Information Technology Security at Indiana University

Bob Albrecht, Western Governors University and EDUCAUSE Center for Applied Research

Judith B. Caruso, University of Wisconsin–Madison and EDUCAUSE Center for Applied Research

ECAR Case Study 8, 2003
Information Technology Security at Indiana University

Preface

The EDUCAUSE Center for Applied Research (ECAR) produces research to promote effective decisions regarding the selection, development, deployment, management, socialization, and use of information technologies in higher education. ECAR research includes

- research bulletins—short summary analyses of key information technology (IT) issues;
- research studies—in-depth applied research on complex and consequential technologies and practices; and
- case studies—institution-specific reports designed to exemplify important themes, trends, and experiences in the management of IT investments and activities.

In its most recent research, ECAR has investigated the state of security practice in higher education and reported its findings in Information Technology Security: Governance, Strategy, and Practice in Higher Education. This research was conducted by a team of researchers from ECAR and from Cap Gemini Ernst & Young. It was undertaken in five phases, described below.

Literature Review

A review of the relevant literature helped us define the study's major elements and create a working set of hypotheses.

Consultation

Researchers consulted with higher education security and policy leaders to identify and validate the most interesting research questions and hypotheses for framing the construction of a quantitative survey instrument. Those consulted include Mark Bruhn of Indiana University, Ken Klingenstein of Internet2, Mark Luker and Rodney Peterson of EDUCAUSE, Dan Updegrove of The University of Texas at Austin, and Gordon Wishon of the University of Notre Dame. The resulting research framework formed the basis for creation of an online survey.

Online Survey

ECAR conducted an online survey of more than 1,600 colleges and universities to establish the current state of computer security practices in higher education. More than 400 colleges and universities responded to the survey.

© 2003 EDUCAUSE. Reproduction by permission only.
Telephone Interviews
Researchers conducted intensive telephone interviews with more than 30 IT and functional executives, managers, and security officers at more than 20 selected EDUCAUSE institutions.

Case Studies
Researchers conducted in-depth studies of institutions regarding the state of their security efforts. To adequately capture the depth and breadth of practice, ECAR researchers chose both public and private institutions that varied in size and mission.

We undertook the present case study to draw on the direct experience of those able to provide insights into policies, technologies, and practices that have worked well and those that haven’t. We assume readers of this case study will also read the primary study, which provides a general context for the individual case study findings.

ECAR wishes to thank the leadership of Indiana University for sharing their time, thoughts, insights, and records with us. In particular, ECAR thanks Mark Bruhn, chief IT security and policy officer and associate director of the IU Center on Applied Cybersecurity Research; Beth Cate, associate university counsel; Eric Cosens, information systems auditor; Tom Davis, university IT security officer; Michael Egolf, manager of enterprise systems administration; Merri Beth Lavagnino, deputy IT policy officer; Michael McRobbie, vice president for information technology, chief information officer, and vice president of research; and Clark Sorensen, senior assistant registrar and manager of information systems.

Introduction
Indiana University (IU) consists of eight campus locations (see Figure 1), the largest being Bloomington (IUB) and Indiana University–Purdue University Indianapolis (IUPUI). The university offers four-year programs, advanced degree programs (professional, master’s and master’s degree equivalents, and doctoral), and associate’s and certificate degree programs. For the fall semester of 2001–2002, IU’s all-campus enrollment was 93,975 graduate and undergraduate students. IU employs approximately 7,000 faculty and 11,000 appointed staff. Established in 1820 in Bloomington, Indiana, IU boasts 116 academic programs ranked in the nation’s top 20. Indiana University is governed by a board of trustees comprising five governor’s appointees, one student appointee, three trustees elected by alumni, and three additional officers appointed by the board.

Figure 1. Indiana University Campuses
Michael A. McRobbie, vice president for information technology, chief information officer, and vice president of research, heads the Office of the Vice President of Information Technology (OVPIT), which includes the central IT organization, University Information Technology Services (UITS), and several other offices (see Figure 2). UITS consists of four divisions:

- Teaching and Learning Information Technologies (TLIT) provides support services to faculty, students, staff, and computing support professionals on the IUPUI and IUB campuses. TLIT’s resources include student computing labs and the Knowledge Base FAQ database. A key mandate for the division is to partner with faculty in integrating technology into their teaching practices.
- Telecommunications is responsible for the development and evolution of IU’s voice, data, and video communications infrastructure and devices.
- University Information Systems (UIS) develops, implements, and manages the enterprise information systems that support IU’s core business processes (including student, financial, human resources,
procurement, facilities, research administration, instructional, library, and other systems). UIS also manages the computing infrastructure supporting these information systems.

- Research and Academic Computing (RAC) provides computing facilities, visualization facilities, support, and services for IU’s research community, including faculty researchers, clinicians, engineers, artists, and students.

In addition to UITS, two other offices central to this study report directly to McRobbie in his role as vice president for information technology:

- The Information Technology Policy Office (ITPO) coordinates policy development, review, and management for a wide array of IT issues.
- The Information Technology Security Office (ITSO), which is closely aligned with the ITPO, provides IT security leadership.

Indiana University has provided support for the Internet2 network for more than five years, beginning with IU’s Internet2 establishment of a connection to the very high performance Backbone Network Service (vBNS), funded in part by the National Science Foundation. IU also supports the Internet2 Abilene network through its Abilene Network Operations Center.

Central IT Security Organization/Authority

Six weeks after McRobbie arrived at IU in 1997, a security breach occurred that provided the impetus for IT security activities over the next few years. McRobbie first commissioned a review of IU information technology security by an external security company. With that report in hand, he asked several colleagues, led by Eugene Spafford, a faculty member at Purdue University, to do a peer review and recommend IT security improvements for IU. The results of this study indicated that, while there was adequate security surrounding administrative systems, significant changes were necessary to improve IT security overall, including improvements in organization and procedures. With the strong support of IU President Myles Brand, McRobbie met with the university deans, the president’s cabinet, and the board of trustees to explain the gravity of the situation and to present the reports and recommended actions. As a result, security became an institutional priority, and McRobbie received the authority to implement necessary changes.

Through briefings and discussions, the president and board of trustees have gained awareness of IT security issues and come to understand the risks to the institution of poor security. Each year, McRobbie reports to the board on the state of IU security in a closed executive session. After a security breach resulting in the release of personal information from the Office of the Bursar in early 2001, the board voted to quantify and strengthen the vice president of information technology and CIO’s responsibility with a resolution that stated, “the Trustees direct the Office of the Vice President for Information Technology and CIO to develop and implement policies necessary to minimize the possibility of unauthorized access to Indiana University’s information technology infrastructure regardless of the Indiana University office involved; and … the Trustees direct the Office of the Vice President for Information Technology and CIO to draw upon the experience and expertise and resources of other university offices (including the Office of Internal Audit), to assume leadership, responsibility, and control of responses to unauthorized access to Indiana University’s information technology infrastructure, unauthorized disclosure of elec-
Electronic information and computer security breaches regardless of the Indiana University office involved.”

