Key Findings

Identity Management in Higher Education: A Baseline Study

Ronald Yanosky, with Gail Salaway

In recent years, higher education IT administrators have become uncomfortably aware that the great progress they've made in putting resources online has outpaced their ability to know with assurance who's asking to use those resources. In part, this simply reflects long-term concerns that have come to a critical point. The enormous spread of Internet usage, from 45 million persons in 1995 to more than one billion in 2005, has relentlessly increased the demand on identity systems, while a correspondingly vast growth in the dollar value and sensitivity of online transactions has raised both the costs of identity error and the incentives for identity fraud. Technologists have had to back-engineer identity mechanisms into an Internet that wasn't designed for them, while struggling to get identity capabilities traditionally embedded in local applications to scale up and interoperate across today's complex IT environments.

Developments in public policy have transformed these digital-identity challenges from an obscure technical concern into front-page news. With the annual cost of identity theft estimated at $50 billion in the United States alone, and as dozens of states are passing security-breach notification laws, all IT organizations are under pressure to strengthen identity and privacy protection. Homeland security issues, meanwhile, have led the federal government to adopt a new identity infrastructure for its employees and contractors and to set more stringent authentication standards for its IT systems and those that interact with them.

New academic and business ambitions that higher education is likely to adopt—from giving users access to the growing universe of digital online content to working more effectively with business partners—will also require more sophisticated and reliable identity mechanisms. It's not surprising, then, that the EDUCAUSE Current Issues Survey of 2005 named security and identity management as the issue most likely to become "much more significant" in the future (Maltz, DeBlois, & EDUCAUSE Current Issues Committee 2005).

But are higher education institutions doing more than worrying about identity concerns? ECAR undertook this study to find out and to establish a baseline of knowledge about identity practices that

might feed future research about activity and best practices in this field. The core functions of identity management (IdM) that we examined include:

- *Establishing identity*—the process of associating a physical person with verified identity information prior to the issuance of digital identifiers and the creation of a user account.
- *Authentication*—the process of gaining confidence that the person using a digital identity is the person who is qualified to use it.
- *Authorization*—the process of determining a specific person's eligibility to gain access to an application or function or to use a resource.
- *Enterprise directory*—a central institutional lookup repository that holds data regarding the institution's people and services, informing authentication and authorization processes.
- *Reduced or single sign-on (RSSO)*—a method of authentication that lets a user log into a network and, for a period of time, have his or her credentials passed to the requested applications, enabling use of the resource without requiring separate authentication for each one.
- *Federated identity*—the loosely-coupled, standards-based exchange of identity attributes across IT domains, carried out by partners who accept one another's authorization assertions.

Though it is often considered an aspect of identity management, for reasons of scope we did not examine account provisioning. We also did not look at aspects of the security infrastructure beyond the identity function.

As summarized below, besides looking at the adoption of technologies related to these functions, we examined the importance respondents saw in the benefits of IdM and their ability to deliver them; the motivations that drive them to adopt IdM and the challenges they face; the policies and plans they are preparing to support IdM; how they are organizing IdM projects; and the factors that influence good outcomes in IdM investment and capability.

Identity Management

Information systems have dealt with identity issues for many years, but only recently have technologists begun to encourage a comprehensive approach to identity *management*. Rather than treating user identity as an afterthought, as the Internet does, or as the local concern of application business logic, as most legacy systems did, IdM takes a holistic approach in which identity attributes are abstracted and standardized for seamless and secure exchange throughout the online environment. IdM also attends to the business and policy issues, not just the infrastructure, relating to identity. To reflect this concern, we built our study around a definition developed by the Burton Group: IdM is "the set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities."

