

Roadmap

TOOLS FOR NAVIGATING COMPLEX DECISIONS

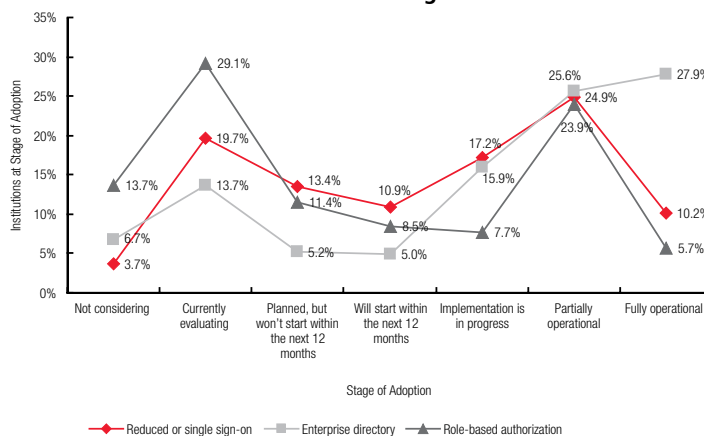
Identity Management in Higher Education: A Baseline Study

By Ronald Yanosky with Gail Salaway, Fellows, EDUCAUSE Center for Applied Research

KEY FINDINGS

- ▶ Identity management (IdM) activity is widespread among respondent institutions, with nine out of ten reporting that they are engaged in IdM efforts or projects.
- ▶ Though fully operational implementations of key IdM technologies are uncommon, virtually all institutions are considering them, and six out of ten are either currently implementing or planning to implement at least one such technology.
- ▶ Security, regulatory compliance, and improved user service and satisfaction are the top factors motivating institutional pursuit of IdM.
- ▶ Responding institutions rely overwhelmingly on passwords for authenticating users to the network. Fewer than three in ten report using a multifactor authentication method.
- ▶ With exceptions in some areas, preparatory work in support of IdM, such as documentation, policy, and planning activity, has not been completed at most institutions. Large majorities, however, have such work in progress or plan to do it.
- ▶ Anticipated central IT spending on IdM over the next three years is modest, especially in light of reported IdM plans, and most respondents believe that senior management does not understand the costs of IdM.
- ▶ Sponsorship and funding of IdM initiatives center predominantly on the IT organization.
- ▶ Respondents who report that their senior management understands IdM also tend to report higher levels of resource sufficiency and overall IdM capability.

Extent to Which Institution Is Considering or Implementing IdM Technologies



Every day, higher education institutions make countless decisions that depend on knowing who's who. Which applicants should be admitted, based on assessments from whom? Who should be able to register for a course, check out a library book, change a grade, pay a bill? And how can this information be used effectively, while keeping it private and secure?

At one time, institutions relied entirely on face-to-face relationships and familiar documentary credentials to identify people and authorize them to do things. But as colleges and universities have moved more and more of their operations online, they have also created a need for electronic mechanisms to

This ECAR roadmap synthesizes the results from a survey of 403 institutions and qualitative interviews with 36 executives and IT staff members from 24 colleges and universities. The roadmap summarizes the 2006 ECAR study Identity Management in Higher Education: A Baseline Study by Ronald Yanosky with Gail Salaway. To order the full study or to learn about subscribing to ECAR, visit the ECAR Web site at <http://www.educause.edu/ecar> or contact us at ecar@educause.edu.

KEY REPORT CONCEPTS

- ▶ Identity management refers to the set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities. (Courtesy the Burton Group.)
- ▶ Authentication is the process of determining whether a person is who he or she claims to be. Authorization is the process of deciding whether to permit a known user access to a particular resource.
- ▶ Enterprise directories are specialized databases that assemble identity information from multiple systems of record, making it available to other systems for authentication, authorization, and other purposes.

perform these functions. It's not a trivial task. Among the billion people who have access to the Internet, Web-based systems must be able to distinguish between those with legitimate purposes and those with malicious intentions. Even within the campus, good business practice and a growing body of regulations demand that online identity transactions be simple, fast, accurate, and secure.