McRobbie delegated these authorities to the ITPO, which served to strengthen the power of the ITPO and ITSO and allow them to more broadly influence and control university IT security. Furthermore, it put the university community on notice that Internal Audit, which reports to the board of trustees as well as to the vice president for administration, should be employed in the effort to strengthen IT security.

In addition to reporting to the board of trustees each year, McRobbie, along with Mark Bruhn, chief IT security and policy officer, and Tom Davis, the ITSO director, meets regularly with institutional committees and groups such as the regional campus CIOs (who report jointly to McRobbie and the campus chancellors), the School of Medicine technical staff, IT advisory committees, and deans and faculty. This effort has paid off in increased awareness and better security across the campuses. According to McRobbie, “The university community, by and large, is both receptive and supportive. Deans are eager to be involved, and faculty are becoming more and more engaged in security-related matters.”

This recent attention to security has directly impacted the campus business units and departments. Clark Sorensen, senior assistant registrar and manager of information systems, summarized: “Since McRobbie came on campus, the campus culture regarding security has changed. We more stringently ensure that people don’t get to data that they shouldn’t have. People at IU are taking security seriously.”

Recommendations from the Spafford task force included separation of policy development and security compliance and creation of offices for each. The ITPO and ITSO were established in 1998 in response to these recommendations. Currently, both of these offices report to Bruhn, who reports directly to McRobbie. Bruhn emphasized the importance of this reporting relationship to Indiana University: “Policy and security responsibilities reside in the vice president’s office and do not report to the IT department, which signals the importance of these efforts.”

The ITPO’s responsibilities include IT policy development dissemination and education, computer incident response, and the assignment and maintenance of centralized computer accounts. The ITSO, headed by university IT security officer Tom Davis, consists of seven staff directly engaged in security analysis, development, education, and guidance for IU’s information assets and IT environment.

Staffing and budgeting for the ITPO and ITSO have increased in recent years. Currently, these offices include approximately 22 staff who are directly involved in policy and security for all IU campuses. While the ITPO and ITSO support all the campuses, most of their staff are located on the Bloomington campus with the deputy IT policy officer, Merri Beth Lavagnino, and five other staff residing on the IUPUI campus.

The budget for the entire ITPO for the 2002–2003 fiscal year was approximately $2 million, with appropriations from both general funds and IT strategic plan funds. The ITSO portion of the budget for the same year was $868,400, with funds again coming from both general and IT strategic plan funds.

Over the past several years, McRobbie commissioned several iterations of an Expenditures Review Committee, tasked with analyzing IT organization and services, identifying areas that no longer benefit IU and can be reduced or cut, and identifying areas where additional funding is needed. The ITPO has been the beneficiary in the last few years of additional allocations of money.
IU Security Goals

In a speech at the Statewide IT Conference in August 2002, McRobbie outlined two security goals for IU:

◆ to ensure, as effectively as possible, the cybersecurity of the IT environment of all IU students, faculty, and staff; and
◆ to contribute to national security by providing leadership in improving the higher education sector’s cybersecurity.

This case study will focus primarily on Indiana University’s progress toward the goal of improving its internal security policies and practices.

Progress toward strengthening IU’s institutional security has been significant. Since first efforts were begun in 1997, the centralized IT staff dedicated to security has grown considerably. Other achievements include addressing security in the IT informational sessions at new-student orientation, monthly monitoring of all centrally supported servers, widespread education and training of campus IT staff, and planning and development of new-staff security orientation.

IU’s 1998 information technology strategic plan, “Architecture for the 21st Century,” received widespread support on campus. Plan items directly impacting UITS included

◆ upgrading applications’ technical environments: an enterprise system implementation team was formed to define standards, production-readiness criteria, and other requirements for new applications;
◆ defining an application information architecture;
◆ developing architecture charts of physical machine and software components;
◆ creating a support matrix that defines all system components and specifies who supports them; and
◆ developing preproduction checklist and recovery requirements.

This plan has been widely accepted and followed. Mike Egolf, manager of Enterprise Systems Administration, recalled that it “had new database systems, new applications, everything new. Unlike our previous plans, it had teeth—it had broad-based support and funding.” The OVPIT/UITS accomplishments report of 2000–2001 summarized accomplishments in implementing the plan and related activities. Some major security accomplishments included

◆ establishing the University Data Administration unit within the OVPIT/ITPO;
◆ completing the first phase of the global directory services (GDS) project;
◆ upgrading technologies to support security services, such as computer system vulnerabilities scanning, and making them available to the entire IU community; and
◆ collaborating with the Copyright Management Center at IUPUI and the university counsel on matters related to intellectual property and copyright.

In February 2003, IU made major progress on McRobbie’s second goal by establishing the first higher education Research and Education Network Information Sharing and Analysis Center, REN-ISAC. This achievement marked an important milestone for higher education and IU and directly supports IU’s desire to contribute to national security by providing leadership in improving higher education’s cybersecurity. In the announcement, Douglas Van Houweling, president and CEO of the University Corporation for Advanced Internet Development, said, “The REN-ISAC will help integrate higher education’s work in security into the broader national effort to strengthen critical infrastructure.” At the same time, to strengthen its academic presence in the area of security, IU created the Center for Applied Research of Cybersecurity.
Security Governance, Culture, and Awareness

Four committees currently advise IU’s four associate vice presidents, one for each of the four divisions: TLIT, Telecommunications, UIS, and RAC (Figure 3). In addition, a university IT committee (UITC) consisting of the chairs of the four advisory committees and other campus executives advises OVPIT and UITS. All policies proposed by the ITPO go through the appropriate advisory committee.

In addition to security governance at OVPIT/UITS, each IU campus has an IT organization headed by a CIO, and schools, colleges, and departments have IT support staff. The regional campus CIOs report jointly to their respective campus chancellor and to Michael McRobbie. Departmental staff responsible for providing IT security support in their units are identified as local support providers (LSPs). UITS’s local support provider services department provides expertise, training, and other support services for LSPs who, in turn, provide valuable input to the ITPO as it drafts security policies and sets direction. For instance, LSPs and others have been providing feedback to the ITPO on its recently developed IT-12 Policy on Security of University IT Resources. Through regular meetings and e-mail advisories, the ITPO keeps LSPs and campus CIOs aware of proposed security policies and directions.