Methodology

Our research methodology had four main components. We began with a review of the relevant literature on IdM issues, policies, and technologies. While developing a survey instrument, we consulted with select individuals representing organizations involved in IdM, including the National Science Foundation Middleware Initiative-Enterprise and Desktop Integration Technologies (NMI-EDIT) Consortium, Internet2, and several higher education institutions and vendor organizations. The largest component of the study was the quantitative analysis of survey responses from 403 EDUCAUSE member institutions. Respondents—primarily chief information officers and director-level IT officers—represented a diverse set of institutions in the United States and Canada, including both public and private institutions and the full range of Carnegie classes and enrollment sizes. Reflecting the EDUCAUSE membership base, doctoral institutions were the best-represented Carnegie group.

Finally, we supplemented the quantitative survey with qualitative interviews with 36 executives and IT staff members involved in IdM, representing 24 institutions.

Significant Findings

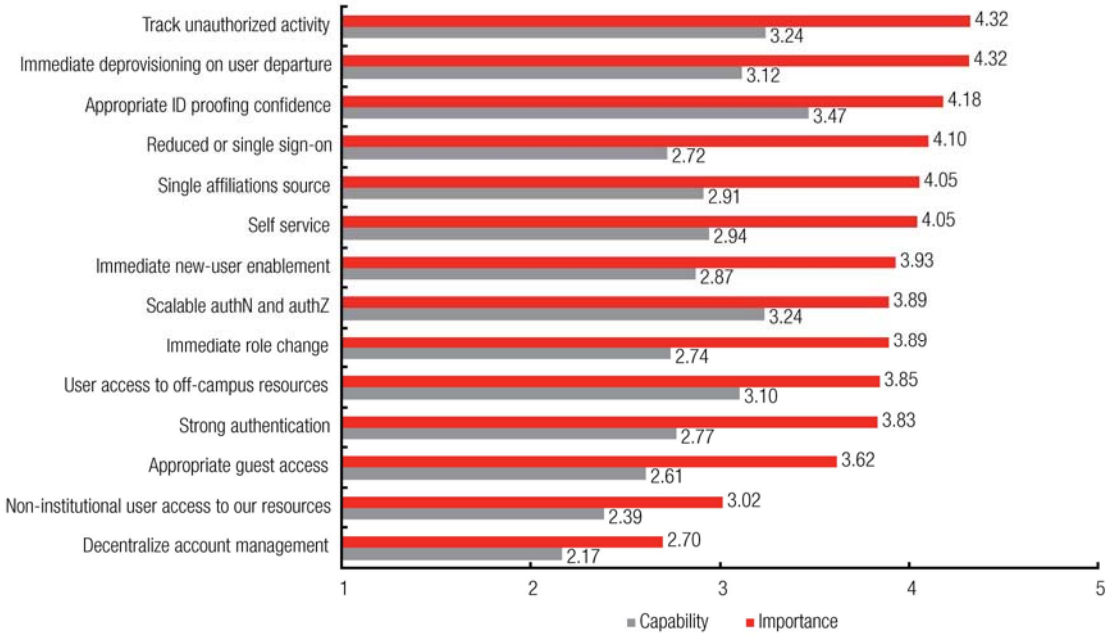
We found that, despite challenges involving resources and other IT priorities, responding institutions are deeply engaged in IdM activities. They told us they thought its benefits were important, and nearly all said they were at least considering implementing its major technologies. At the same time, we found that experience with fully operational IdM technologies was relatively rare. So, too, is completed work dealing with the policy, planning, and measurement issues needed to support IdM initiatives, though we found much in-progress activity. Here we integrate and summarize our findings.

Importance and Capability: The IdM Capability Gap

Respondents made it clear that they think IdM delivers important benefits. Presented with a list of 14 practical benefits commonly attributed to IdM and asked to rate each one's importance to their institution on a scale of 1 (very low) to 5 (very high), respondents gave six items mean ratings at or above the level of high (= 4) importance and rated only two at or below the level of medium (= 3) importance (see Figure 1). Security-related items such as tracking unauthorized activity and deprovisioning user accounts when users leave dominated the top slots, while core-community service improvements such as fast new user enablement and RSSO were close behind.

