

## 1

# Executive Summary

**P**roviding sound information technology (IT) security at colleges and universities is essential to protecting information assets, safeguarding the integrity of institutional processes, and ensuring compliance with state and federal regulations. One challenging characteristic of higher education is a culture that values relatively unfettered and timely access to information and the free and continuous scholarly exchange of ideas. This culture requires that a secure environment carefully balance the extremes of leaving institutional and faculty information assets unprotected in a misplaced spirit of academic *laissez faire*, and choking off critical pathways of scholarly exchange by controlling access to these assets too tightly.

The advent of the World Wide Web in 1993 and its commercialization and globalization in the mid-1990s heightened the importance of protecting institutional infrastructure and intellectual assets. Recent legislation such as the Health Insurance Portability and Accountability Act (HIPAA), the Digital Millennium Copyright Act, and the Gramm-Leach-Bliley Act has imposed additional security requirements on higher education. Successful security efforts require not only increased investments in technologies, policies, software, and personnel but

also the time and attention of all students, faculty, and staff.

Despite this heightened attention, very little is known about the current state and future plans of IT security at colleges and universities. This study was undertaken, then, to investigate the state of IT security practices and investments in higher education and to compare and contrast the practices and investments, where possible, with those in other industries.

For this study, information security is defined as

- ◆ preserving confidentiality;
- ◆ protecting information from unauthorized use or disclosure;
- ◆ assuring information's integrity, including the accuracy and completeness of the data, through protection from unauthorized, unanticipated, and unintentional modification; and
- ◆ making data available to authorized users on a timely basis.

Using the ISO/IEC 17799 framework for security standards as a guide, we designed this study to provide an analytical baseline of higher education's security environment. This study identifies what security policies, tools, and procedures are currently in place and thus raises important policy and op-

erational questions that can constitute the basis for deeper analysis and research. With this study, institutions can begin to compare their investments and practices with those of similar institutions. This study also—within limits—lets us tentatively compare higher education’s practices with those in other industries, again suggesting areas for deeper inquiry and possible action.

## Methodology and Study Participants

This study consisted of five data collection and analytical initiatives:

- ◆ a literature review to identify and clarify the study’s major elements and create a working set of hypotheses to be tested;
- ◆ consultation with a select group of IT security leaders in higher education to identify and validate the most interesting research questions and hypotheses that would frame the quantitative survey instrument;
- ◆ a quantitative survey of 435 higher education institutions;
- ◆ qualitative telephone interviews with 42 technology executives, managers, and faculty members at 18 institutions; and
- ◆ four in-depth case studies including institution studies of the Massachusetts Institute of Technology, the University of Indiana, and the University of Washington, and a study of the management procedures for press-reported security incidents at the Georgia Institute of Technology, the University of Montana, and The University of Texas at Austin.

The participants in the quantitative Web-based survey consisted of 414 U.S. and 21 Canadian institutions of which 57 percent are public. With a survey response rate of 30 percent from EDUCAUSE institutions, the responding schools mirror closely the EDUCAUSE membership by Carnegie class.

In our data analysis we looked for factors that proved to be significant differentiators in IT security. Size of institution, whether measured by number of students, network users, or devices proved to be a significant variable, while Carnegie class did not. The survey respondents consisted largely of CIOs (42 percent), chief IT security officers (12 percent), and other IT staff (39.5 percent). Nearly one-half of the respondents (46 percent) had more than 10 years of experience with IT security.

## Key Findings

Several IT security taxonomies guide our findings. The first looks at institutions in two dimensions: security technologies in use and the security culture—leadership, organization, values, and rules. Institutional investments in these areas result from

- ◆ perceptions about the risks facing the institution—internal, external, or both;
- ◆ the institution’s propensity to take or accept risks;
- ◆ the resources an institution has to deploy, both financial and human; and
- ◆ the institution’s priorities and culture reflecting where it feels it can effectively make changes.

## Firewalls

Firewalls are a key technology in higher education. Of all technologies employed by survey respondents, firewalls were the most commonly used (87 percent), and another 10 percent are currently installing them. Carnegie class was a significant differentiator regarding perimeter firewall implementation. Eighty-three percent of the baccalaureate institutions have installed perimeter firewalls, while only 40 percent of the doctoral-extensive institutions have installed them. Terry Gray of the University of Washington explained why large institutions avoid perimeter firewalls: “Border

firewalls have some long-term negative consequences, such as encouraging people to tunnel all manner of applications through ports that are rarely blocked by firewalls. Instead, push security perimeters and policy definition as close to the organizations and computers to be protected as possible, and make sure all sensitive traffic is encrypted. This serves the reality of the large institution. A one-size-fits-all strategy is problematic for the research university.”

