

## Presidents and Campus Cybersecurity

CIOs cringe when they hear about the latest security incident at some other college or university. They know that their colleagues at the other institution are being besieged by anxious students, parents, alumni, faculty, and staff—all of whom are angry that the institution has betrayed their trust by allowing access to private data. The CIOs know that the federal agencies that provide research dollars to the institution will be calling to find out if research data were at risk and may lose confidence in the institution's ability to protect that data. They know that if the college or university is a state institution, there is bound to be a resolution (or two) introduced in the state legislature to allow greater control of the institution's IT systems. They also know that the same security problem that led to the reputation-harming press coverage for the compromised institution exists on their own campuses. Even though their own campuses may not have suffered a major infiltration by a criminal or malicious hacker—yet—they know that the issue is not “if” but “when.” This knowledge keeps CIOs awake at night, planning strategies for convincing their campus administration that the threats are genuine, serious, and immediate and that much money, time, and culture change will be needed to prevent similar damage at their own institutions.

Most college and university presidents are confident that their major computer systems are secure. And indeed, most of the systems centrally managed *are* reasonably secure. However, the central staff needs both money and time to install and monitor an increasing array of expensive

detection and protection systems in order to keep them that way. In addition, at most institutions, many of the servers, desktops, and laptops that store private data are not under the control of the campus CIO. The data on these machines often come directly from the central administrative systems.

The campus meal plan server, the housing server, the parking services server, the campus police server, and the international students office server are examples of servers that store confidential data, that are not usually managed by central IT, and that have been hit by hackers in highly publicized incidents. Often, the people administering these servers wear many hats and do not have the time or the expertise to keep the servers secure. The hardware may be old and the operating systems too outdated to be made secure.

Higher education institutions expend enormous effort and money to secure central systems, but then they allow departments and individuals to download data from these systems and store the data on insecure servers, desktops, and laptops. When one of these machines is hit, it does not help for the CIO to say: “That machine doesn't come under my area of responsibility.” Such an excuse is not acceptable to the students or alumni whose data were violated. All they know is that the institution and its leadership failed to keep their data secure.

Presidents of colleges and universities are taking action in response to these threats. In an open letter to the campus community on April 4, 2005, Robert J. Birgeneau, the chancellor of the University of California–Berkeley, vowed that

UC-Berkeley would do all that it could to safeguard personal data stored on campus computers. He wrote: “As Chancellor of the Berkeley campus, I was stunned to learn of the theft of a laptop computer in the Graduate Division, which contained personal information for approximately 98,000 current and former graduate students as well as persons who applied to our graduate programs. Our students, staff and alumni expect us to protect the information they have given us confidentially, and we have not maintained that trust. This incident revealed serious gaps in our management of this kind of data. The campus has been instituting new policies to address these issues for several months, and we will do much more. Accountability for this effort ultimately lies with me.” Birgeneau promised to “engage one of the nation's leading data-security management firms to conduct an immediate external audit of how the campus handles all personal information. This firm will examine the security of the systems, the policies and practices regarding access and use of such information, and the policies for insuring that such data are gathered and/or retained only when imperative.” He also pledged to “move quickly to require the full encryption of all personal information stored on departmental computer systems.” He added: “We will also require all units on campus to review again personal data stored on departmental machines and to remove all unessential data.”<sup>1</sup>

Freeman A. Hrabowski III, the president of the University of Maryland–Baltimore County (UMBC), is passionate about auditing. A state audit in 2001 identified network security vulnerabilities.

Hrabowski seized the opportunity presented by major campus construction projects to authorize a major redesign of the university network around security. In 2002 the network was redesigned to include such security features as firewalls, intrusion prevention, and virtual network segmentation. These changes provide real-time protection against intrusions and ensure that traffic is segmented so that machines that should not be accepting network connections from the outside are protected from doing so. In 2001 Hrabowski also authorized the funding for a new ERP system that eliminated the



Illustration by Steve McCracken, © 2005

use of Social Security numbers as identifiers in payroll, and the university is now focused on eliminating Social Security numbers throughout the campus.

In November 2002 Alan Merten, the president of George Mason University, formed a Privacy and Security Compliance Team (PSCT), chaired by his chief of staff and composed of representatives from the major academic and administrative units. The PSCT developed a data-stewardship policy that holds unit heads accountable for securing confidential data. Merten also directed all unit heads to appoint a security liaison to work with the CIO on preventive measures. Like Hrabowski, Merten allocated resources to implement systems that enabled the university to stop using Social Security numbers as identifiers.

Presidents Hrabowski and Merten collaborated with their CIOs (the authors of this article) to produce a provocative video on the responsibility of college and

university presidents to ensure cybersecurity. The moderator of the discussion is Frank Sesno, a former senior vice president and Washington, D.C., bureau chief for CNN, who is now a member of the faculty at George Mason and continues to produce specials for CNN. In the video, Frank challenges presidents and CIOs to articulate what they have done to fulfill the trust their constituencies have placed in them, why their actions matter, and what more can be done. (To view and/or download the video, see <<http://www.educause.edu/LibraryDetailPage/666?ID=CSD4121>>.)<sup>2</sup>

In some states, laws and regulations have already been enacted that forbid the use of the Social Security number as a primary identifier, that require sensitive data to be encrypted, that call for certain network protections, and that set strict guidelines for when people must be notified about a security incursion. At the federal level, laws have been introduced, but not yet enacted, that would set much stricter and more expensive standards for customer notification in the event of an incident.

Institutional leadership, especially presidential leadership, is essential for campuses to navigate the changing legislative and regulatory landscape. In a time of flat or declining resources, college and university presidents must exert strong leadership to provide the additional funding, staffing, and changes needed to keep sensitive data secure.

#### Notes

1. "Chancellor's Message on Personal Data Security," <<http://1dalert.berkeley.edu/chancellorletter.html>>.
2. Additional security resources for higher education are available at the EDUCAUSE/Internet2 Computer and Network Security Task Force Web site: <<http://www.educause.edu/security>>.

**Joy R. Hughes is CIO and Vice President, Information Technology, at George Mason University. Jack Suess is Vice President of Information Technology at the University of Maryland, Baltimore County.**



# EDUCAUSE

## Transforming Education Through Information Technologies

EDUCAUSE, a consolidation in 1998 of Educom and CAUSE, is a nonprofit consortium of colleges, universities, and other organizations, dedicated to the transformation of higher education through the application of information technologies. Through direct services and cooperative efforts, EDUCAUSE assists its members and provides leadership for addressing critical issues about the role of information technology in higher education.

## EDUCAUSE Board of Directors

### Perry O. Hanson, Chair

CIO and Associate Provost for Educational Technology  
Brandeis University

### Kathleen Christoph, Vice Chair

Director, DoIT Academic Technology Solutions  
University of Wisconsin-Madison

### Robyn R. Render, Secretary

Vice President for Information Resources and CIO  
University of North Carolina, Office of the President

### John E. Bucher, Treasurer

Director of Information Technology  
Oberlin College

### John C. Hitt

President  
University of Central Florida

### Rebecca L. King

Director for Information Systems & Services  
Baylor University

### Jeffrey W. Noyes

CIO and Associate Vice President for Information Technology  
University of Texas at San Antonio

### Margaret F. Plympton

Vice President for Finance & Administration  
Lehigh University

### David L. Smallen

Vice President, Information Technology  
Hamilton College

### George O. Strawn

CIO  
National Science Foundation

### Ellen J. Waite-Franzen

Vice President, Information Services  
Brown University

### David Ward

President  
American Council on Education

### Ex Officio Member

**Brian L. Hawkins**  
President  
EDUCAUSE