Respondents did not, however, rate their capability to deliver these benefits as highly as they rated their importance. In every case, capability to deliver rated lower, usually by about one level of the 5-point scale. The existence of this "capability gap" suggests a widespread sense among respondents that they are not delivering IdM services at a level commensurate with their importance. The ambitious plans that we discovered for adopting IdM technologies, reported below, imply that institutions see pressing unmet needs that they plan to fulfill. However, it's also possible that some institutions are "satisficing"—that is, tolerating suboptimal performance because the political or financial costs of optimizing are too high. (For more on "satisficing," see Kvavik & Goldstein, 2005.)

Figure 1. IdM Benefit Mean Importance and Capability Ratings



(1 = very low, 2 = low, 3 = medium, 4 = high, 5 = very high)

Motivations and Challenges

Both the quantitative results and the interviews made it clear that our respondents see "security and privacy best practices" as the greatest motivator for pursuing IdM: 81 percent identified this as one of their top-three motivators, more than any other motivator we asked about. Somewhat surprisingly, however, respondents also gave generally high ratings to the security of their central data, networks, and applications (4.0 on a scale of 1 to 5). Slightly over half of respondents, moreover, said that they had had no significant security incidents related to user identification, authentication, or authorization in the past two years, and another 18 percent said they had had only one such incident. Such findings may reflect optimistic self-reporting about sensitive issues, but it also suggests that, although they are concerned about security issues, many institutions see them as manageable.

Enhanced user services and satisfaction was the second-highest ranked motivator, chosen among their top three by 61 percent of institutions. Interviewees told us that benefits such as reducing the number of accounts and passwords users must keep track of, provisioning accounts faster, and improving self-service were key ways to rally the support of users and campus managers for investment in IdM.

Compliance with regulations such as the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley Act was third among motivators, selected by 43 percent of respondents. Few or no respondents chose a strategy of early adoption or the desire to reduce vendor dependencies as a motivator.

Busy agendas and resource constraints dominated the challenges to pursuing IdM that respondents identified. Fifty-four percent put higher IT priorities among their top-three IdM challenges, and 39 percent named the unavailability of adequate funding. The higher education budget crunch that started around 2001 still seems to be a factor for some institutions: among those who told us their IT budgets had declined in the past three years, nearly half named inadequate funding as a top-three challenge, while only about one in five of those with rising budgets did so.

Besides resource constraints, organizational challenges were noteworthy. Difficulty developing campus policies and procedures was the third-highest ranked challenge for 30 percent of respondents, and another 21 percent cited the lack of IdM ownership by a central group. These findings may help explain why we found relatively low levels of completed work in most areas of IdM policy and planning.

Readiness for IdM Activity

In many ways, an identity management infrastructure is the technical expression of business rules and policies that require input and decision making from many parts of the institution. Advisory organizations commonly warn organizations that these activities, which are critical to its success, can be the most difficult part of an IdM initiative.

We found that responding institutions were heavily engaged in documentation, planning, and policy activities but that completed work in these areas is generally low. Only about one-third of institutions had completed documenting campus data custodians/owners, for example, and only about one in four had completed an inventory of campus identifiers (see Table 1). Despite the prominent role that security plays as a motivator for IdM, only 13 percent had completed a risk assessment of data access security and privacy practices. At the same time, large majorities either had such work in progress or planned to undertake it.

Table 1. Documentation of IdM Data Sources, Risks, and Needs (N = 401)

Documentation Activity	Completed	In Progress	Planning to Do	Not Planning to Do	Don't Know
Documented campus data custodians/owners	32.5%	33.5%	23.8%	6.5%	3.8%
Inventory of campus identifiers (such as used by library, e-mail, etc.)	26.2%	33.4%	24.7%	10.0%	5.7%
Documented data definitions, reconciling differences between different data sources	15.0%	38.3%	28.8%	10.8%	7.3%
Risk assessment of data access security and privacy practices	12.8%	34.4%	36.2%	11.8%	4.8%
Released an RFI or RFP for IdM	5.5%	4.5%	16.1%	62.0%	11.8%

We found a similar pattern in the areas of documented IdM plan and business case development. Only about 12 percent of respondents said they had a completed, documented IdM plan, and just 17

percent told us they had a completed business case for any area of IdM. As with the documentation activity, however, the great majority of respondents indicated that they had such work either in progress or planned. Only 15 percent told us they did not expect to create a documented IdM plan for their institution, though a larger 28 percent said they didn't expect to create a business case.

