

Key Findings

Identity Management in Higher Education, 2011

Mark C. Sheehan

Managers of IT systems have a strong interest in the identity of the individuals attempting to access those systems. To ensure their security, institutional resources require protection against intrusion, theft, and vandalism. The privacy of faculty, staff, and students is important as well, and personal information stored on institutional systems must be protected for the sake of its owners, for the sake of the institution's reputation, and to comply with governmental regulations.

These concerns are well known and are an essential part of the IT environment throughout higher education. Evidence that security and identity management (IdM) are on the minds of most IT administrators comes from the past decade's EDUCAUSE Current Issues surveys. In 2006, those concerns together were ranked as the most important IT issue to resolve for the institution's strategic success.¹ Subsequent Current Issues surveys separated "security" from "identity and access management." Security remained one of the top-three items between 2007 and 2010, and despite its separation from that key issue, identity and access management never fell below the middle third of the 10-item list (in 2010 it ranked fifth).²

To investigate IdM practices in higher education, ECAR conducted a baseline study in 2005.³ For our research purposes, we defined IdM as the policies, infrastructure, and practices related to establishing, maintaining, and using digital identities. We reprised our IdM study beginning in 2010 in order to examine both the progress that has been made and the challenges that remain in safeguarding the IT resources of the institution and the privacy of the individuals it serves.

We learned from our 2005 study that central IT organizations were struggling to deliver the benefits of IdM to their constituents. Nevertheless, it was clear that those benefits were considered important and that IT organizations were deeply involved in basic IdM activities. This study, based on our 2010 survey, looks at institutional readiness for IdM across several dimensions and evaluates their impact on IdM outcomes. The bulk of our work focused on a set of five core elements of IdM practices: authentication, reduced or single sign-on, enterprise directories, automated role- and privilege-based authorization, and federated identity. The last of these has taken on particular importance over the past five years as the evolution of cloud-based resources and services has expanded the definition of the institutional IT domain.

While we find that much progress has been made since 2005, delivering the benefits of IdM remains a challenge for the average institution. There is much that the institution can do to support IdM work, including executive engagement, funding, and attending to a host of IdM readiness activities such as infrastructure and policy provision, planning, documentation, and the use of a variety of IdM metrics. We measured success in terms of perceived return on investment and agreement that the institution delivers a carefully chosen set of 14 IdM benefits. Where institutions have invested in IdM and where

they have prepared for it more extensively, these measures of success are substantially stronger. IT leaders concerned about system security and user privacy may wish to follow the path laid out by these successful institutions.

Methodology

To reprise our 2005 study of IdM in higher education, we took a multipart approach that consisted of

- a literature review to define issues, examine IdM practices, and establish research questions;
- consultation with higher education IT administrators and IdM experts to identify and validate survey questions;
- a quantitative web-based survey of EDUCAUSE member institutions that received 323 responses, 55.8% of which were from the institutional CIO or equivalent;
- qualitative interviews with 52 higher education IT leaders and staff; and
- two case studies, one examining the evolution of IdM at Coppin State University and one chronicling the development of a federated identity solution at the University of North Carolina.

Our 2005 study involved 403 institutions surveyed in mid-2005. The current study involved 323 institutions surveyed in spring 2010. Note that in the discussion that follows, comparisons between the two survey populations involve only the 137 institutions that took part in both years' studies. We refer to these institutions as the "longitudinal sample."

Key Findings

Considered in overview, higher education has made strong progress in implementing IdM solutions in the past five years. At the detail level, however, there is much variability. Demographic factors such as institution size and Carnegie class exert influence in largely predictable ways, but a variety of other environmental factors come into play as well. In the following discussion, we scan the institutional environment for these factors, consider their influence on our set of five core IdM elements, and examine their relation to IdM outcomes.

Environmental Factors

As they did in 2005, respondents told us that their IdM efforts were motivated primarily by concerns related to the security of the institution's IT systems and the privacy of faculty, staff, and students. Other top IdM motivators included enhancing user services and satisfaction and complying with governmental regulations. Positioning the institution to implement federated identity solutions joined the group of top motivators in 2010. As we will see later, that technology's versatility makes it attractive to different institutions for different reasons.