ECAR's study *Identity Management in Higher Education: A Baseline Study* examines the business processes and infrastructure that support the essential tasks of creating, maintaining, and using digital identities. We found that respondents were keenly interested in these issues and working hard on them. Yet we also discovered that both the foundational policy and planning work and the technology infrastructure for IdM were incomplete at most institutions. Our findings also suggest a mismatch between institutions' IdM ambitions and the resources they have to realize them.

Improving Security, Serving Users—and Facing Constraints

Our results reflect the climate of concern surrounding security and privacy issues that have dominated IT agendas in the past few years. Fostering security and privacy best practices was the highest-ranked motivator for pursuing IdM, identified by 81 percent of respondents, and complying with privacy regulations like FERPA and HIPAA was ranked third at 43 percent. In between these two, 61 percent named improved user services and satisfaction.

Among top challenges to pursuing IdM, respondents mainly named resource and organizational issues. Higher IT priorities (54 percent) and lack of adequate funding (39 percent) were the top two challenges named. The difficulty of developing campus policies and procedures—a crucial issue for IdM—was the third-highest ranked challenge at 30 percent. Technical challenges generally ranked low.

Asked to rate the importance to their institutions of 14 specific benefits of IdM, respondents generally gave ratings that mirrored the motivation results. At the top of the list were security-related items like tracking unauthorized activity to responsible persons (rated 4.32 on a five-point scale where 1 = very low and 5 = very high) and immediately deprovisioning users when their relationship with the institution ends (also 4.32). Altogether, six items had mean ratings at or above the level of high importance, and only two were at or below the level of medium importance.

Respondents were more guarded, however, when rating their capability to deliver these benefits. In every case, capability to deliver was rated lower, usually by about one point of the five-point scale. This “capability gap” suggests that institutions are not delivering IdM at a level commensurate with its perceived level of importance.

Readiness

Advisory organizations commonly warn that, while critical to the success of an IdM initiative, documentation, policy, and planning activities can be the most difficult parts of such an effort. By this measure, we found readiness to pursue IdM low overall. In a few critical areas, such as establishing user identity and user authentication, majorities of institutions had completed policies. But only about one-third had documented identity-data custodians, and only about one in four had completed an inventory of campus identifiers. Despite the priority of security concerns, only 13 percent reported having completed a risk assessment of data access security and privacy. In most cases, large majorities had such activities in progress or planned them, suggesting that institutions recognize the importance of such work, but the success of the ambitious IdM initiatives many respondents described may depend on the completion of these preparatory endeavors.

METHODOLOGY

- ▀ A literature review on IdM
- ▀ Consultation with select IdM experts representing higher education organizations and institutions, as well as vendor organizations
- ▀ A quantitative survey of 403 EDUCAUSE member higher education institutions
- ▀ Qualitative telephone interviews with 36 executives and IT staff members at 24 institutions

Technologies

More than 90 percent of institutions told us they rely on conventional passwords to authenticate users for network access, and another 55 percent reported using “strong” passwords—that is, those using formulation rules that make them harder to guess or compute. Security experts, however, often recommend adopting still stronger authentication measures that combine multiple factors of identification—for example, requiring both something you know (such as a password) and something you have (such as a smart card or physical token). These multifactor authentication methods are much less prevalent. Altogether, only 28 percent said they used at least one multifactor method, and 63 percent of those using no such methods either didn’t plan to use them in the future or didn’t know their plans.

Adoption plans were much more ambitious for three other key technologies we asked about: enterprise directories (see “Key Concepts”); reduced or single sign-on (the ability to authenticate once and then move among multiple applications, minimizing the number of accounts and passwords needed); and role-based authorization (giving users access to resources automatically, based on known characteristics such as job title or enrollment status). Fully operational implementations of these technologies were relatively rare, but most respondents were engaged in them somehow, from evaluating them to having operational deployments.

Nearly two-thirds (64 percent) of respondents told us they were implementing one or more of these technologies now or planned to in some timeframe. Even among those who told us they were not considering one of the technologies now, most said they expected to in the future. Taken together, such plans add up to an ambitious enhancement of IdM capabilities.

