

What Higher Ed Leaders Need to Know about IdM

Today's institutions of higher education are both empowered by and dependent on electronic information for academic and administrative communications and services. Since much of this information is tailored to the needs and roles of individuals, it is important to have a good means of identifying those who use and modify the information. If a college or university is not concerned about the proper identification of those who access its information assets, institution leaders need only read some of the recent press about unauthorized intrusions into the confidential data of other colleges and universities. Although in the past, hackers were often looking for unprotected resources such as servers for sharing music or video, today professional gangs of criminals are intent on stealing personal identification and financial information from institutional systems and selling that information to others worldwide for use in criminal schemes. To manage these increasing risks, every institution must have a solid environment in place to properly identify all users of its systems and to validate, on a case-by-case basis, the authority of those accessing each system.

Such an environment requires that three things be in place for adequate protection and trust:

- **Identification:** making sure that electronic credentials for access to a system are granted only to the right person
- **Authentication:** checking the validity of these credentials at the time of access
- **Authorization:** determining that the person so identified has been granted the authority to perform the requested actions

Since this approach must apply to all users of every sensitive system and application, both central and departmental, its implementation requires an organized, institution-wide approach, summed up in the term *identity management*, or IdM. The past implementations of user-names and passwords managed separately on each system have not and cannot meet the current challenge.

IdM is an issue that involves much more than the IT organization, since many others in the institution are involved—for example, in admitting and graduating students, hiring and terminating staff, and managing all of their roles and privileges. Effective IdM requires an integrated system of business processes, policies, and technologies that enable institutions to facilitate and control their users' access to online applications, as well as physical resources, while protecting confidential personal and business information from unauthorized users.

Numerous departments and units must be involved in the implementation of an institutional IdM environment. In many institutions, the technology is managed centrally (usually by the IT organization), but distributed authority and stewardship, as well as local decision-making, are retained by the departments involved. Policies must be instituted in advance to clearly state the roles and responsibilities of each player—from system manager to data steward to user—including who should do what in case of a break-in or a service failure. Awareness is critical. To maintain trust in the system and, indeed, the campus itself, key departments—such as the registrar, alumni association, human resources, and finance—must understand the importance of IdM.

Since IdM cuts across many departments and units, institutional sponsorship and commitment must come from the top. Boards and presidents need to understand this ownership issue and establish a governance committee to ensure that IdM is implemented and maintained throughout the institution. Schools and departments must implement campus policies and procedures to govern the use of their constituents' electronic identities and roles, as well as technologies to support that use.

Implementing IdM requires a high-level champion who views this issue as an institutional priority. A business case for IdM on campus needs to be made to upper administration (presidents, provosts, boards, associations, CFO, et al.). A wide range of stakeholders is involved, including the auditor and general counsel, the security officer, the controller, and risk management officers. Some institutions bring in an external consultant to explain this need. Preparing executive summaries to precede a full discussion can be helpful.

IdM policy must be considered in the context of other policy issues and must address privacy and institutional values. It should clarify and define roles, responsibilities, and accountability, and it should document guidelines and requirements. Compliance is an important factor, and institutions are increasingly being held accountable. IdM policy must be publicly documented with a feedback mechanism, approved, and communicated institution-wide.

Institutions must undertake risk assessment and risk management in order to evaluate the impact of public embarrassment, loss of trust and integrity, and financial loss. Not being adequately positioned with IdM infrastructure may



Illustration by Randy Lyhus, © 2007

also pose legal risks. Institutions have dealt severely with those in charge of securing sensitive data on campus when such data have been compromised.

Communication and training are both key to achieving success with any IdM implementation. Anecdotes of IdM victory and defeat at other institutions can be shared to good effect. Simple, ongoing messages, free of technical jargon, are best. This communication should be a shared responsibility integrated into established channels on campus. Legal counsel should be involved. Different audiences need customized messages that communicate the positive as well as the negative aspects of IdM. Campuses might consider including IdM training as a regular requirement for users.

Articles and presentations that forge tighter relationships between the campus functional offices and information technology are needed across the higher education community. An event with an EDUCAUSE partner association is being considered for late 2007 or 2008 that would bring together leaders from other campus areas to discuss how to move ahead with IdM implementations on their campuses. The sharing of best

practices, costs, tools, and experiences will be extremely beneficial.

Presidents, provosts, and boards need to understand the risks of not having a robust IdM system in place: bad public relations, public terminations, lawsuits, students who leave and do not return, alumni who refuse to continue to donate, and the high costs of being in a reactive mode. They need to make decisions based on solid data. If an institution does not have an IdM plan, there is little or no recourse when confidential data are compromised. A trusted environment in which the institution knows the identity and access authority for every user is excellent insurance. Lest this sound like scare tactics, another consideration is that the leading institutions in IdM also enjoy an environment that saves time, effort, and money in dealing with the omnipresent recurring failures of legacy user-name and password systems and one that enables ever more powerful applications that span beyond institutional systems to virtual communities sharing information, communications, and physical resources for the betterment of research and education.

Brian L. Hawkins is President of EDUCAUSE.

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

John E. Bucher, Chair

Director of Information Technology
Oberlin College

David L. Smallen, Vice Chair

Vice President, Information Technology
Hamilton College

Rebecca L. King, Secretary

Director for Information Systems & Services
Baylor University

Tracy M. Mitrano, Treasurer

Director of IT Policy and Computer Policy and Law Program
Cornell University

Jerry D. Campbell

President
Claremont School of Theology

John C. Hitt

President
University of Central Florida

Lucinda T. Lea

Vice President for Information Technology & CIO
Middle Tennessee State University

Marilyn A. McMillan

Associate Provost and Chief Information Technology Officer
New York University

Margaret F. Plympton

Vice President for Finance & Administration
Lehigh University

Kathleen C. Santora

Chief Executive Officer
National Association of College & University Attorneys (NACUA)

Scott E. Siddall

Assistant Provost for Instructional Resources & Director of Instructional Technology
Denison University

Ellen J. Waite-Franzen

Vice President for Information Technology
Dartmouth College

Ex Officio Member

Brian L. Hawkins

President
EDUCAUSE