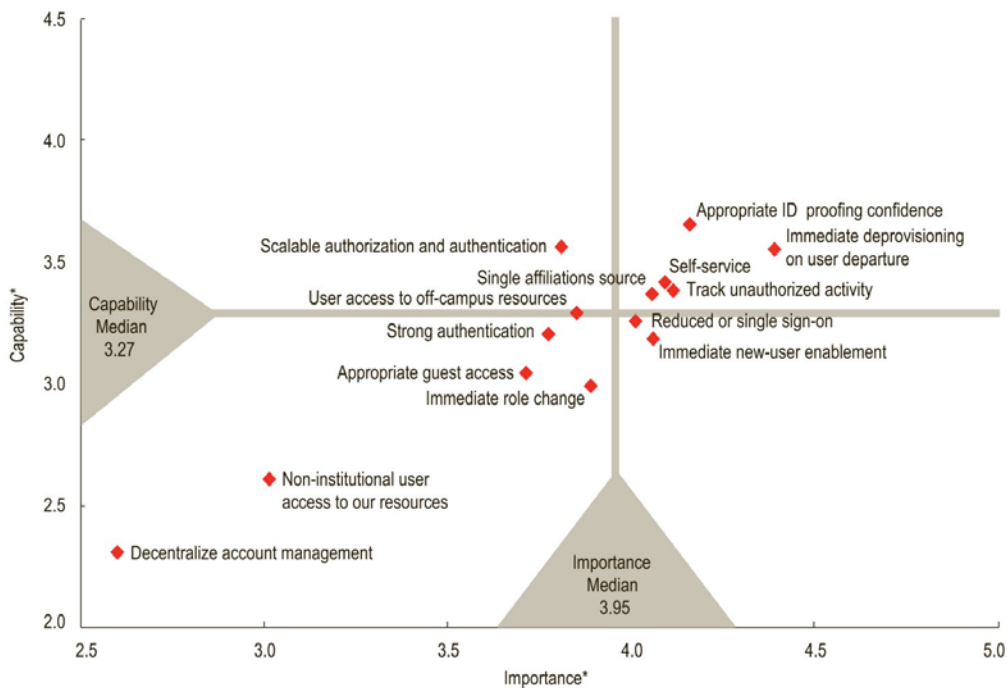
It appears that the factors motivating or obstructing higher education's pursuit of IdM are common to all institutions. Carnegie class, institution size, and institutional control (private versus public) seldom significantly influenced respondents' selection of primary motivators for pursuing IdM and rarely influenced their selection of primary challenges.

For the survey population, overall, those challenges were more organizational than technical in 2005, and they became more so in 2010. For a majority of institutions in both years, higher-priority IT projects were the primary obstacle to more aggressive pursuit of IdM. A lack of adequate funding was also among the most frequently cited organizational challenges. Only one of them declined significantly in importance in 2010: In 2005, difficulty in developing campus policies and procedures was cited as an obstacle by nearly 4 in 10 respondents in the longitudinal sample, but it dropped to 2 in 10 in 2010.

Two technical challenges became less important in 2010: The immaturity of technical solutions was seen as a problem half as often by 2010 respondents as by those in 2005, as were problems with vendor software and support. Lack of IT staff expertise was frequently cited as a primary challenge in both years, although this is one challenge that varied significantly by institution size: Smaller institutions—those with 15,000 or fewer FTE students—were twice as likely as larger institutions to select it as a top-three challenge.

As we did in 2005, we asked 2010 survey respondents to evaluate the importance of 14 different benefits of IdM to their institutions, using a 5-point scale (see Figure 1). We also asked them to use that scale to rate their institution’s capability to deliver each of the benefits. IdM is clearly still a challenge; for each of the benefits, mean importance exceeded the mean reported capability to deliver it. While there is still room for improvement, the gap between importance and capability has shrunk significantly for 13 of the 14 benefits. In the longitudinal sample, respondents reported an average gap of 1.04 points in 2005; in 2010 the average gap was 0.63 points.

Figure 1. Identity Management Benefit Mean Importance and Capability Ratings (N = 314)



*Scale: 1 = very low, 2 = low, 3 = medium, 4 = high, 5 = very high

For the remainder of this discussion we will summarize each institution's capability to deliver the benefits of IdM in terms of the institution's "capability score." This is simply the mean of the capability ratings the institution reported for each of the benefits. Capability score ranges from a low of 1 to a high of 5. In 2005 the mean capability score for the longitudinal sample was 3.12; in 2010 it was 3.46.

Executive Engagement

ECAR often finds that executive engagement in IT projects is a factor in their success. Support from the top can help ensure that the project is adequately funded and can smooth the project's path through any political difficulties that might arise. Several indicators of executive engagement in IdM projects have improved since 2005, and at institutions where those indicators are more positive, we often find greater success in IdM outcomes.