Recent attention to security issues has increased appreciation of the importance of security throughout the IU campus cultures. Eric Cosens, information systems auditor, remarked on recent audits: “Over the last four and a half years we’ve developed an effective partnership with the ITPO/ITSO. The general culture at IU is moving in the direction of one where clients are receptive to security expectations.” Lavagnino, who recently joined IU, noted, “Security is working here. It is unusual today to start a new job and find that a good policy foundation already exists. I’m not cleaning up messes or starting anew. There is already a broad understanding of the issues here—both legal and practical aspects of security.”

The ITPO and ITSO leadership has been key to improving security awareness at IU. Through newsletters, e-mail, and their Web-based Knowledge Base online help, the ITPO and ITSO continually strive to ensure campus users are aware of good security practices. McRobbie believes, “Increasing awareness has to be continual. It must be top-down; bottom-up doesn’t work.” Work-
ing with the OVPIT Office of Communications and Planning, the ITPO and ITSO place news articles in university publications and student newspapers. The offices also create “how to” guides and bookmarks.

Two recent major educational/awareness projects concerned spam e-mail and media copyright. Documents including “What is the Digital Millennium Copyright Act?”6 can be found at the online help Web site, Knowledge Base.7 In addition to the Web-based information, IT security articles have appeared in the faculty and staff newspaper, IU Home Pages.8

The ITPO and ITSO also strive to improve student awareness of IT security and policy. Mark Bruhn noted, “Many students are not coming in with an awareness of IT security issues, and some don’t behave ethically as it relates to technology, such as sharing of music recordings. It is not something they are generally taught in K–12. So we’re trying to modify existing bad behavior.” During student orientation, a 50-minute presentation on IT, including security and policy, is given to incoming freshmen and transfers. Currently there is no test required for students to demonstrate their knowledge of good security practices, but it is likely coming.

Increasing security awareness among faculty and staff facilitates security discussions. According to Bruhn, “If you have to dictate some action in order to improve security of a particular system, it is easier if you’ve had a conversation with them ahead of time on security issues.”

Currently new faculty and staff use a security orientation Web-based “starter kit” (further described below under Institutional Security Practices and Procedures) that includes information on appropriate use of computing resources and activation of accounts. It is similar to brochures that provided this information in the past. This kit is part of the account management system and uses the global directory service.

In addition, once each semester, the ITPO presents general end-user information on security and policy for faculty and staff. This includes in addition to the regular IT training provided by the UITS IT training and education group. Regularly offered training includes topics such as spam e-mail, e-mail management, and copyright. These training courses are targeted for students, departmental secretaries, and LSPs. Also, the ITSO offers a program of classes for LSPs called EdCert (further described below).

The heightened attention to security on the IU campus has also enabled campus departments to improve their own security practices. For example, the Office of the Registrar, which runs 18 computer servers, was able to get additional campus funding to create a separate server room with key card entry in 2002. This server room contains software to support desktop applications, Oracle applications that interface with the PeopleSoft applications, and applications that supplement the PeopleSoft functionality. According to Sorensen, “Our applications are more secure today than a few years ago. We have also benefited from increased security directions, advice, and standardization on campus, such as the IU Web home page standards. In the Office of the Registrar we are doing vulnerability scanning weekly. We’re doing weekly reviews of our audit files.”

Policy Development

IT policy plays an important role in improving the security environment at IU. Bruhn emphasized the importance of policy: “Institutional values drive policy; policy dictates processes, procedures, and standards; and security implements those.”

The Information Technology Policy Office’s mission includes
- IT policy development, dissemination, and education;
- information usage and management policy development and education (in conjunction with data management committees);
- review and analysis of existing policies for continued applicability and effectiveness;
- interpretation of current policy related to specific issues, situations, and incidents;
- coordinating response to incidents of inappropriate use of information or IT; and
- interaction with computer security officers to develop and administer security education and awareness programs and to assist with investigation of computer security incidents.

Since 1998, the ITPO has guided IT policy development at IU. The ITPO typically drafts policies, usually in collaboration with the university counsel, human resources management, the faculty councils, or other offices or groups as needed. Campus IT professionals, faculty senate and other appropriate committees, and the campus university counsel then review the drafts. For simple policies such as appropriate use of university IT resources, the ITPO seeks little feedback, but for policies directly impacting how departments manage their IT resources, the ITPO designates a longer input and review period and seeks feedback from more groups and offices. This review can take as long as several years, although after an initial request-for-comment period of up to 18 months, the ITPO modifies the draft to address these comments and publishes the policy as “interim.” This lengthy time period to test the policy’s application in real-life situations allows for an additional period of review before it is finalized.

Bruhn described the process: “Policies go through extensive iterations in their creation and review. Policies that are labeled ‘interim,’ however, are enforced even though they have not yet been formally and fully adopted. They cover areas in which no clear policies previously existed, but where a clear statement is required because of questions or issues we or other university offices are handling.” The process recognizes the genuine need for policy and permits ample time for review without delaying action.

Approximately 20 policies are currently approved, interim, or out for comment. They include:

- Computer Users’ Privileges and Responsibilities
- Policy on Use of Indiana University Information Technology Resources (IT-01)
- Policy on Sanctions for Misuse or Abuse of Indiana University Technology Resources (IT-02)
- Policy on Eligibility to Use Indiana University Technology Resources (IT-03)
- Policy on Privacy of University Information Technology Resources (IT-07)
- Policy on Security of University IT Resources (IT-12)
- Policy on Network and Computer Accounts Administration (IT-18)
- Policy on Extending the Network (IT-19)
- Policy on Wireless Networking (IT-20)
- Policy on Use of Electronic Mail (IT-21)
- Policy on Use of E-Mail for Mass Communications (IT-22)

For example, one of the policies currently under review—IT-12, Policy on Security of University IT Resources—delineates departmental security responsibilities. It identifies what departments need in regard to appropriate security processes, change management, and training. It details what technicians need to do to keep their servers safe. It also clearly defines the ITPO’s role and outlines incident response processes.

Important to policy development at IU is the relationship between the efforts of the ITPO, the ITSO, university counsel, and the local support providers. There is much com-
communication between these offices. “Fortunately, the ITPO and ITSO are really good at explaining the technology in plain English for us ‘laypeople’ in the counsel’s office, so that we can better identify potential legal issues and discuss policy options,” explained Beth Cate, IU associate university counsel. Clark Sorensen, senior assistant registrar and information systems manager in the Office of the Registrar, emphasized, “I have as much input as I want into policies. I read them and send feedback.”

For federal and state regulation compliance, the ITPO works closely with the School of Medicine, the Sponsored Research Services Office, the university counsel, Internal Audit, and other campus departments. Additionally, some of the compliance efforts are appropriately distributed to the other campus units. For example, the Health Insurance Portability and Accountability Act (HIPAA) officer for IU resides in the School of Medicine at IUPUI and consults with other departments, but isn’t charged with helping those units. For Family Educational Rights and Privacy Act (FERPA) awareness and compliance, the Office of the Registrar leads the effort, and new staff who handle student information are made aware of FERPA requirements on their first day of employment.