We did find some areas where IdM readiness was stronger: over half of respondents reported completed policies in the key areas of user authentication (58 percent) and establishing identity (51 percent), with most of the rest working on them. We also found that in certain areas, completion of readiness activities went up among institutions reporting more advanced stages of IdM technology adoption. Completion of an inventory of campus identifiers, for example, was reported by only 12 percent of those who were evaluating an enterprise directory, but this figure rose to 48 percent for those with a fully operational enterprise directory. These increases tended to appear in the later stages rather than the planning stages of adoption, and they still left significant percentages of fully operational respondents without completed documentation, plans, and policies.

Technology Adoption

We found respondents busy with IdM technologies at many levels, from evaluating them, to planning their adoption, to using them in partially or fully operational implementations. At the same time, there were relatively few institutions with fully operational instances of IdM technologies, and "not planning to use" rates were far higher for certain technologies than for others.

User Authentication

Respondents continue to rely overwhelmingly on passwords for authenticating users to the network (see Table 2). Ninety-one percent reported using conventional passwords or PINs for authentication, and 55 percent said they used strong passwords (i.e., passwords using formulation rules that make them harder to guess or compute). Another 24 percent said they planned to use strong passwords in the future.

Table 2. Authentication Methods for Network Access (Multiple Responses Allowed)

Method	Using	Planning to Use	Not Planning to Use	Don't Know
Conventional password/PIN	91.1%	2.1%	6.5%	0.3%
Strong password	55.0%	23.8%	16.5%	4.7%
Kerberos	26.2%	11.5%	46.1%	16.1%
PKI certificate (software) without PIN	7.1%	7.4%	58.9%	26.5%
PKI certificate (software) with PIN	4.8%	10.6%	55.9%	28.7%
PKI hardware token without PIN	0.6%	2.8%	68.9%	27.7%
PKI hardware token with PIN	1.8%	7.6%	62.2%	28.4%
SecurID-style one-time password	12.7%	11.8%	54.6%	20.9%
Other multifactor authentication methods	6.5%	17.9%	48.7%	27.0%
Biometric identification	3.3%	12.6%	66.1%	18.0%

Beyond these common authentication methods, however, use and planned use dropped dramatically. Slightly more than one in four reported using the Kerberos network authentication protocol, with doctorals more than twice as likely to use it than the other Carnegie categories.