But disagreement exists even among large institutions. Paul Howell, information systems security officer at the University of Michigan, stated, “If you can install [perimeter firewalls] and operate them correctly, they tend to be the key thing to go after because they tend to keep undesirable traffic from the Internet [from] washing up on your machines. [Such traffic] can cause a lot of headaches.”

### SSL Technology

The most significant difference in technology use among large versus small institutions was in the adoption of Secure Sockets Layer (SSL) for Web transactions. SSL, a commonly used protocol for securing Internet data exchange, is an integral part of most Web browsers and uses a public- and private-key encryption system, including the use of a digital certificate. More than 86 percent of large institutions employed SSL compared with just 66 percent of small institutions. Also, SSL was heavily used by all doctoral institutions.

### Security Technology Use in Higher Education Versus Industry

In general, higher education employs security technologies less often than industry. For example, the 2003 CSI/FBI Computer Crime and Security Survey<sup>1</sup> found that 98 percent of industry respondents had

installed firewalls, versus 87 percent in our higher education survey. In addition, 73 percent of the CSI/FBI respondents use intrusion detection tools, versus 43 percent of our survey respondents. The greatest contrast between industry and higher education technology security is in electronic signature use, with usage of 56 percent reported by industry in a survey conducted by Top Layer Networks<sup>2</sup> and just 7 percent reported in our survey. These findings need to be viewed cautiously, as they reflect results obtained from different surveys administered at different times, but they do suggest further study and discussion.

### Wireless Security

Large institutions and doctoral institutions differ from master’s, baccalaureate, associate’s, and, to some degree, Canadian institutions in the use of strategies to secure wireless network access. For example, the latter four institution types more often used 128-bit wired equivalency privacy (WEP), extensible authentication protocol (EAP), and firewalls, whereas large and doctoral institutions more often used Internet Protocol virtual private network (IP VPN), Kerberos, and remote authentication dial-in user service (RADIUS). Little difference exists between public and private institutions. Overall, the most commonly used wireless security technology was firewall technology, with more than 57 percent of institutions reporting its use.

### Authentication

All institutions responding to the survey reported using some form of authentication. In addition, 24 percent of the institutions use two forms of authentication, and 50 percent use three or more forms. The form of authentication used—multiple-use passwords, multilevel passwords, password/PIN combinations, Kerberos, and the like—

varies depending on the perceived sensitivity of the data being protected at the institution. Nineteen percent of the survey respondents had implemented a single-sign-on system, another 19 percent were currently implementing one, and 48 percent said they plan to implement such a system in the next two years.

### **Biometrics**

Biometric authentication technologies are virtually nonexistent in higher education. When comparing biometric technology use between our higher education survey respondents and respondents to three industry surveys, we found a significant difference in adoption. In the 2003 CSI/FBI Computer Crime and Security Survey, 11 percent of the industry respondents had installed biometric tools. In our study, only 1 percent of the higher education institutions reported using biometric technologies.

### **Antivirus Protection**

Ninety-seven percent of the surveyed institutions have installed antivirus protection on their operating systems, 90 percent on their application servers, 92 percent on their e-mail servers, and 88 percent on other servers. These figures compare favorably with industry respondents' 99 percent reported use of antivirus software in the 2003 CSI/FBI Computer Crime and Security Survey. Many higher education institutions (68 percent) said they require that all institutionally owned systems have antivirus protection installed to connect to the network, but only 36 percent required it of noninstitutionally owned systems. This requirement was weakest at large and doctoral institutions. This may be explained by the diversity of systems prevalent at those institutions, where nonmainstream desktop systems may not have readily available antivirus solutions at competitive prices.

### **Security Management**

According to our respondents, day-to-day IT security management is the responsibility of central IT organizations (96 percent), and directors of networking are most often in charge (31 percent), followed by chief IT security officers (29 percent) and CIOs (7 percent). The position of chief IT security officer has been created largely since 1994; more than 22 percent of the institutions report having this position. Reasons for creating the position, however, vary among the institutions and include

- ◆ an enterprise resource planning system implementation at Yale University;
- ◆ government and regulatory issues at South Dakota State University;
- ◆ new technology leadership at Notre Dame University; and
- ◆ for the Maricopa Community Colleges, the September 11 disaster.