For example, mean agreement that the institution's senior management understands the costs and benefits of IdM increased significantly between 2005 and 2010, and where agreement was stronger, respondents were much more likely to agree that the institution provided the resources needed for IdM. While agreement that senior management was willing to address the policy implications of IdM did not vary significantly from survey to survey, this factor too was significantly associated with stronger agreement that the institution provided the resources needed for IdM.

If executive engagement helps ensure adequate funding for IdM, adequate funding, in turn, helps ensure the institution's capability to deliver the benefits of IdM. Focusing on the full 2010 population, we found that where senior management had a better understanding of the costs and benefits of IdM, where they were more willing to address IdM policy issues, and where the institution provided the funding needed for IdM, mean capability score was significantly higher than where those factors were weaker.

Among the executives whose influence bears upon IdM projects is the institution's senior-most IT leader. We found that IdM projects had become more centralized between 2005 and 2010. They were significantly more likely than they were in 2005 to stand alone rather than be bundled in campus security or portal projects and to be funded through one-time campus budget allocations; and they were less likely to be sponsored by IT administrators other than the CIO or chief information security officer.

Readiness

Institutions can take a number of actions to prepare for success in IdM. These range from laying a firm financial foundation, as discussed above, to carrying out planning and policy development activities. That these actions bear fruit is clear from our survey data. We found that capability score was greater where the institution was further along in completing a diverse set of readiness activities, including

- providing sufficient IT infrastructure,
- developing IdM-related policies,
- monitoring a set of IdM-related metrics,
- developing a documented business case for any area of IdM,

- developing a documented plan for IdM,
- conducting an inventory of campus identifiers,
- conducting a risk assessment of data access security and privacy practices,
- documenting campus data custodians/owners, and
- developing a continuity-of-operations plan that addresses the disaster recovery of identity services.

The institutions in our longitudinal sample have, on average, made substantial progress in key IdM readiness activities between 2005 and 2010. For example, in 2010 more than twice as many institutions as in 2005 had completed a risk assessment of data access security/privacy practices and had released a request for information or a request for proposals for IdM.

With regard to IdM policies, capability score is higher where a set of user authorization policies is in place, but user authentication polices are so pervasive by now that they are no longer a good differentiator among respondent institutions.

Core Elements of IdM

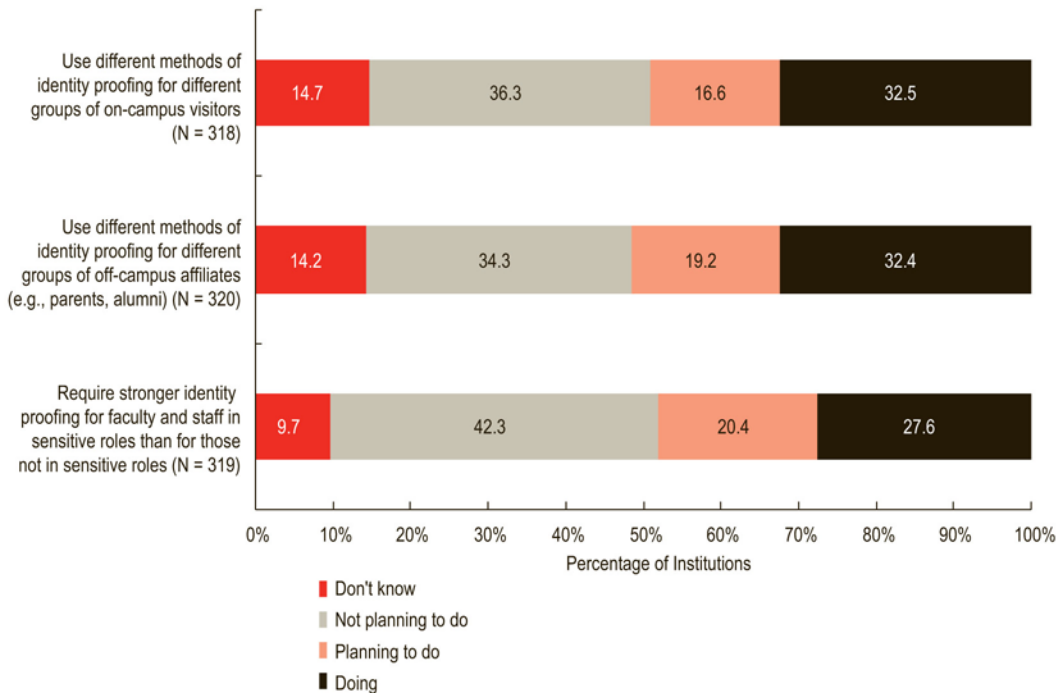
Again, the five core elements of IdM that we have examined in our IdM studies are authentication, reduced or single sign-on, enterprise directories, automated role- and privilege-based authorization, and federated identity. The 2010 data reveal substantial progress in each of these areas, although much remains to be done in most of them.