Federated identity, another key IdM technology we asked about, allows entities in different IT domains to share user attribute information, giving users access to outside

resources such as digital library content after authenticating in their home domain. Only about 14 percent of respondents told us they thought their institutions had a need now for a federated identity solution, but another 48 percent said they saw a need in coming years.

IdM Projects: An IT-Centric Endeavor

Engagement in IdM projects was almost ubiquitous, with 89 percent of respondents saying they were involved in IdM efforts or projects. Bundling IdM work with other projects was the most common implementation strategy, named in some form by 62 percent of project-active respondents. By contrast, only 28 percent said they had a stand-alone IdM project. Funding and sponsorship for IdM projects depended heavily on the IT unit. Nearly three-fourths of project-active respondents named the central IT budget as a funding source, and 51 percent identified it as their sole funding source. Sponsorship was even more IT-centric: 99 percent named at least one IT sponsor, and 72 percent named *only* IT sponsors for their IdM initiatives.

Spending

Given the high degree of project activity and ambitious technology adoption plans we found, anticipated spending levels on IdM were modest. Forty-seven percent of respondents expected their central IT units to spend \$100,000 or less on IdM over the next three years, and 76 percent expected to spend \$500,000 or less. (Another 14 percent answered “don’t know.”)

Our question did not attempt to uncover spending outside of central IT, and it may have missed expenditures on staff and project spending not considered “IdM spending.” But even as a lower bound to what would be higher expenditures were all sources included, we see these spending levels as sufficiently modest to challenge the aggressive adoption plans many respondents reported.

RECOMMENDATIONS

Based on its findings in *Identity Management in Higher Education: A Baseline Study*, ECAR offers the following recommendations:

1. Build the policy foundation.

The identity infrastructure is in essence a technical implementation of rules about access, data control, and, ultimately, the management of the institution. Where these rules are ad hoc and undocumented, identity systems are exposed to security risks, inconsistencies, and redundancies. Auditability suffers as well. Clear identity policies reflecting an explicit campus consensus will greatly improve identity processes even where the infrastructure is underdeveloped.

2. Unsnarl the data tangle.

No concern was voiced more often in the course of our study than the observation that basic identity-related elements lack an enterprise-wide definition. Seeking out data stewards and working with them to create cleaner, more portable, and better defined data structures can enhance the accuracy and leveragability of identity systems.

3. Embrace standards and flexible architectures.

It's hard to think of an area of IT that could benefit more from open standards and architectures than IdM. Though IdM standards remain immature, a solid core exists. Institutions that make the maximum possible use of standards and flexible architectures will be in the best position to exploit a maturing product marketplace and respond to emerging IdM demands.

4. Make the most of incremental improvements.

Where central IT needs to move forward without generous resources or campus buy-in, projects should be organized to demonstrate quick wins with clear business benefits that are brought to the attention of users.

5. Get senior management aware and involved.

Though it is something of an old chestnut in IT administration, the value of senior management awareness and support is hard to overstate. Making senior leaders aware of the business and academic benefits of a sound identity infrastructure is a way to enlist their aid with the political and financial challenges that confront IdM initiatives.

Leadership Matters

Respondents presented a mixed bag of responses when we asked about senior management understanding of IdM. Fifty-five percent agreed or strongly agreed with the statement that senior management "is willing to address the policy issues related to IdM." But respondents were less optimistic about senior management understanding of the benefits of investing in IdM (41 percent agreed or strongly agreed) and were outright pessimistic about understanding of the costs of IdM (17 percent).

It will be important for IT units to close these gaps in understanding. Institutions reporting a more optimistic assessment of senior management also reported higher agreement about getting needed resources for IdM, higher overall IdM capability, and greater success achieving cost savings through IdM projects.

Standing at the Threshold

Though the agendas of respondents were crowded with activity, we more often found them approaching and planning for IdM than practicing it. Interest is high, and important gains have been made. But given the resource constraints higher education faces, institutions will have to pursue their IdM plans with an eye on flexibility and agility, putting limited resources where they will do the most good. As a key enabler of online transactions and many desirable new services, IdM will almost certainly justify investments beyond the amounts we found. Institutions will have to prepare the ground, however, by transforming virtual identity from a parochial IT concern to an institutional priority.