Most often these chief IT security officers report to the CIO (51 percent) or another vice president (13 percent). According to survey respondents, 54 (12 percent) of their IT security managers have formal IT security certification such as a Certified Information Systems Security Professional (CISSP) certificate or a Global Information Assurance Certificate (GIAC). Martin Fraser, professor and chair of the computer science department at Georgia State University, commented on the significance of certification: "From the faculty perspective, certification does help—it lends credence and authority that can get the attention of academic units better. [It is] training that is acknowledged."

### **Security Staffing**

In the recent EDUCAUSE Core Data Service survey, institutions reported on the size of their IT security staff. Doctoral institutions employ the largest security staff, with an average of 2.5 full-time staff; baccalaureate institutions average only 0.37

full-time staff. The number of full-time staff, however, is more closely linked to the number of devices on the network than to Carnegie class. As the number of network devices increases, the number of full-time staff increases, especially as the number of devices exceeds 10,000.

The existence and size of a dedicated security staff proved a significant factor when we analyzed how many survey respondents viewed their security programs as successful. Respondents employing full-time security staff viewed their security programs as more successful than those who did not have full-time security staff.

As would be expected, the organization of staffing for IT security varies greatly from campus to campus. The majority (57 percent) report that security staffing is spread across multiple functions, 22 percent report having a single dedicated staff member, and 11 percent report having more than one dedicated staff member. The tug between centralization and decentralization of security staff is common in large decentralized campuses.

### **Security Policies**

Two hundred and thirty-five of the institutions surveyed (54 percent) indicated that they have formal institutional policies covering IT security. Of these, 19 percent also had interim policies or policies in progress. Ninety-nine percent of the institutions had implemented policies regarding appropriate use of institutional assets, whereas only 39 percent had security policies covering application development. The number of policies, their scope, and the policy development and enforcement processes are unique to each institution, with some institutions viewing policies as critical and others intentionally limiting the number of institution-level policies. All respondents, however, agreed on the importance of policies that are easy to

read, accessible, enforced, comprehensive in scope, regularly updated, and consistent across the institution. Mark Bruhn, chief IT security and policy officer at Indiana University, emphasized, "We need and want the formal policies to exist, but we also need another format that makes them easier to read, less formal, and more narrative."

### **Policy Development Leadership**

The policy development literature encourages the active engagement of senior management, not simply executive support or endorsement. According to James Wright, president of Dartmouth College, "It is vital that decisions on policies and practices regarding security and related issues be carefully vetted, understood, and authorized by both the highest levels of the campus leadership and the representatives of the campus community." Michael McRobbie, vice president of information technology and CIO of Indiana University, advised, "Get your president on your side. Get him to say security is important publicly." The ECAR survey indicated that most institutions include the IT organization, the CIO, and a campus or faculty task force in IT security policy development. Policy development was least likely to involve state agencies, boards of trustees, and presidents.

### **Security as Institutional Priority**

We asked if IT security was one of the top three IT issues confronting higher education institutions today. Seventy-five percent of respondents agreed or strongly agreed, while only 10 percent disagreed or strongly disagreed. The respondents who strongly agreed were most likely to come from large doctoral institutions. When asked if IT security was a priority at their institutions, however, only 61 percent agreed or strongly

agreed. The gap between security as a top issue confronting the institutions (75 percent) and security as a priority (61 percent) raises some concerns. As with other risk-management activities, most people view IT security as a behind-the-scenes activity, and institutional leaders often attend to it only when a costly or embarrassing breach occurs.

### **Security Awareness**

Surprisingly, only 33 percent of the institutions in our study had a formal security awareness program for students and faculty. A formal awareness program for staff was only slightly higher, at 39 percent for all institutions. Doctoral institutions were more likely to have awareness programs than other institutions. Some institutions include security awareness education as part of their student orientation. These percentages are disappointing, as this is one area where an increased expenditure and effort could have an enormous payback to the institution.

### **Resources**

Obtaining adequate financial and human resources for IT security is a challenge for higher education institutions. When queried about the percentage of the total IT budget spent on security, 50 percent of the respondents reported that the budget for security represented 1 to 5 percent of the total central IT budget. When asked whether these resources were adequate, 44 percent disagreed or strongly disagreed. The reported security spending by higher education in our study is significantly less proportionately than that reported by government, banking, telecommunications, and other industries. According to *Information Week's* 2002 Global Information Security Survey,<sup>3</sup> fielded by PricewaterhouseCoopers, respondents spent on average 12.4 percent of their overall IT budget on IT security.