Authentication

Authentication practices are foundational to any IdM strategy, and we are pleased to report strong advances in several of them between 2005 and 2010. The use of strong passwords increased from about 60% of responding institutions in 2005 to about 75% in 2010; institutions not using them should take note that they are falling behind in this important area. Similarly, reports of prohibitions against using unencrypted passwords over the network more than doubled, rising from fewer than 3 in 10 responding institutions in 2005 to nearly 6 in 10 in 2010. And use of “unique-for-all-time” identifiers was up one-third from the 2005 findings. Overall, more than half of 2010 respondents reported using this kind of identifier, and another quarter said they were planning to do so.

Despite the progress in these areas, little is being done with identity proofing—making sure that individuals applying for login credentials are who they say they are (see Figure 2). In 2010 fewer than 3 in 10 responding institutions reported applying stricter-than-normal identity proofing policies for individuals in sensitive roles, and only an additional 2 in 10 reported any plans to do so. Within the longitudinal sample, there was no significant change in this practice from 2005 to 2010, suggesting that it presents challenges the other basic authentication practices we investigated do not.

Figure 2. Differentiated Identity Proofing for Constituencies



In the early years of this century, public key infrastructure (PKI) showed promise as a tool not just for authentication but also for ensuring the integrity of information transferred between automated systems. Our 2010 survey found that interest in PKI had increased slightly since 2005 but that it was still rarely adopted, with fewer than 2 in 10 respondents reporting its use. More important, though, the future of this technology seems limited. Within the longitudinal sample, respondents saying they had no plans to implement it grew from 2 in 10 in 2005 to 7 in 10 in 2010.

In 2010, multifactor approaches to network authentication other than PKI, including one-time passwords, were being used at fewer than 2 of 10 respondent institutions, and about half the institutions reported no plans to use them. Biometric identification was in use at fewer than 5% of respondent institutions, and most of the remainder reported no plans to use it.

Reduced or Single Sign-On

The days of single, multipurpose IT systems are long past, and most institutions segregate their various IT-based activities onto separate platforms. Each platform is likely to require separate login credentials, and managing even a few of them can be burdensome for the user and can reduce information security by indirectly encouraging system users to keep insecure password memory aids. Many institutions provide relief in the form of a network login, which brokers system access activities for the user based on a single set of login credentials. This and a number of other techniques are used; collectively they are referred to as reduced or single sign-on (RSSO) solutions.

Within our longitudinal sample, little change occurred between 2005 and 2010 in overall adoption of RSSO solutions. In each year, roughly two-thirds of respondents reported active involvement with the

technology. While we did not ask detailed questions about specific RSSO solutions in 2010, more than 3 in 10 respondents did report using Kerberos, a technology well known for its RSSO applications, although it is one that has other uses as well. Variation by Carnegie class was significant, with doctoral institutions being more than twice as likely as any other Carnegie class to report using Kerberos.

Enterprise Directories

A key practice in IdM is to maintain a single, authoritative, online directory of the institution's people and services. Such enterprise directories (EDs) were commonly reported in both years' survey populations and are becoming more common, with 7 in 10 reporting engagement in the technology in 2005 and 8 in 10 reporting the same in 2010. Fully operational implementations increased substantially, from 32.1% of respondents in 2005 to 55.5% in 2010.

The most frequent approach cited for implementing an ED was the use of commercial software, with nearly all respondents reporting its use. About 2 in 10 institutions also reported using open-source software in their ED implementations, a proportion that remained the same between 2005 and 2010 in the longitudinal sample.

Most respondents agreed that their goal is to have most or all central IT applications use the institutional ED. Use of the ED is common for campus e-mail directories and course management systems, moderately common for other administrative systems, and least common for ID-card and physical access systems.

Automated Role- and Privilege-Based Authorization

Manually assigning access rights to users of the institution's IT systems can be a burdensome task. It is more efficient to assign groups of individuals to specific roles and automatically grant them role-appropriate access. This is a difficult process at several levels, not only requiring sophisticated IT solutions but also necessitating collaboration and consensus among diverse campus offices to define the roles the solutions are based on.