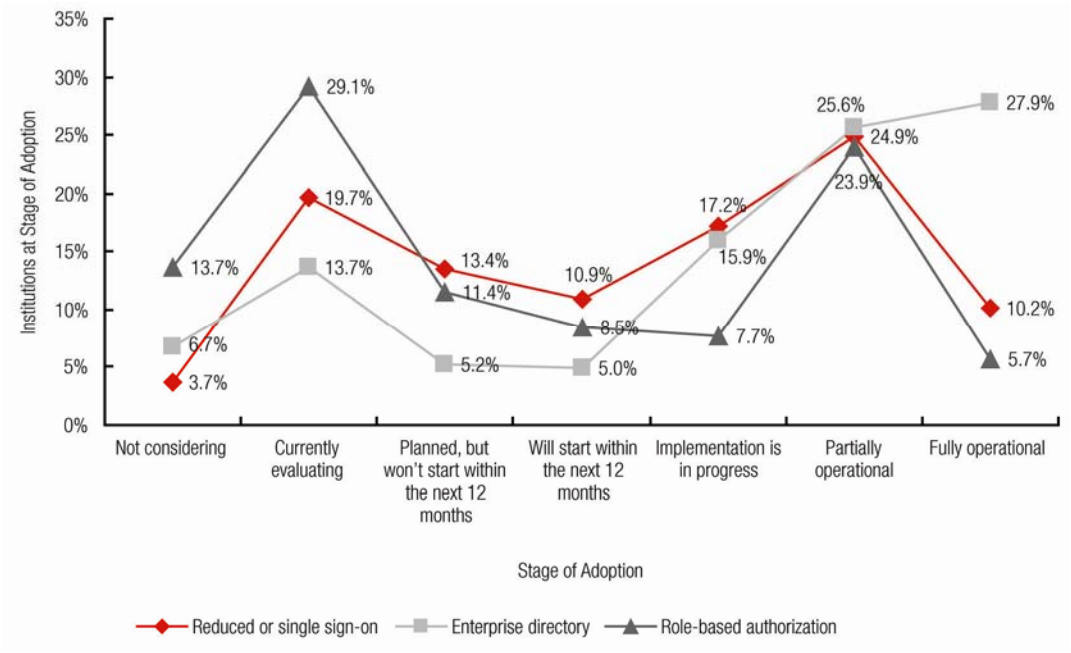
Though multifactor authentication methods (those employing two or more factors of identification, such as a hardware token combined with a password) are increasingly recommended at least in some situations by security experts, only 28 percent of respondents said their institution used at least one such method. Plans to use them in the future in many cases suggest considerable relative growth: 1.8 percent now using PKI hard tokens with a PIN, versus 7.6 percent planning to use them. This growth, however, will come on top of a low base of current use, and "not planning to use" rates were high for all of these technologies. Overall, 63 percent of those not using at least one such method either said they had no plans to use them or didn't know their plans.

With increasing pressure for multifactor authentication coming from sources such as the federal government's E-Authentication initiative, which requires multifactor methods for some defined levels of assurance, and from federal banking industry regulators, the resistance to such methods may decrease over time. For now, however, we found that most institutions have few arrows in their network authentication quivers, and a majority of respondents have no firm plans to change.

Enterprise Directories, RSSO, and RBA

We asked detailed questions about institutions' adoption of three key IdM technologies: enterprise directories, RSSO, and automated role-based authorization of users (RBA). Figure 2 shows the distribution of responses among the stages of adoption we specified, ranging from "not considering" to "fully operational."

Figure 2. Extent to Which Institution Is Considering or Implementing IdM Technologies (N = 402)



Enterprise directories were easily the most widely adopted IdM technology, with 53.5 percent of respondents reporting being either partially or fully operational. RSSO and RBA had about the same level of partially operational respondents as enterprise directories—roughly one in four institutions each—but were much less likely to be reported as fully operational. For RSSO and enterprise directories, levels of adoption tended to be more advanced as Carnegie highest-degree levels and institutional size increased. Institutions that had implemented data warehouses and student portals tended, in each case, to report more advanced stages of adoption for all three technologies.

More striking than the degree of operationality is the widespread activity among pre-operational institutions. Overall, 64 percent of respondents told us that they were either in progress with an implementation of at least one of the technologies or had plans to implement one or more in some time frame. When those currently evaluating the technologies are included, the percentage of institutions that are "in the game" but not yet operational reaches 61 percent for RSSO, 57 percent for RBA, and 40 percent for enterprise directories. Even among those who told us they were not considering one of these technologies, most said they expected to some time in the future. Finally, adding to the level of planned activity, a majority of those with operational enterprise directories told us that they expected to add functionality in the future.

The applications most commonly reported as using enterprise directories were classic central infrastructure services, such as e-mail directories and network operating systems, and enterprise applications, such as course management systems, library systems, and student information systems. Only 27 percent of institutions with a partially or fully operational enterprise directory reported that any departmental systems used it, underscoring the decentralized nature of many campus IT environments. The dominant technologies in use or planned for use in enterprise directories were LDAP and Microsoft Active Directory, each claiming well over half of all respondent institutions with operational enterprise directories.

