

The Myth about IT Security

“Security Is the CIO’s Responsibility.”

Seeing an institution’s name in the headlines for a security breach may be among a CIO’s—and a president’s—worst nightmares. Whether the breached data involves social security numbers, credit card accounts, clinical records, or research, this is bad news. Federal agencies that provide research funding may lose confidence in data integrity, putting millions of dollars in grants at risk. Legislators may seek additional oversight. Beyond image, institutions face issues of liability and business continuity. Considering that colleges and universities manage some of the world’s largest networks and collections of computers, the risk and the importance of the issue should not be underestimated.¹

Information security cannot be the responsibility of only the CIO—or even a chief security officer (CSO). Part of the reason is its importance. Institutions rely on information for academic, research, and outreach programs and for support services. Information security ensures the availability, integrity, and confidentiality of information, services, networks, and computer systems. These systems and networks must be available on a timely basis. Their information must be protected from unauthorized use or disclosure as well as from unapproved, unanticipated, or unintentional modification.

Security incidents include inappropriate access, alteration of data, virus infiltrations, and denial-of-service attacks. Contrary to common belief, the greatest risks may be internal, rather than external. Incidents may be precipitated by disgruntled or dishonest employees. Hackers are found on campus as well as

off. Other incidents are due to unsecured systems resulting from unlocked computer rooms or from passwords posted on monitors. Even the lack of antivirus software on one student’s machine or a single inadvertent download of malicious code by a staff member can put the entire IT system at risk. Although the campus provides much of the IT infrastructure, a host of systems that are not managed by the CIO process or store private data: the campus meal-plan server, the housing server, the parking services server, the international student office server—all of which have been hit by hackers in publicized incidents.² It would be convenient if we could solve security problems by installing a piece of technology, but the truth is that security is as much an issue of people and process as it is technology.

Security problems are no longer rare. Over a thirteen-month period from February 2005 to March 2006, Privacy Rights Clearinghouse estimated that 53.5 million Americans had their personal information compromised; nearly half of the incidents reported involved higher education institutions.³ Half of the 489 colleges surveyed in the 2005 Campus Computing Project experienced network attacks in the previous year; nearly 20 percent of those represented major security breaches involving personal information that could leave people vulnerable to identity theft.⁴ Findings from the 2005 EDUCAUSE Center for Applied Research (ECAR) IT security survey reported that

The truth is that security is as much an issue of people and process as it is technology.

incidents involved system unavailability (34%), network unavailability (29%), compromise of information confidentiality (26%), damage to data (12%), and identity theft (8%).⁵

Security-related IT incidents involve direct costs for an institution. Simply notifying affected individuals of a security breach can cost \$300,000 to \$500,000.⁶ One study published in 2000 estimated that thirty known security-related IT incidents resulted in over \$1 million in

direct and indirect costs; more than 9,000 employee hours were diverted for incident investigation and resolution; and nearly 270,000 computer and network users were affected.⁷ But the true cost of information security breaches is not easy to quantify. Beyond repairing the problem, costs can include legal liability, loss of intellectual property or institutional assets, and delayed or compromised research.⁸

According to a 2003 ECAR study, just over half of the 435 institutions surveyed had official institutional policies covering IT security; only one-third had formal security awareness programs for students and faculty. Although IT security is recognized as a top issue by CIOs, institutions struggle to establish meaningful security policies. The result is that less than two-thirds of the survey respondents said that IT security was actually a priority at their colleges and universities.⁹

Making security an institutional priority faces cultural hurdles. Even though all may agree that security is important,

specific practices elicit differences of opinion. For example, IT staff may feel that a firewall is necessary, but faculty may see this restriction on access as an impediment to intellectual freedom. Logging user access is one method of tracking intruders; however, monitoring and recording user access may be considered a threat to privacy. Attempts to demand that faculty, staff, and students update software, change passwords regularly, or use antivirus software have been perceived as contrary to academic freedom.¹⁰

Technology is clearly important in information security. Networks, systems, and applications should be periodically scanned to check for vulnerabilities. Automatic password changes should be enforced, and computers should be protected with antivirus software and should be updated regularly with the latest operating system patches.¹¹ Authentication systems can place higher levels of security on more sensitive assets. Although the CIO can provide guidance on these types of technical issues, information security is not just the CIO's responsibility. An effective cybersecurity program requires the cooperation of senior executives, legal counsel, auditors, policy and public safety, faculty, staff, and students.

In addition, someone must be in charge. Is there a person on campus whose primary responsibility is information security? Does that person have the authority to manage and ensure compliance with policies? Finally, education is a critical component as well. Does the institution have an ongoing education and awareness program? Is communication effective? If policies are in place, are they easy to understand? Is there a method for communicating policies to faculty, staff, and students? Are the consequences for noncompliance clearly explained—and enforced?