Interest in automated role- and privilege-based authorization (RBA) is growing, as reflected in our finding that nearly half of 2010 respondents were actively engaged in RBA projects, while only a third were engaged in them in 2005. Fewer than 1 in 10 2010 respondents reported fully operational implementations, though, up from 1 in 30 in 2005, attesting to the difficulty of adopting this technology.

In 2010, most RBA implementations were based on commercial software. Of all the IdM technologies we researched, RBA was the least likely to be based on open-source software. Nevertheless, open-source software may be gaining ground; reports of its use did increase significantly between 2005 and 2010.

Federated Identity

Until recently, for most applications, IdM has been a campus-based activity. IdM policies and practices have been unique to each institution, and there has been little demand to accommodate access to local resources by unaffiliated individuals or to enable the institution's faculty, staff, and students to access protected resources housed at other institutions. Nevertheless, a certain level of

demand for such exchanges of access privilege has existed for some time, principally in the research and library communities. The Internet community's response has been to develop federated identity (FID) solutions under which groups of institutions agree to trust the identity credentials of each other's users and to allow appropriate access to each other's campus resources.

A related reason for pursuing an FID solution is to make cloud resources more accessible to faculty, staff, and students. Some cloud service providers honor credentials from selected identity federations, facilitating access for members of the affiliated institutions. With interest in cloud-based solutions growing in higher education and elsewhere, it is little surprise that more than half of responding institutions agreed in 2010 that demand for cloud computing resources over the next year would increase the institution's need for FID.

In addition to facilitating access to extra-institutional resources including the cloud, FID can play a useful role on a campus by providing a single sign-on mechanism for institutional systems. In fact, among respondents whose institutions were at least considering an FID implementation, nearly two-thirds from nondoctoral institutions said reduced/single sign-on was a top-three motivator, while fewer than 3 in 10 respondents from doctoral institutions selected that motivator.

Despite its benefits, FID was the least used of the five core IdM elements discussed in this report. Only 32.2% of respondents to the 2010 survey said they were at least beginning to implement FID, and only 12.7% reported fully operational implementations (most of these were based on Internet2's Shibboleth technology). Partially and fully operational implementations were most common among doctoral institutions and institutions that characterized themselves as early adopters of new technologies. Respondents in the latter group were more likely to select academically oriented motivators.

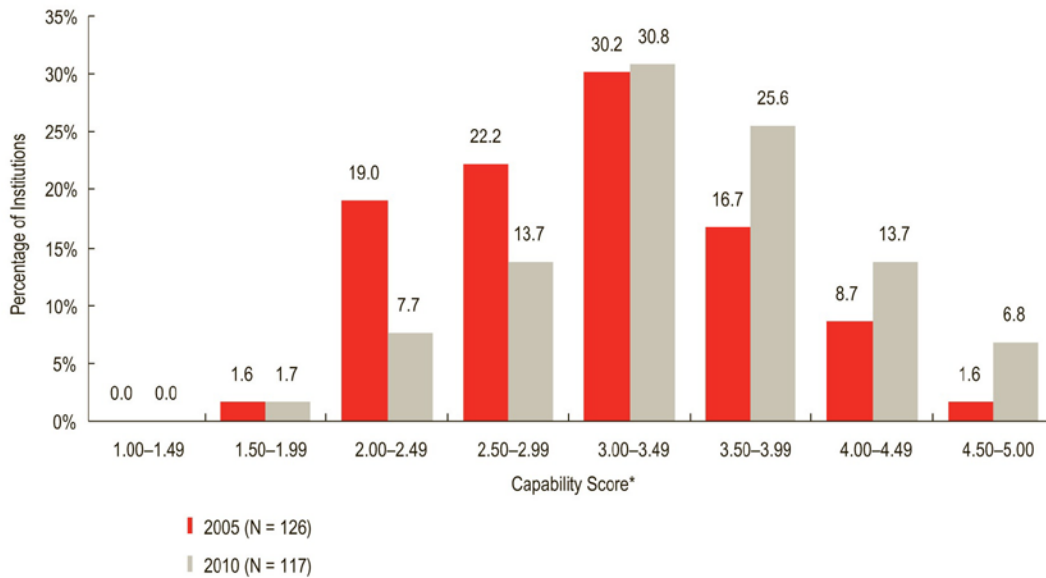
An institution can create its own identity federation, but most elect to become members of an established federation whose credentialing policies they feel comfortable with. The InCommon federation is the one most interesting to our respondents, with a third reporting membership now and another quarter expressing intent to join. About a third also reported current membership in a federation based in a higher education system or consortium, but fewer reported plans to join such a federation.