Federated Identity

Federated identity allows entities in different IT domains to share user attribute information, making resources from the entire group available to users who are known and authorized in only one domain. Using a standards-based, loosely coupled approach to interoperability, federated identity could become a key technology for giving institutional users access to resources like digital library collections, research databases, and business partner information systems.

We found interest in federated identity solutions high, but most respondents did not see an immediate need for one at their institution. Only about one in seven (14 percent) said that their institution had a current need for a federated identity solution. This perception varied widely by Carnegie class: 30 percent of doctorals reported such a need, nearly three times the rate of the next highest Carnegie category (associate's institutions). "Don't know" answers were relatively high for this question (23 percent), indicating the newness of the technology. A high growth rate for federated identity adoption is suggested by the 24 percent who told us they anticipated a need within the next two years, but overall we found no clear time frame that looked like a potential "tipping point" for explosive growth.

Seeing a need does not equate to implementing a federating technology, such as Internet2's open source Shibboleth solution or the more corporate-oriented Liberty Alliance technology. Overall, 13 percent of respondents said they were implementing such a technology. Among those who said they see a need for a federated identity solution now, 42 percent reported implementing a federating

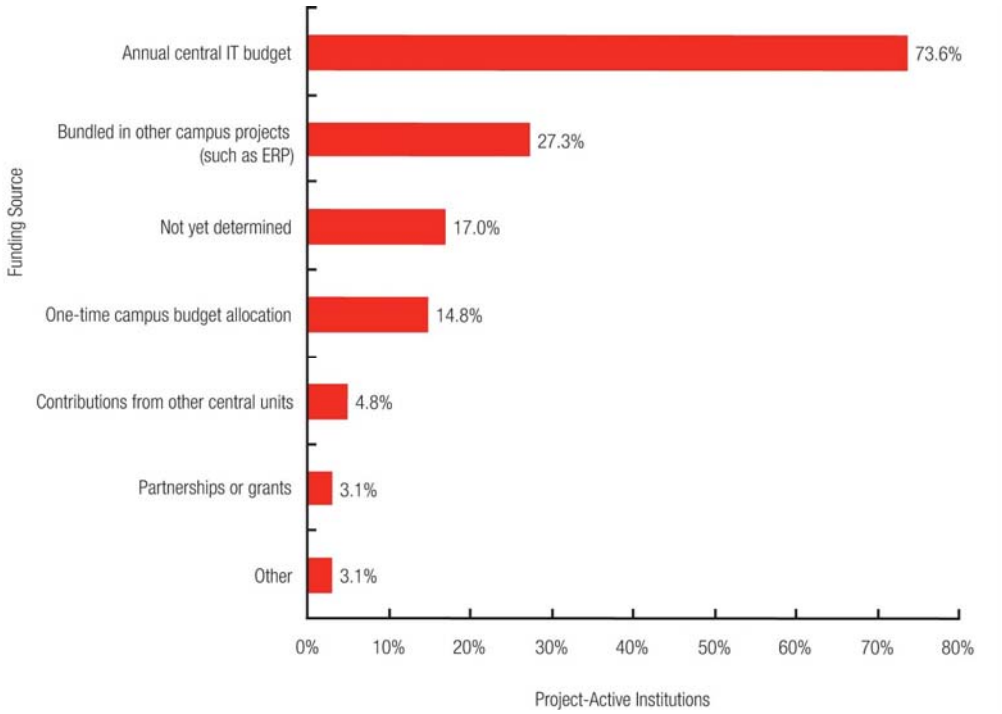
technology, and another 29 percent said they plan to. While our question did not specify a particular solution, interviewee comments made it clear that respondent interest is overwhelmingly in Shibboleth rather than other federated identity products.

