well its university community members are engaged in its development; how well they understand their individual roles and responsibilities; how effectively the institution can minimize damage from malicious attacks on and unauthorized access to their systems; and how well the institution protects the privacy of individuals and confidentiality of data. Attributes of a successful policy development program or process include the following:

- Active engagement of the president or provost is important. In “Meeting the Cybersecurity Challenge,” Johnson, Mitrano, and Vernon recommended establishing IT security policy as an executive priority, advising that either a centralized policy office or a group of the most senior executive administrators initiate and sign off on policies.[19]

- Involving institutional stakeholders in policy development is imperative to ensuring that policies are aligned with institutional practice. Active buy-in and input from across the institution is necessary for policies to be understood and followed. As illustrated in Table 2, many institutions seek active engagement from a campus/faculty task force, system office, internal and external audit, and provost in the development and dissemination of IT security policy.

- Institutional stakeholders, including faculty, staff, and students, should read, understand, and follow the policies developed. Awareness and informational programs are needed to ensure compliance.
- The security practices, processes, and procedures implemented at an institution should directly align with its IT security policies.
- According to the results of the ECAR security study, security policies must be easy to read, accessible, enforced, comprehensive in scope, regularly updated, and consistent across the institution so that faculty, staff, and students understand what is expected of them.[20]
- Policy compliance must be monitored and enforced by the appropriate university offices.
- Which IT security policies an institution needs varies by institution. It is important to designate a responsible party for keeping abreast of what is happening legislatively and culturally and recommending adjustments. Also, rather than developing an institutional policy, some institutions develop guidelines, encourage best practices, or create incentives to ensure appropriate IT security.
- IT security policy development processes must fit within the institution's priorities, culture, posture about risk, and policy development processes. IT security policies that accurately reflect the academic principles and priorities of the institution are more readily adopted than those that do not.

As an institution develops its IT security policies, it should keep in mind what benefits it hopes to achieve and measure its accomplishments correspondingly. These measurements can be enlightening to an institution as it tries to maintain a balance between academic freedom and ensuring a secure technical environment.

## What It Means to Higher Education

The world is in a new age of digital information, with networked access challenging higher education's ability to protect its assets, ensure the confidentiality of its data, respect the privacy of its university citizens, protect intellectual property rights, and comply with federal and state legislation. This challenge is not an IT organization issue but a much larger issue that each institution must address for itself. For higher education institutions, this requires a new look at its values and policies for information technology security.

Before the advent of the commercial Internet, IT security policies targeted protecting university assets and the privacy of students, faculty, and staff. Today, however, institutions are subject to a host of legal and cultural issues that can most effectively be addressed through IT security policies first and, ultimately, through enforcement. Legally, institutions are subject to a great deal of legislation regarding electronic information. Since higher education is often in multiple lines of business, it is subject to legislation designed with other business sectors in mind. As a financial institution, it is subject to the Gramm-Leach-Bliley Act; as a health-care entity it is subject to HIPAA; as a producer and consumer of copyrighted materials, it is subject to copyright law, the Digital Millennium Copyright Act (DMCA), and the TEACH Act. As an Internet service provider subject to DMCA provisions, higher education now finds itself the target of the Recording Industry Association of America and the Motion Picture Association of America in the conflict regarding peer-to-peer sharing of copyrighted music and video files. All these legal and cultural changes require higher education to be responsible and responsive, with IT security policies that ensure legal compliance.

IT security policies provide behavioral guidance to faculty, staff, and students. This guidance is especially important to students who haven't previously been taught about copyright, privacy, and appropriate use of IT. One of the important goals of higher education's IT security policies is to educate and inform students about appropriate behavior in an electronic environment. Since the student population is constantly changing, this education must be continuous.

A real tension exists between academic freedom and the need for open, unfiltered access to information resources and IT security policies that may limit this access. In policies that reflect the institution's academic stance, however, these policies can have a positive impact on the ability of the academic community to access required resources. For example, denial-of-service attacks and infection by computer viruses and worms can be mitigated by strong and flexible IT security policies designed to protect access to computing resources for the institution at large. These policies can enhance user confidence that academic freedom is being respected while providing needed protection for university assets.

Another concern in higher education is ensuring the privacy of members of the university community. Since authentication best practices require that records are kept of access to information resources, students, faculty, and staff may fear that data is being collected about their activities. This concern can be mitigated by having clear IT security policies that outline what information can be collected and how it can be used.

The future for IT security policy is complex and challenging. Yet, with increasing federal and state legislation, the opportunity exists to develop policies that assist in legal compliance and also help higher education protect its resources and privacy. With increased legislation comes increased accountability. Policies that are not enforced may not meet the test of due diligence, and institutions will need to focus attention on awareness and monitoring activities. As technologies continue to improve, so does the sophistication of the software designed to exploit vulnerabilities. Institutions must ensure that their IT security policies and practices are constantly updated to meet this challenge.