**Institutional Security Practices and Procedures**

The efforts of the Information Technology Security Office (ITSO) are critical to the improvement of security practices at IU. The ITSO’s mission is “to provide proactive security analysis, development, education, and guidance related to IU’s information asset and information technology environment. The overall objective is a safe and secure atmosphere for teaching and learning, research, service, and the conduct of university business.” In addition to Director Tom Davis, the office currently includes six security staff: four at the Bloomington campus and two at the IUPUI campus. These staff include both technical security generalists and specialists and provide the following security services to all IU campuses:

- intrusion detection,
- risk assessment,
- scanning of network-connected computers for vulnerabilities,
- coordination of incident response,
- security information resources,
- awareness and training, and
- consulting.

Many see ongoing communication from the ITSO to the local support providers as imperative to improving security on campus. The ITSO uses e-mail announcements, newsletters, and other publications to inform the local support providers of virus alerts, important software patches, and other security information. “It’s a constant challenge to improve security at the university,” Cosens noted. “You must communicate best practices on a continuous basis to local support providers and others.”

An important part of the ITSO’s mission is training IT staff from the schools, colleges, and departments. Training available at no cost to IU staff includes classes in security fundamentals, UNIX security, and Windows security. In addition to stand-alone classes, the ITSO offers a certificate of completion to IU staff who have completed a series of classes. This program of classes, called Security EdCert, is specifically designed for LSPs who want to enhance their knowledge and understanding of IT security. The EdCert is free and open to all registered LSPs on all IU campuses. Spring 2003 classes included security fundamentals, Windows security (introduction, intermediate, and advanced), UNIX security (introduction, intermediate, and advanced), and security foundations.
Davis thinks these classes are critical for the ITSO in serving the campus well. He singled out the training for local support providers. “I personally teach the introductory class. These classes not only provide an opportunity to train the LSP staff, but they also provide an opportunity to open up communications between the ITSO and LSP staff. They help make our relationship collegial.”

While both the ITSO and the ITPO obtained institution-level authority for security in the May 2001 board of trustees resolution, demonstration of good security practices, in-depth expertise, and training are the primary means of improving security at IU institutions. As Davis noted, “We [the ITPO and ITSO] cannot be responsible for securing all IU systems. By developing guides such as our best practices documents and system administrator security training, we are helping our departmental administrators secure systems within their areas of responsibility.” Compliance with IU policy is also largely handled in this way, with the goal of eventual compliance institution-wide. Sorensen of the Office of the Registrar is pleased with this approach: “Our regular dialog [between the ITSO and LSPs] provides valuable information-sharing opportunities. I feel supported by the ITSO, not in competition with them. There is a good balance between centralization and decentralization.”

Security best practices listed on the ITSO Web site include:
- applying vendor-supplied fixes necessary to repair security vulnerabilities,
- scanning computers for security vulnerabilities using available technical tools,
- removing unneeded services and software,
- installing and maintaining antivirus software,
- encrypting sensitive data where possible, and
- following adequate procedures for user accounts and access.

In addition to the ITPO and ITSO’s campus training and awareness activities, some campus departments also provide information for their systems’ users. For instance, the Office of the Registrar provides brownbag informational sessions on computer and security-related issues for campus staff for whom the Office of the Registrar provides IT support. Sorensen sponsors these sessions. “Our goal with the brown-bag is to uncover [security and data access] problems early,” he explained. “We’re probably ahead of most departments at IU.”

**Enterprise Applications**

To improve security practices at IU, security leadership looked first to practices within the central IT organization, UITS. Many improvements were made or are under way in this organization’s security practices. One key area that UITS supports is IU’s enterprise applications.

University Information Systems staff develop, implement, and run university enterprise applications under the leadership of Norma Holland, UIS associate vice president. UIS Director Dennis Cromwell leads computer system operations and is responsible for infrastructure components, including mainframe systems, enterprise Oracle database systems, decision support/data warehouse, production services, and systems development life-cycle standards. Mike Egolf is responsible for enterprise system administration. The enterprise systems supported include approximately 100 non-mainframe machines, 50 to 60 percent of which are UNIX AIX. The remainder are Windows based. The Tivoli storage manager provides more than 18 terabytes of disk space. These machines are treated as a pool of resources, rather than each machine being attached to a single application, and backed-up production data is sent off site to a private firm in Indianapolis. Every 28 days, all servers are
scanned for security vulnerabilities. Currently, no intrusion-detection software is being used for these systems.

The physical security of data center operations is managed by two UITS facilities staff in consultation with the ITPO/ITSO staff. All staff must wear ID cards or badges at all times.

**Identification, Authorization, and Authentication**

Adequate security in the areas of identification, authorization, and authentication is very important to the ITSO. As mentioned earlier, a newly hired faculty or staff member uses a Web-based “starter kit” for setting up university accounts. This software routes new employees through a series of pages about appropriate use and requires them to acknowledge awareness of their responsibilities. When leaving IU, an employee drops off the account database when human resources staff record the departure. If a departing employee represents a suspected security risk, the department contacts the ITSO and the employee’s IT privileges are terminated at 5:00 p.m. on their last day.

Authorization for access to enterprise applications is controlled by Kerberos with an IP filter, by smart cards, or by challenge/response cards called Safeword, a Secure Computing Inc. software product. UITS policy dictates that access for the development test environment is the same as for its respective production environment. Additionally, data stewards and data managers control data access and are responsible for understanding and applying the legal and ethical restrictions associated with their particular functional area and assigning classifications to the data per university guidelines. Data stewards are director-level staff appointed to represent data subject areas and are responsible for access policy. Data managers are operational staff in the functional offices who receive and approve requests to access restricted data. Only data stewards and managers have the authority to review actual needs and grant access to campus users. The ITPO retains documentation for these approvals.

At the campus level, the committee of data stewards, chaired by a functional area staff member, consists of university data stewards each responsible for a data area. The committee is responsible for recommending policies and establishing procedures and guidelines for university-wide management of institutional data. In addition, the campus-level committee on institutional data, chaired by a functional director, is charged with establishing general policies governing access to institutional data, making the final determination on requesting access rights to institutional data, and reviewing regularly the performance of the university’s entire data administration effort.

For authentication, IU’s goal is for all systems to eventually use Kerberos as the password validation service. The Indiana University Central Authentication Service (IUCAS), based on Yale University’s service with extensive Indiana modifications, provides authentication of IU students, faculty, and staff. Application systems don’t interface directly with Kerberos or Safeword but instead use the IUCAS, which in turn operates with Kerberos and Safeword. The application owner and data steward can choose whether to use password tokens or Safeword. One use of Safeword is to protect access, as a second authentication factor, to most administrative system data on the mainframe.