Project Activity and Strategies

Not surprisingly, in light of the IdM technology adoption activity reported above, respondent institutions were heavily involved in projects: 89 percent reported being engaged in efforts or projects related to IdM. While participation was high across the board, it rose with institutional size. Seventy-four percent of institutions with 2,000 or fewer students were active, compared with 95 percent of those with more than 8,000 students. About one-third of project-active respondents said they had organized their IdM initiatives as formal projects, and another 22 percent said they were considering doing so. This IdM activity was often bundled with other projects. In fact, 62 percent of respondents reported that they bundled IdM project work with a security, portal, ERP, or other implementation project, more than double the 28 percent that reported a stand-alone IdM project.

Despite these bundling strategies, we found strong indications that IdM is an IT-centric activity at most institutions. By far the most common funding source cited for IdM projects was the annual central IT budget; nearly three out of four respondent institutions named it (see Figure 3). Bundling with other campus projects, at 27 percent, was the second-most named funding source, though this number was only about half the percentage of those mentioning bundling as an implementation strategy. Only about three in ten respondents told us that their IdM projects had any kind of non-IT sponsorship (for example, a functional area executive), and virtually all of these also mentioned some kind of IT sponsor, usually the CIO. Institutions that had organized their IdM projects as formal initiatives were about twice as likely to say they had a non-IT sponsor.

Figure 3. How IdM Projects Are Paid For (Multiple Responses Allowed)



Resources, Spending, and Staffing

We found respondents about evenly divided in their perceptions about the sufficiency of funding for IdM at their institutions, though slightly leaning toward pessimism. Thirty-six percent disagreed or strongly disagreed with the statement that their institution was providing the resources needed for IdM, while the remainder was about equally divided between those who were neutral and those who agreed or strongly agreed. Institutions that had more aggressive technology adoption strategies, and those that said creating competitive advantage was their institutional IT goal, tended to report higher agreement that they were getting needed resources.

Consistent with this less-than-enthusiastic characterization of resource sufficiency, respondents' reported levels of anticipated spending by central IT on IdM projects over the next three years were, on the whole, quite modest. Forty-seven percent of respondents said they expected to spend $100,000 or less, and three-fourths (76 percent) said they would spend $500,000 or less. Since about 14 percent said they didn't know what they would spend, this leaves about one in ten with definite plans to spend $500,000 or more. Most of these anticipated spending less than $1 million. Spending in the $500,000 or more bracket was dominated by doctorals and institutions of 15,000 or more students.

These figures should be understood as a lower bound to what would certainly be higher expenditures were all internal and external spending considered. Our question did not attempt to capture all institution spending comprehensively, leaving out routine non-project spending and spending not controlled by central IT (such as expenditures by departments, schools, or special project offices). It is possible as well that some respondents did not consider bundled projects in which IdM work was being done as "IdM projects" and so did not report spending on IdM within them, even if it was controlled by central IT. Also, when we asked interviewees to confirm their spending responses, some told us that they had included all internal and external spending, while others told us that they included external goods and services but not staff costs. All but one of our interviewees, however, did confirm their spending responses.

Even with these caveats, however, our conclusion remains that anticipated central IT spending on IdM projects over the next three years is modest enough to be a challenge to the aggressive adoption plans many respondents reported. We did not find evidence for a pending wave of "big bang" IdM projects, and the multimillion dollar IdM projects that some product and services firms promote will be relatively rare among our respondent base.

We found a corresponding modesty in IdM project staffing. About 14 percent of project-active institutions reported no central IT staff dedicated to IdM projects, and 58 percent said they had either one or two full-time-equivalent staff. Though staffing levels tended to rise with institutional size, even among institutions of 15,000 or more students, slightly over half reported two or fewer IdM staff.

Value and Cost Savings

Project-active respondents gave a strong, if not quite overwhelming, endorsement to the value of IdM investment. Asked how strongly they agreed with the statement that their institution was getting the expected value from money spent on IdM projects, six out of ten agreed or strongly agreed, and

another 26 percent were neutral. Most of the rest said they didn't know, leaving only a small sliver (2 percent) of disagreement.