Outcomes

We gauged the success of IdM implementations in three ways. IdM capability score, defined above as the mean of the institution's self-assessed capability to deliver the benefits of IdM, is one way. The others involved the return on IdM investments (ROI) that the institution felt it had gained. Our two ROI questions looked at whether the institution had achieved cost savings from its IdM projects (or expected to) and, more broadly, whether it had obtained the value it expected from them.

As we have discussed, mean IdM capability score improved significantly between 2005 and 2010 (see Figure 3). We identified a number of factors associated with higher scores, including the long list of IdM readiness activities reported above in the Environmental Factors section of this summary.

Figure 3. Identity Management Capability Score, by Year



*Scale: 1 = very low, 2 = low, 3 = medium, 4 = high, 5 = very high

Like many aspects of IT infrastructure, IdM seems to yield cost savings only infrequently. In 2010 only 1 respondent in 5 reported achieving cost savings from their IdM projects, and fewer reported that they expected to achieve still more savings. This is not a situation that appears to improve over time: Within the longitudinal sample, there was no significant increase—or decrease—in reports of cost savings by year.

Readiness activities appear to influence perceived ROI, similarly to how readiness influences capability score. We found a significant positive association between agreement that the institution provided sufficient resources for IdM and reports of cost savings. As we found in 2005, it appears that in order to save money through IdM projects, an institution needs to invest sufficiently in them. Organization appears to help as well: Achievement of IdM-related cost savings was reported more than twice as frequently when the institution had completed such IdM readiness activities as having a documented plan or business case for any area of IdM or keeping an inventory of campus identifiers, as when those activities were still being planned or were not being planned at all.

Another finding that encourages investment in IdM is that a large majority of respondents agreed or strongly agreed that they had obtained the expected value from the funds spent on IdM projects. This held true in both 2005 and 2010. Again, where agreement was stronger that the institution provided sufficient resources for IdM—invested in it, in other words—agreement that the expected value had been obtained from IdM projects was significantly higher. Most other readiness activities had no significant effect on agreement about value gained from IdM projects. Existence of a completed IdM plan and having IdM infrastructure and policies in place to manage access to intra- and extra-institutional resources were the exceptions; respondents were substantially more likely to agree that expected value had been obtained where these preparations for IdM were in place.

Summary

Concerns about IT security and the privacy of faculty, staff, and students drive most institutions to keep their identity management environments reasonably up to date. Approaches are highly varied, but overall we found that substantial progress has been made in the past five years. Critical factors in IdM success are executive engagement, institutional investment, and the completion of a wide range of readiness activities. While IdM projects seldom result in perceptible cost savings, their value seems clear, and a strong majority of respondents to our survey agreed that their institutions are getting the value they expect from the money they spend on those projects. As the Internet continues its evolution toward a highly collaborative space and as more activities migrate to the cloud, the institutional boundaries constraining most higher education IdM practices will be stretched. Federated identity solutions hold much promise as tools to allow faculty, staff, and students to participate fully—and conveniently—in this broader IT community. While FID solutions are in use by a minority of institutions now, even at the doctoral level, we expect to see rapid and substantial progress in their adoption in the near future.

Endnotes

1. Barbara I. Dewey, Peter B. DeBlois, and the EDUCAUSE Current Issues Committee, "Current IT Issues Survey Report, 2006," *EDUCAUSE Quarterly* 29, no. 2 (2006), 12–30, available from <http://net.educause.edu/ir/library/pdf/eqm0622.pdf>.
2. Bret L. Ingerman, Catherine Yang, and the 2010 EDUCAUSE Current Issues Committee, "Top-Ten IT Issues, 2010," *EDUCAUSE Review* 45, no. 3 (May/June 2010), 46–60, available from <http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume45/TopTenITIssues2010/205503>.
3. Ronald Yanosky, with Gail Salaway, *Identity Management in Higher Education: A Baseline Study* (Research Study 2, 2006) (Boulder, CO: EDUCAUSE Center for Applied Research, 2006), 25, available from <http://www.educause.edu/ecar>.

Mark C. Sheehan (msheehan@educause.edu) is Senior Research Analyst at the EDUCAUSE Center for Applied Research.

A copy of the full study referenced above is available via subscription or purchase through the EDUCAUSE Center for Applied Research (www.educause.edu/ecar/).