### **Security Planning**

Comprehensive IT security plans exist in almost 13 percent of the higher education institutions responding to our survey. Another 78 percent report that they either have a partial plan in place or are currently developing a plan. Small institutions are less likely than large institutions to have an IT security plan. Institutions with dedicated security staff are more likely to have a plan than those without dedicated staff.

### **Risk Assessment and Audit**

Risk assessments help institutions evaluate the potential harm to their business should a security failure cause a loss of confidentiality, integrity, or information availability. Yet only 30 percent of higher education institutions responding to the survey have conducted such an assessment. Also, when asked about regular audits of enterprise systems and router configurations, 46 percent of the institutions reported that they audited on an irregular basis or not at all. These numbers appear to be low, indicating a need for both deeper research and greater attention to work in this security area.

### **Security Exposure Practices**

All computers connected to a campus network present potential security exposures to the institution. This is an area where most institutions have good practices in place. In our study, 62 percent of institutions agreed or strongly agreed that they required all campus-owned computers connected to the network to have known security holes fixed. Fifty-nine percent agreed or strongly agreed that their institutions conduct regular and frequent scans to detect known security exposures in critical systems, but only 40 percent agreed or strongly agreed that their institutions conduct regular and frequent scans to detect known security exposures

in all campus-owned computers connected to the network. Clearly, exposure can be greatly reduced if computers connected to the campus network are regularly scanned for known security exposures.

### **Monitoring Networks, Operating and Enterprise Systems, and Routers**

Most institutions surveyed (55 to 68 percent) monitor their networks, operating systems, and enterprise systems daily. Larger institutions and doctoral institutions are more likely to monitor on a daily basis. According to the University of Washington's Terry Gray, proactive vulnerability probing is one of the most important tools available to secure a population of computers. It is not a one-time activity but requires an ongoing and recurring effort. Regularly monitoring institutional networks for abnormal activity helps institutions identify incoming attacks, locate and isolate machines with known vulnerabilities, or react to security breaches in process.

### **Incident-Response Procedures**

Respondents were asked if they had a formal IT security incident-response procedure. Forty-five percent did, with public and doctoral institutions and those with more than 25,000 students enrolled most likely to have these procedures in place. As enrollments increase, so does the likelihood that an institution will have a formal incident-response policy. Those institutions with formal incident-response procedures can respond to an incident quickly, ensure that damage is assessed, and effectively manage internal and external public relations. William Paraska, director of university computing and communications at Georgia State University, emphasized, "You have got to have a plan—you have to know what's out there, what's going to happen to you,

and how you're going to deal with it. Some schools are out there floundering—without an overall approach [to IT security]."

### **Incidents**

Only 19 percent of our survey respondents reported that they had had an IT security incident that had been reported to the press. Larger institutions and doctoral institutions were more likely than other institutions to have had an incident reported in the press. Of the 19 institutions with enrollments of more than 25,000, 58 percent had an incident reported in the press. As the number of devices and users increases, the percentage of institutions with security incidents reported in the press increases dramatically.

### **Impact of Residence Halls**

Residence halls connected to the campus network are often cited as a potential risk area. Of the institutions surveyed, 76 percent had residence halls. These institutions were more likely to have policies in place to shut off Internet access (89 percent versus 68 percent) and formal incident handling procedures (48 percent versus 34 percent) than institutions without residence halls connected to the network. It appears that the added risk posed by residence halls raised IT security awareness in general, resulting in the adoption of good practices.

### **Successful Security Programs**

Respondents were asked several questions related to the perceived success of their IT security program. Overall, the respondents felt more secure today than they did two years ago but also felt that their IT security programs needed strengthening. Institutions, by and large, have not developed metrics for measuring their IT security programs' effectiveness. The individuals we interviewed had varying opinions about

what constituted success. Bruce Judd, associate vice president for university computing and telecommunications at San Jose State University, stated, "Success is measured by the number of problems we have." Dick Jacobson, IT security officer at the North Dakota State University System, reflected, "I think our program is effective, and the effectiveness has grown because of the formalized structure that we have put in place with the designated security officers on the campuses." Morrow Long, director for information security at Yale University, noted, "IT [security] is effective: over time we have been able to achieve quite a bit in terms of increasing security.... It is an incremental, evolutionary approach, year by year—but we have moved quite a bit in terms of where we've come."

Survey respondents who have IT security policies in place, dedicated IT staff, or security as part of their IT plan characterize their IT security program as successful and feel more secure today than they did two years ago. Also, at institutions where the president and provost are involved in policy development, the IT security program is viewed as more successful than at institutions where they are uninvolved. When IT security policies exist, the survey respondents reported feeling that the IT security program was successful.