In thinking about information security, the CIO and the executive team should ask themselves the following strategic questions:

1. *Do we treat security as a campus governance issue or as an IT governance issue?* Higher education faces a host of potential security vulnerabilities, ranging from unsecured wireless networks to student-owned equipment to incom-

plete security policies and unclear oversight. Because of the mission-critical nature of information security, responsibilities for information security go beyond IT. College and university boards are being encouraged to adopt information security principles, for example. Are roles and responsibilities clearly defined? Does authority accompany those roles? Are adequate resources available? Have senior managers established policies and controls? Are regular reports on information security made to institutional leaders? Does the executive team consider information security part of its responsibility, or has security been relegated to IT?

2. *Do we know which institutional assets need to be protected?* Not all information is equally important. Do senior leaders know what needs to be protected? Can they differentiate information needing high levels of security from that requiring lower levels? Has the institution considered physical assets, such as laptops and servers, along with the information stored on them? Are machine rooms locked? Is the institution safeguarding older formats? For example, is the information in file cabinets secured in locked drawers?

3. *Do all IT users consider that security is their responsibility?* It is easy to feel that information security is someone else's responsibility. However, a single breach can put the entire campus at risk. Everyone shares responsibility for information security. At James Madison University, for example, all users—students, staff, faculty, and administrators—must complete a tutorial/quiz to obtain or change a password. The security awareness program makes it clear that everyone, not just the IT organization, is involved. President Linwood Rose argues, "We must all become much more vigilant in the provision of secure systems, in intrusion detection, in rapid response, and especially in education."¹²

4. *How do we ensure academic values and institutional integrity without ensuring security?* Security is necessary for higher education to be able to manifest its core values. Has the campus engaged in discussions of academic values and

security concerns? The perspectives of faculty and IT staff are likely to differ. And the culture of autonomy and self-governance may make the adoption of uniform standards difficult. Is it possible to ensure privacy without security? Have campus constituents explored the risks of not adopting a deliberate security strategy? Has the institution found an appropriate balance among values, risk, and realistic safeguards?

Security is not just the CIO's problem; it is everyone's problem. And everyone is responsible for the solution.

Notes

1. Security Risk Assessment Working Group, EDUCAUSE/Internet2 Computer and Network Security Task Force, "Information Security Governance Assessment Tool for Higher Education," <<http://www.educause.edu/ir/library/pdf/SEC0421.pdf>>.
2. Joy R. Hughes and Jack Suess, "Presidents and Campus Cybersecurity," *EDUCAUSE Review*, vol. 40, no. 6 (November/December 2005): 118–19, <<http://www.educause.edu/er/erm05/erm05613.asp>>.
3. "A Chronology of Data Breaches Reported since the ChoicePoint Incident," <<http://www.privacyrights.org/ar/ChronDataBreaches.htm>>.
4. Andrea L. Foster, "Technology: Safeguarding Networks Is Priority No. 1," *Chronicle of Higher Education*, January 6, 2006.
5. Robert Kvavik, personal communication with author, January 2006.
6. Rodney Petersen, personal communication with author, December 2005.
7. Virginia Rezmierski et al., "Incident Cost and Analysis Modeling Project: I-Camp II," <<http://www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/archive/Report/ICAMP.shtml>>.
8. Diana Oblinger and Rodney Petersen, "Cyber-Security: It Takes a Community," *University Business*, April 2004, <<http://www.universitybusiness.com/page.cfm?p=517>>.
9. Robert B. Kvavik and John Voloudakis, "Information Technology Security: Governance, Strategy, and Practice in Higher Education," *EDUCAUSE Center for Applied Research (ECAR) Study*, vol. 5 (2003), <<http://www.educause.edu/LibraryDetailPage/666?ID=ERS0305>>.
10. Diana Oblinger, "IT Security and Academic Values," in Mark Luker and Rodney Petersen, eds., *Computer and Network Security in Higher Education*, vol. 8, EDUCAUSE Leadership Strategies Series (San Francisco: Jossey-Bass, 2003), <<http://www.educause.edu/ir/library/pdf/pub7008e.pdf>>.
11. Security Risk Assessment Working Group, "Information Security Governance Assessment Tool."
12. Linwood H. Rose, "Information Security: A Difficult Balance," *EDUCAUSE Review*, vol. 39, no. 5 (September/October 2004): 10, <<http://www.educause.edu/er/erm04/erm0456.asp>>.

Diana G. Oblinger is Vice President of EDUCAUSE, where she is responsible for the association's teaching and learning activities and for the EDUCAUSE Learning Initiative (ELI). Brian L. Hawkins is President of EDUCAUSE.