The global directory services (GDS) project (see “Future Projects” below), currently under way to replace an outdated accounts management system, includes a central directory based on Lightweight Directory Access Protocol (LDAP), new authentication and authorization mechanisms,
address books, and identification of all stu-

dents, faculty, and staff. Based on Open 
LDAP from the University of Michigan, it is 
projected to be in production in June 2004. 
As part of the GDS project, the Web-based 
accounts management system project is ex-
pected to be in production in 2003. This 
system includes the employee “starter kit” 
and will contain “secrets” for each person. 
This project is discussed further in “Current 
Projects” below.

Server and Network Security
UITs’s telecommunications division is re-
sponsible for the development and evolu-
tion of the university’s data, video, and voice 
communication infrastructure and devices. 
This includes an estimated 50,000 to 60,000 
devices on IU Bloomington’s network, the 
residence hall network, off-campus connec-
tions, and the wireless network.

Currently, departmental hardware ad-
dresses are not registered on campus; only 
student computers in the halls of residence 
are. All systems with static IP addresses, 
however, are supposed to be in the Domain 
Name Server (DNS). Computers with Dy-
namic Host Configuration Protocol (DHCP) 
addresses are not specifically identified in the 
DNS, but the set of DHCP addresses they 
are assigned are defined in the DNS. All of 
these network devices are required to fol-
low campus security policies. Off-campus 
network access is available via a virtual pri-
ivate network (VPN) service.

On April 8, 2003, UITs announced the 
installation of more than 1,000 wireless ac-
cess points over the next few months, in 
addition to the existing 400 access points. 
Through the VPN, an IU computer user can 
establish a private encrypted connection to 
servers on campus. Bruhn noted in a press 
release13 that “The virtual private network 
is a key component in our layered security 
approach because it provides for authenti-
cation and secure communication for users 
connecting from off campus…. Having al-
ready deployed VPN to support off-net con-
nections, our network staff had a jump start 
on using it for this new wireless initiative.” 

IU’s network tools include flow-tools 
from The Ohio State University to monitor 
network traffic, and ISS-Internet Scanner, 
used for scanning devices for security prob-
lems. According to Davis, “As software vul-
nerabilities are discovered and as patches for 
those vulnerabilities are released, it becomes 
difficult to deploy those patches to all of the 
devices. These tools provide us a way to 
identify machines that have security issues. 
Vulnerability assessment scans, in particu-
lar, can be perceived as intrusive, so those 
to date have not been centrally enforced by 
our office. Instead, we offer a vulnerability 
scanning service and let the local support 
providers request the scans themselves.”

The LSPs access an IU-developed Web-
based application and enter the device they 
want scanned. After the relationship is veri-
fied between the LSP and the server for 
which the scan is being requested, the scan 
is released into the queue and the ISS net-
work scanner engines scan the device for 
vulnerabilities. The application then e-mails 
the LSP indicating that the scan is complete 
and where to find the results. The ITSU re-
views the results if the LSP asks for assistance, 
or under other specific circumstances such 
as a compromised machine. After the first 
scan of a server when the LSP–server rela-
tionship is verified, the LSP can schedule scans 
as needed. Currently, an open-source prod-
uct, NESSUS, is being reviewed for potential 
campus-wide vulnerability scanning.

LSPs are completely responsible for local 
system administration. Davis described his 
support for their work: “My job is to ensure 
that the system administrators have the re-
sources and the ability to protect IU’s infor-
mation systems. With about 120,000 faculty,
staff, and students, we cannot begin to be responsible for their systems. We have to help them do it.” At present only devices under UITS responsibility are required to be scanned for vulnerability every 28 days, but in the future scanning will be mandatory for all network-connected devices, per IT-12, Policy on Security of University IT Resources.

For virus protection, both Antigen and Norton AntiVirus are deployed. Students, faculty, and staff can buy CDs at the university bookstore that contain Microsoft products and the antivirus software. Also for sale is a security CD containing operating system patches, secure shell, and other security software. Other network safeguards include intrusion detection using open-source tools such as Snort.

Table 1 details the technologies IU has adopted centrally for its security efforts.

**Incident Response and Compliance**

IU has fallen victim to several attacks and security breaches in recent years. Shortly after McRobbie’s arrival in 1997, an unauthorized release of personal information about faculty researchers, including Social Security numbers, occurred. As recently as spring 2001, two significant incidents occurred, one in which a departmental server that housed a file of student names was found to have open FTP access, and another in which there was an intrusion into a Web server not appropriately patched by the department. These incidents reaffirmed the importance of good security practices on the IU campus.

Such incidents catalyzed improved security and incident response at IU. Merri Beth Lavagnino of the ITPO leads a formal incident response process. She and other ITPO and ITSO staff assist in responding to and investigating incidents related to misuse or abuse of IU information technology resources. Training of ITPO staff in incident response is done via various sources, including EDUCAUSE and SANS.

Incidents are reported via e-mail to it-incent@iu.edu, security@iu.edu, or abuse@iu.edu, and ITPO staff log them into a central incident response reporting system. When an incident occurs, a full-time incident response coordinator and security analyst, working for Lavagnino, handles the item and triages it. Most incidents are not reported by administrators of the impacted system but rather by other system administrators or someone outside the institution. After a compromise is suspected, ITPO staff identify the incident’s location and the system administrator, who is asked to respond immediately. If the appropriate system administrator doesn’t respond or can’t be found, the ITPO has the ability to isolate the machine from the network. “This is rare, though. Maybe 5 to 10 percent of the time we don’t have records identifying the appropriate system administrator,” noted Lavagnino. “And in those cases we do our best to find someone to unplug the machine from the network locally, often even calling the dean’s office of the affected department to ask them to help locate someone. But, if all else fails, we do disable the machine’s access to the network to protect other computers on our network,” Lavagnino explained. If the suspected compromised machine contains any personally identifiable data, a security engineer from ITSO is sent to the department to do forensic work and document what happened.