## Key Questions to Ask

- What are the benefits of IT security policies to the institution?
- Who are the key stakeholders in IT security policies?
- How can broad input and engagement in setting policy be obtained?
- How can executive leadership be engaged in policy development and dissemination?
- Which policies make sense for the institution?
- What are peer institutions doing?
- What are the legal obligations of the institution?
- What awareness and informational efforts are appropriate?
- How can compliance be assured?
- How can effectiveness be measured?

## Where to Learn More

- EDUCAUSE Policy Initiatives, <http://www.educause.edu/policy/>.
- EDUCAUSE Policy Library Home Page, <http://www.educause.edu/icpl/policies.asp>.
- Indiana University Information Technology Policy Office, *Benefits Provided to the University*, <http://www.itpo.iu.edu/>.
- R. Kvavik et al., *Information Technology Security: Governance, Strategy, and Practice in Higher Education*, EDUCAUSE Center for Applied Research, Research Study, Volume 5, 2003.

## Endnotes

1. C. Stoll, *The Cuckoo's Egg: Tracking a Spy through the Maze of Computer Espionage* (Doubleday, 1989).

2. For example, see K. W. Arenson, "Princeton Pries into Web Site for Yale Applicants," *New York Times*, July 26, 2002 (abstract available at <http://query.nytimes.com/gst/abstract.html?res=F30613FB355C0C758EDDAE0894DA404482>; R. K. M. Haurwitz, "Hackers Steal Vital Data about UT Students, Staff," *Austin American Statesman*, March 6, 2003; and Michael Arnone, "Hacker Steals Personal Data on Foreign Students at U. of Kansas," *Chronicle of Higher Education*, January 24, 2003.

3. For a brief summary of the contents of a security policy, see ISO/IEC 17799:2000, p. 2.

4. K. D. Salomon, P. C. Cassat, and B. E. Thibeaus, *IT Security for Higher Education: A Legal Perspective*, (EDUCAUSE/Internet2 Computer and Network Security Task Force, funded by a grant from the National Science Foundation, 2003), pp. 3–4.

5. G. Hill, author conversation, July 9, 2003.

6. Indiana University Information Technology Policy Office, *Benefits Provided to the University*, <http://www.itpo.iu.edu/>.

7. M. A. McMilllan and T. D. Sitko, "Managing University Business Continuity," in *Organizing and Managing Information Resources on Your Campus*, Polley Ann McClure, ed., *EDUCAUSE Leadership Strategies*, Vol. 7 (San Fransisco: Jossey Bass, 2003), pp.113–127.

8. T. Mitrano, "Resolving Information Technology Policy Issues on the Networked Campus," in *Organizing and Managing Information Resources on Your Campus*, Polley Ann McClure, ed., *EDUCAUSE Leadership Strategies*, Vol. 7 (San Fransisco: Jossey Bass, 2003), pp.77–92.

9. R. Kvavik et al., *Information Technology Security: Governance, Strategy, and Practice in Higher Education*, EDUCAUSE Center for Applied Research, Research Study, Volume 5, 2003.

10. B. Albrecht and J. Caruso, "Information Technology Security at Indiana University," EDUCAUSE Center for Applied Research, Case Study 8, 2003, p. 8.

11. K. Wada, "IT Security on Campus: A Fragile Equilibrium," *Syllabus*, May 2003, p. 20.

12. Salomon, Cassat, and Thibeaus, op. cit.

13. Kvavik et al., op. cit., pp. 60–61.

14. "Formulation and Issuance of University Policies," Cornell University Policy Library—Policy 4.1, Volume 4: Governance/Legal (Cornell University, March 1993 [revised May 2002]), available at <http://www.univco.cornell.edu/policy/pop.html>.

15. Kvavik et al., op. cit., p. 72.

16. Ibid., p. 76.

17. Ibid., pp. 72–73

18. The EDUCAUSE Policy Program is described at <http://www.educause.edu/policy/about.asp>.

19. R. Johnson, T. Mitrano, and R. Vernon, "Meeting the Cybersecurity Challenge," in *Organizing and Managing Information Resources on Your Campus*, Polley Ann McClure, ed. (EDUCAUSE Leadership Strategies, Volume 7, 2003), pp. 93–111.

20. Kvavik et al., op. cit., p. 74.

## About the Author

*Judith Borreson Caruso (judy.caruso@doit.wisc.edu) is Director of Policy, Security, and Planning at the University of Wisconsin–Madison and Research Fellow at the EDUCAUSE Center for Applied Research.*