### **IT Security Barriers**

Our respondents indicated that the absence of resources was by far the largest barrier (72 percent) to IT security. When comparing the IT security budget share against the evaluation of IT security program success we found that institutions that spent the largest percentage of their total IT budget on security were more likely to view their security program as successful. Yet a dichotomy exists between the perceived importance of IT security (75 percent considered IT security as one of the top three

institutional priorities) and the resources being made available (only 28 percent of institutions agreed or strongly agreed that their institutions were providing the necessary resources). Notre Dame's CIO Gordon Wishon stated, "Justifying investment in security is very difficult because it is a negative deliverable. You only know when you don't have security." San Jose State University's Bruce Judd noted how he obtained funding at his institution: "Because I have kept the president's cabinet as well as the academic senate budget committee apprised with quarterly reports on network security and security issues, now they recognize the importance of network security. They raised security funding up to the mission-critical [level], whereas before it was viewed as just an option." Other barriers to IT security that respondents identified included awareness (46 percent) and cultural reasons, such as academic freedom (32 percent) and culture of decentralization (30 percent).

### **IT Security and Internal Business Practices**

One challenge of having security policies and practices is determining when and how to grant exceptions to the stated policy. A majority (55 percent) of our survey respondents indicated that business requirements take precedence over IT security when the two conflict. Only 17 percent of the respondents disagreed or strongly disagreed with this approach. This confirms the anecdotal belief that functionality takes precedence over IT security when new systems are installed. Some institutions, however, have found an acceptable balance by weaving their IT security into their business practices. According to Yale University's Morrow Long, "In 1997 we built IT security into the new administrative system and into training.... HIPAA forced the medical school to increase information security awareness as well."

## IT Security: Not Just About Technology

Although using technology is necessary to achieve effective security, the human side often needs the greater attention. Fifty-two percent of the institutions in our survey agree or strongly agree that IT security problems inadvertently caused by authorized users are a significant concern. Despite this perception, nearly 66 percent of institutions reported having no formal awareness programs in place for students, faculty, or staff. Recommendations from higher education staff emphasize the importance of paying attention to user training and awareness. Notre Dame's Gordon Wishon recommended, "Commit resources not only to technology solutions, but to education and awareness—particularly education and awareness among students and faculty, and certainly staff too."

Andrew Conley, network security officer at South Dakota State University, advised, "You can put all the technology in place, but if you don't let the users know, a lot of times they can find ways around it or they may do 'bad' things unknowingly. User awareness is one of the areas that really needs to be addressed in the security realm." Larry Lidz, senior network security officer at the University of Chicago, recommended, "There are two main things—convince everyone that security is something they should be concerned about, and build up trust [among the user community]."

## Conclusion

This ECAR study of IT security in higher education portrays an industry that is struggling to secure a culturally open environment against the rising tide of threats posed both from within and without higher education. In the main, survey respondents consider

their institutions' information resources to be secure, but most insist on the need for more resources to remain "in the fight." The data strongly suggest that some investments and strategies work; investments in security experts and in a security organization are strongly associated with expressed feelings of security. On the other hand, lack of investment in efforts on the soft side of security, such as education and awareness programming, is highly associated with a reported sense of insecurity. It is clear that investments in the technologies of IT security are necessary. It is equally clear that these investments are insufficient.

IT security, in the end, comes down to people's behavior. Most of the dramatic IT security risks relate to attacks by viruses, worms, super-worms, and the like. Perhaps the greatest damage is reflected in the opportunity costs of shutdowns in the wake of denial-of-service attacks, and the most bone-chilling risk may be that of identity theft. Even so, most hazards facing higher education fall into the gray area of unintended mistakes made by colleagues within our institutional bounds.

## Endnotes

1. The Computer Crime and Security Survey is conducted by the Computer Security Institute with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad, <<http://www.gocsi.com/press/20030528.jhtml>>.
2. J. Surmacz, "Most Security Experts Fear Cyber Attacks," CSO Online, 27 Feb. 2003, <<http://www.csoonline.com/metrics/viewmetric.cfm?id=509>>.
3. Check Point, RSA, Symantec, and Secure Computing Magazine sponsored KPMG's 2002 Global Information Security Survey, <<http://www.kpmg.com/microsite/informationsecurity/issurvey.html>>. Telephone interviews were held with 641 senior managers responsible for information security worldwide.