The ITPO and ITSO are generally not involved in the sanctions or punishment for inappropriate or illegal behavior by faculty, staff, or students. Rather, they collect the data and provide it to the appropriate office, usually the dean of students, human resources, or IU police. The staff may also act as a resource for those offices to explain the technologies involved and the investigation data gathered. The role of the ITPO/
Table 1. Technology Matrix

<table>
<thead>
<tr>
<th>Function</th>
<th>Product</th>
<th>Technologies</th>
<th>Vendor</th>
<th>Affected Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td>Legacy: distributed accounts generation system (DAGS)</td>
<td>Sybase and Sybperl, Web pages</td>
<td>In-house</td>
<td>University systems campus systems, some departmental systems</td>
</tr>
<tr>
<td></td>
<td>New: global directory service (GDS), accounts management system (AMS)</td>
<td>Open LDAP, PHP</td>
<td>UM (Open LDAP), in-house (AMS)</td>
<td>University systems, campus systems, some departmental systems</td>
</tr>
<tr>
<td>Authentication</td>
<td>Global directory service (GDS) IU-Central Authentication Service (IU-CAS)</td>
<td>YALE/CAS, Java</td>
<td>Yale (YALE/CAS), in-house (IU-CAS)</td>
<td>All university administrative systems</td>
</tr>
<tr>
<td></td>
<td>Password generator token</td>
<td>Safeword A/S, with various card styles</td>
<td>Secure Computing Inc.</td>
<td>University systems, some campus systems, some departmental systems, administrative systems</td>
</tr>
<tr>
<td></td>
<td>Passwords</td>
<td>Kerberos</td>
<td></td>
<td>University systems, campus systems, some departmental systems</td>
</tr>
<tr>
<td>PIN</td>
<td>Oracle</td>
<td>In-house</td>
<td></td>
<td>Student systems</td>
</tr>
<tr>
<td>Guest</td>
<td></td>
<td>Open LDAP</td>
<td>UM (Open LDAP), in-house</td>
<td></td>
</tr>
<tr>
<td>Authorization</td>
<td>Global directory service (GDS) IU-Central Authorization Service (IU-Authz)</td>
<td>Java, Open LDAP</td>
<td>In-house</td>
<td>All enterprise?</td>
</tr>
<tr>
<td>Scanning</td>
<td>Internet security scanner (network vulnerability scanning)</td>
<td>Internet Security Services; in-house application</td>
<td></td>
<td>Several scanning engines deployed behind a locally developed application system</td>
</tr>
<tr>
<td></td>
<td>System scanner (onboard vulnerability scanning)</td>
<td>Internet Security Services</td>
<td>Console is deployed and used by department technicians</td>
<td></td>
</tr>
<tr>
<td>Virus protection</td>
<td>Desktop antivirus software</td>
<td>Norton AntiVirus</td>
<td></td>
<td>Issued on CDs and from a Web site</td>
</tr>
<tr>
<td></td>
<td>E-mail server</td>
<td>Sybari Antigen</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network security</td>
<td>Firewalls</td>
<td>Netscreen</td>
<td></td>
<td>Being deployed for our two major data centers and for our perimeter connections</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intrusion detection</td>
<td>Snort; flow-tools</td>
<td>Open source with IU extensions</td>
<td></td>
</tr>
<tr>
<td>Training/reference</td>
<td>Classes</td>
<td>Classroom teaching</td>
<td>Series of security in-house education/certification courses</td>
<td></td>
</tr>
<tr>
<td></td>
<td>How-to guides</td>
<td></td>
<td>Set of how-to guides developed in-house, set of operating system security guides licensed from SANS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Guidance</td>
<td></td>
<td>Best practices documents for security and for protecting sensitive information</td>
<td></td>
</tr>
</tbody>
</table>
ITSO staff is usually one of discovery, not enforcement. Lavagnino is pleased with this: “I don’t have to discipline IU students, faculty, and staff. This responsibility is readily accepted by the appropriate judicial offices, which are set up to do this already for other kinds of infractions not involving technology.” Beth Cate, associate university counsel, agreed with Lavagnino: “The ITPO gets in touch with our office and the appropriate campus authorities as soon as possible when a problem arises, which gives us a much better chance of responding effectively.”

The ITPO and ITSO sometimes interact directly with the violating students, faculty, or staff. For minor abuses such as forwarding chain mail, the ITPO/ITSO informs the violator. If there is no immediate response, a second warning may be sent. Only when the violator fails to remedy the situation is the matter escalated to the enforcing office. Also, in the case of Digital Millennium Copyright Act (DMCA) notices, under certain circumstances the ITPO/ITSO blocks access to the device, as required by law. When ITPO/ITSO staff discover major policy violations or illegal activities, they immediately inform the enforcing authorities.

The relationship between the ITPO/ITSO and the campus police department is important to both organizations. As technology resources facilitate more and more illegal activities, the campus police department seeks advice from the ITPO/ITSO. Also, any reports of illegal activities that come to the ITPO/ITSO are directed to the campus police.

Incidents such as those described have resulted in greater awareness of security issues on campus. Cate noted, “Prior incidents here at IU, as well as incidents elsewhere that the IU community reads about in the papers, have certainly increased awareness of security issues. We hope, through educational efforts, to keep people aware, informed, and able to assist in keeping the university’s networks secure.”

Risk Assessment and Audit

IU’s Internal Audit office works closely with the ITPO and ITSO. “We have a strategic partnership with the ITPO office,” explained information systems auditor Eric Cosens. “While to protect our independence we do not actively participate in the development of security policies, we do express our opinions and give advice on risk. As we do departmental and functional audits, we typically include IT security as a significant component. The importance of our relationship with the ITPO and ITSO can’t be overstated.”

Internal Audit includes computer security in its risk assessment. Since the office reports to both the vice president for administration and the board of trustees, it has the authority to perform technical audits in IT. Cosens is both a certified NetWare engineer and a certified information systems auditor. Coupling staff expertise with institutional authority promotes the significance of IT security in the university.

When Internal Audit provides a system audit, IT security is typically one of the areas addressed. A five-year audit plan ranks systems to be audited on the basis of their risk, with high-risk systems being audited most frequently. Annually, at one of the regular bi-monthly meetings between Internal Audit and ITPO, the audit plan is reviewed. According to Cosens, “We try to audit those systems with the highest risk. Our risk assessment is based upon a number of factors, such as when the system was last audited, the probability of an adverse event occurrence, and the potential impact of an adverse event on the university. Then we rank systems as high, medium, or low risk.” When planning their audit schedule, Internal Audit also builds in time for new systems and general consulting and for high-profile items that may come up during the year.

During a system audit, Internal Audit compares a system’s management practices
against security best practices such as regular scanning for security vulnerabilities, other policies, and standards. Policy IT-12, for example, details system technician responsibilities, including performing regular vulnerability scanning. On the basis of recent audits, Cosens estimates that approximately 50 percent of the audited systems are being scanned regularly. Other things examined include timely application of system patches, authentication, password and account lockout settings, and other security controls and procedures. When an audit is completed, the findings and recommendations are discussed with the audit client and communicated to the audit client’s supervisor.

Current Projects

A network security review project, led jointly by the ITSO and UITS Telecommunications, started in fall 2002 and is scheduled for completion in fall 2003. The project team, called the network defense team, includes staff from the ITSO, telecommunications, IT user support, and the data center. It is charged with recommending and developing layers of network security, including host-based firewalls and other filtering techniques, router access control lists, data center firewalls, and perimeter firewalls. Clark Sorensen of the Office of the Registrar is pleased that this project is proceeding. “I’m glad to see the ITSO is looking at firewalls,” he said. “We need to look at firewall technologies for all the educational institutions in Indiana.” As part of this project, IU is implementing Netscreen firewalls for the two main data centers, one at IUB and one at IUPUI, and is evaluating larger Netscreen firewalls for perimeter protection.

Another project under way is reviewing potential elimination of support for Windows 95 and 98 in 2003. When Davis reviewed the proposed schedule with the local support providers, they expressed concern about the implementation date, so it was extended to the end of the calendar year 2003.

A third effort, the global directory services project, will provide the foundation for student, faculty, and staff identification, authentication, and authorization. Begun in 2001, this project is expected to be completed in July 2004 and aims to

- establish standards, procedures, and mechanisms for appropriate identification and authentication of IT resource users, including management of university account administration procedures, applications, processes, and authentication devices;
- develop and administer a comprehensive university online user information store (directory) with application program interfaces and associated access controls as required;
- establish procedures for address book services, including procedures for record suppression as required in consultation with data stewards and other data and functional area experts; and
- establish procedures for computer account generation, distribution, and management, in conjunction with technology support centers, service administrators, and functional area staff.

An integral part of the global directory services project is the creation of an institution-wide directory that uniquely identifies faculty, staff, and students. Its purposes are to

- consolidate information across disparate systems,
- offer controlled access to institutional data,
- reduce the risk of incorrect information being used for business processes,
- provide consistent and standard data for applications,
- provide a standard access mechanism for access to distributed data,
◆ support many security solutions,
◆ support single sign-on, and
◆ support lookup services such as the University Address Book.

Other current projects include replacing the incident tracking system, ITRACK, with the Open Source Request Tracker system this year and replacing Kerberos Version 4 with Kerberos Version 5.

**Challenges to IU’s Security Program**

IU’s security program is successful but faces several challenges to its continued progress.

**ITPO and ITSO Staffing Issues**

The ITPO and ITSO must continually recruit highly skilled staff and keep existing staff up to date on the latest techniques and technologies. “The ideal job candidate is someone already bringing technical and security skills and who has the important verbal and writing skills, but many times you have to hire someone with the excellent technical skills and then teach them the security-specific skills,” noted Bruhn. Existing ITPO and ITSO staff are trained primarily via SANS Institute classes but augment these sessions with books, journals, and conferences. Bruhn, Davis, and other security staff participate in national and international security organizations, including the Forum of Incident Response and Security Teams, EDUCAUSE Policy, and Infraguard (part of the Federal Bureau of Investigation).

**Tension Between Centralized and Decentralized Units**

Another challenge IU’s security program faces is the natural tension and synergy between centralized policy development and security and the decentralized units. Cate emphasized, however, that good communications can mitigate potential conflicts. “Tensions can arise because some units historically have operated their systems in a decentralized way, and generally favor as much autonomy as possible in the service of academic freedom, but their technological expertise and resources may vary and create substantial risks to the security of those systems,” she said. “The key in lessening this tension is good communication between the centralized IT offices and the units, which emphasizes the help that the central offices can provide the units in meeting their computing needs while ensuring an appropriate level of security for their systems, and that also educates the units about the risks involved with decentralization. In this way, the units may become less suspicious of some necessary degree of central authority.”

Sorensen agreed. “Indiana University has a tribal culture. Having a central organization [ITPO and ITSO] with lots of authority—while the power is in the units—doesn’t fit real well. Shadow systems in the departments and test servers impact the network, yet centrally little is known about them. I think they [ITPO and ITSO] do a terrific job in an impossible situation,” he explained when asked about the relationships between the central organizations and the decentralized IT.

**Culture of Constant Improvement**

Key to Indiana University’s success is its propensity for and interest in support and improvement of teaching and learning, research, and other university missions. While this is absolutely necessary for IU as one of the country’s top universities, it does challenge technicians and security staff to keep up with the latest technologies.
Lessons Learned

IU personnel think they know why their IT security program has been successful. Strongly supportive of their leadership, they have implemented security procedures and policies they believe provide the foundation for security now and into the future. Notably, lessons learned include the importance of effective leadership, policy, communication, training, awareness, and—although not mentioned—focused personnel.

Senior Leadership Is Imperative

McRobbie advised, “Get your president on your side. Get him to say security is important publicly.” When McRobbie came to IU in January 1997, he immediately established a good working relationship with then-president Myles Brand. President Brand became a strong advocate for UITS’s security efforts. This executive-level support has enabled IU to proceed more quickly in adopting good security practices than it could have without this support. Cosens concurred: “It all starts with the tone at the top. The CIO and campus administration here have made security a priority. The proper tone at the top makes what we do more effective. It is the foundation of the control structure; otherwise policies are seen as optional and not taken seriously. It has to become part of the institutional culture.”

Put Policy First, Security Second

Key to the IU implementation of policy and security is the distinction between policy development and security implementation. The IU culture includes a belief that procedures and standards spring from policy, and policy springs from institutional values and attitudes. So, a general policy is created to meet an institutional need, and security procedures and standards are developed in response to those policies. McRobbie advised, “Policy comes first, then security. You can get preoccupied with tactics and lose sight of the grand scheme. You need constant policy education. Put policies in place that make security possible.”

Lavagnino agreed: “You must have the foundation of policies built first. They must be easy to read, understand, and interpret. I refer to them every day.” This belief in the primacy of security policy is reflected in the implementation of interim policies, although the final approval may occur months later.

Enhance Security Practices with Training, Communication, and Support

The primary benefit of IU’s security program is improved security practices throughout IU. Communication with local support providers is an important part of the work done by the ITPO and ITSO. “With the regular communications from the ITSO, we [local support providers] are informed quickly of problems such as viruses and patches, resulting in better security on campus,” noted Sorensen.

Another strategy for improving security practices in the schools, colleges, and departments is education. For instance, the ITSO supplies free security-related training to local support providers. This training, supplemented by free consultation if desired, helps IT staff in the schools, colleges, and departments obtain needed expertise to improve their security efforts.

The emphasis on communication, training, and consultation has raised the awareness of security best practices among faculty and researchers. McRobbie noted, “The research climate is now such that people want to do the right thing. It is important to involve departments and researchers in the development and implementation of policies. If the approach is such that one respects
their autonomy and their research agenda through the process, they are more inclined to be supportive as one works to implement best practices within the university.”

Cate emphasized, “The more educated IU personnel are concerning security issues and the tools at hand, and ways to minimize risks, the better off we will be.”

Establish Good Relationships Among Campus Units

Through regular communication and joint projects, staff from Internal Audit, university counsel, campus police, and central security can greatly enhance campus security awareness and effort. Cosens explained, “The strategic partnership between Internal Audit and the ITPO/ITSO offices ties our security practices together.” This collaboration is important to IU throughout the entire security effort—from the time policies are drafted through to the time a breach occurs. By providing a consistent and unified approach, these offices all help ensure that IU is as secure as possible. IT security is built into IU’s legal and audit procedures, reinforcing the notion that security is neither an add-on nor the property of the security office alone.

Central IT Organization Should Take the Security Lead

Cosens believes the central IT organization must lead security initiatives. “It is important for central IT to take a leadership role,” he noted. “The stronger the leadership in IT the better. They set the culture at a technical level. Everything flows from the tone at the top.” The board of trustees also reinforced this through its May 2001 resolution that directed the vice president of information technology to “develop and implement policies necessary to minimize the possibility of unauthorized access to Indiana University’s information technology infrastructure regardless of the Indiana University office involved.”

Establishing Security Awareness on Campus Is a Continuous Activity

Security awareness campaigns should be ongoing and updated frequently. Since best practices in security are constantly evolving, education and training must be continuous in order to meet campus security needs. Through newsletters, e-mail, and their Web-based Knowledge Base online help, the ITPO and ITSO continuously ensure that campus users are aware of good security practices. Security information is also an important part of IU’s IT presentation at new-student orientations.

Good Policy and Security Practices Require Resources

Since the 1998 strategy plan was published, the number of UITS staff dedicated to policy and security has more than doubled. Although the ITPO and ITSO have 22 staff members, Bruhn commented, “We could do a lot more with more people. We’d like to be able to send staff physically to visit with the departments to brief them, discuss what they should be doing, and give them additional security consulting. As it is, we get them as much information as we can and only visit when there is a serious situation.”

Egolf acknowledged the difficulty of having adequate resources: “Security—dollars or not—it has to be done. You can’t compromise on that.” While the security effort necessarily rests on current resources, the IU leadership has precise plans for the use of additional resources as they become available.

Security Can’t Be an Afterthought

As systems are designed and developed, security must be a part of the effort. Egolf explained, “Security must be a job and sys-
Information Technology Security at Indiana University

ECAR Case Study 8, 2003

Policies Must Be Easy to Understand

Understanding that institutional policies often remain unread, whether on the shelf or on the Web, IU works to make them both accessible and readable. “Even though we have foundation policies, it’s very difficult for the person who doesn’t work with them every day to understand them,” remarked Lavagnino. “These folks call Mark [Bruhn] or me. We need to work on education and awareness. I’d love to spend more time in making policies more accessible—maybe have an ‘ask the policy guy.’” Bruhn agreed: “We need and want the formal policies to exist, but also we need another format that makes them easier to read, less formal, and more narrative.”

Interim Policies Provide Opportunity for Input

Like many other institutions, IU needed to adopt a process to put policies in place with all the necessary governance participation but without excessive delays. After the ITPO (along with other campus departments) drafts an IT security policy, it is designated “interim.” While the policy is in interim status, it is vetted throughout the university for feedback. During this time, it can be enforced, thereby providing real-life guidance to faculty and staff. Also, this time gives IU staff an opportunity to try out the policy in actual practice and recommend changes.

The Future of IT Security at IU

IU resists the temptation to just do more of what is now being done. It continues to improve and expand its policy efforts and looks forward to future efforts on its campuses. Both challenges and opportunities await.

Privacy Challenges

As more and more requests come to the university for information on individuals on IU campuses, more philosophical questions arise. Cate predicted, “This will continue to be a challenge. We obviously need to comply with the law, but we are concerned about the risks to individual privacy and the chilling of free speech and academic freedom. In some respects, increased access to electronic data about individuals is a function of post-September 11 legislation; in other cases, it reflects increased enforcement activity under the copyright laws.”

Citing a recent district court case, currently on appeal, in which the court ruled that the Recording Industry Association of America could obtain the names of individual Verizon subscribers with a subpoena rather than having to first file a “John Doe” lawsuit, Cate prophesied, “I think we will continue to see increasing numbers of requests, and we will have to continue to be vigilant about preserving privacy and speech rights as much as possible.”

Legislation

Cate also expects that state and federal legislative efforts involving network security and use will continue. She noted, for example, “We (IU) recently worked with an Indiana state legislator on a bill addressing unsolicited commercial e-mail, which campus users are increasingly experiencing.” This is but one example of the growing national
Tighter Controls

Tighter technical control of university systems seems inevitable, but this threatens the internal values of privacy and freedom. “It is likely that our systems are going to be less open to nefarious activities than previously,” predicted Cosens. “We want to be as open as we can for our educational mission, but higher education is tricky—a balancing act. It’s like walking a tightrope. I’d like to see more intelligent control technologies developed and exploited. Allowing for freedom while having adequate controls in place is the goal.” As universities ensure compliance with security and privacy legislation, they must also balance openness and needed access to data.

Continuing IT Security Education and Improvement of Best Practices

Cate emphasized the importance of continued communication and training with campus units. “Education on security and network use issues is a continual effort,” she stated. “We can’t just give a talk one day and declare ourselves done.” The involvement of IU’s local support providers is critical to establishing security best practices at IU. The ITSO plans to continue its educational efforts with the local support providers through its Security EdCert classes and other communication and educational efforts. As additional resources become available, the ITPO plans to increase communication and training in campus units.

Planning and Funding

“Planning, prioritization, and resource allocation for security will continue to be a challenge, given other demands for resources, such as implementation of a student enterprise resource planning [ERP] system,” theorized Egolf. Because security continues to be viewed as an infrastructure or background function, it will continue to struggle for awareness and funds. More visible projects, such as a new ERP system, are expected to continue to attract campus administrators’ attention. The struggle for greater resources may be the greatest single challenge for IT security.

National and International Initiatives

The establishment of the REN-ISAC and the Advanced Network Management Laboratory (ANML) in February 2003 provided an opportunity for IU to expand its security presence in higher education. Over the next few years, the ANML is expected to provide security research of academic value to IU. University leaders also envision that IU will continue to make cybersecurity a broader institutional priority.

Endnotes

1. The scope of the security study was based on ISO17799, including system access control, system development and maintenance, compliance, personnel security, security organization, computer and operations management, asset classification and control, and security policy and its deployment, and excluding business continuity planning or disaster recovery and physical security.

2. While this survey was not randomized or stratified, creating the risk of both survey and respondent bias, it was universal for research universities and oversampled both M.A. and B.A. Carnegie institutions. The data reflect very closely the general EDUCAUSE membership, including the relatively smaller participation of A.A. institutions.


7. See <http://kb.indiana.edu/>. The UITS Support Center has been providing IT assistance for many years. It has created, over the years, numerous online "knowledge bases." A new iteration of the Knowledge Base code, KB3, was written by UITS staff and went into production on July 22, 2002. Currently it provides answers to more than 8,000 questions about the software products and services being used today at IU. Knowledge Base has won numerous national and international awards.
11. Ibid.