We got more mixed and nuanced responses when we asked about expectations of cost savings. Only 10 percent of respondents told us they had achieved cost savings from their IdM projects, though another 27 percent said that they expected to in the future. The largest group, more than 40 percent, said they had not and didn't expect to. This isn't surprising in light of the fact that only 18 percent of respondents named cost savings or greater efficiencies as top motivators for pursuing IdM. Security and user service were much more frequently cited motivators.

IdM Capability and Cost Savings: What Matters?

As we noted above (see Figure 1), our survey asked respondents to rate the importance of 14 benefits of IdM and to rate their institution's capability to deliver each benefit. (The rating scale ranged from 1 = very low to 5 = very high.) To develop an overall IdM capability score for each respondent, we calculated the mean of all their separate benefit capability ratings. We then looked for attributes and practices associated with higher capability scores. We also performed a similar search for factors related to achieving cost savings from IdM projects. Our findings about the characteristics associated with good outcomes are summarized below.

Resources

Not surprisingly, we found that institutions reporting greater agreement that their institutions provided the needed resources for IdM had higher IdM capability scores than those reporting less agreement. Capability scores rose from 2.51 (std. deviation = 0.449) among those strongly disagreeing to 3.34 (std. deviation = 0.838) among those strongly agreeing. Perhaps less intuitively, respondents who reported achieving cost savings from IdM projects also tended to rate resource sufficiency higher than those who did not achieve cost savings. The lesson may be that it takes resources to save resources.

Senior Management Understanding

We found a mixed bag of respondent perceptions about senior management attitudes toward IdM. Fifty-five percent agreed or strongly agreed with the statement that their senior management "is willing to address the policy issues related to identity management," but only 41 percent felt the same way about the statement that senior management "understands the benefits of investing in identity management." Respondents were most pessimistic about the statement that senior management "understands the costs of identity management": 56 percent disagreed or strongly disagreed, while only 17 percent agreed or strongly agreed.

Our findings suggest that it will be important for IT administrators to do what they can to raise senior management understanding and support and to get senior leaders to appreciate the costs as well as the benefits of IdM. Respondents who gave higher agreement ratings about senior management attitudes tended to report higher IdM resource sufficiency. Moreover, as Table 3 shows, where respondents agreed more about senior management understanding of costs and their willingness to address relevant policy issues, IdM capability scores were higher. Likewise, institutions rating these two senior management measures higher also were more likely to report cost savings from IdM projects.

Table 3. Mean IdM Capability Score, by Agreement Rating of Senior Management Attitudes

Attitude	Agreement Rating	IdM Capability Score	
		Mean	Std. Deviation
Understands costs of IdM	Strongly agree	3.05	0.702
	Agree	3.06	0.704
	Neutral	2.97	0.635
	Disagree	2.80	0.598
	Strongly disagree	2.68	0.673
Willing to address policy issues	Strongly agree	3.21	0.771
	Agree	2.93	0.616
	Neutral	2.87	0.623
	Disagree	2.56	0.514
	Strongly disagree	2.44	0.684

(1 = very low, 2 = low, 3 = medium, 4 = high, 5 = very high)

Policies and Readiness

As we noted above, many IdM experts recommend that organizations prepare the ground for IdM with documentation, planning, and policy work. But does this complicated, politically difficult work really matter?

Our findings suggest that at least some of it does. Institutions that reported completing policies for user authentication and authorization had a higher mean IdM capability score than those with policies in progress, which in turn had a higher mean score than those with no documented policies. We found a similar pattern, though involving different readiness actives, with IdM cost savings: institutions that had a documented business case for some area of IdM, had a documented plan for IdM, and had documented relevant data definitions were more likely to report cost savings from IdM projects than those at lower stages of completion.

Technology Leadership

Higher education, like other industries, has historically relied on innovators and aggressive competitors to develop techniques and competencies in new technologies ahead of the mainstream demand curve. We found some signs that this process is continuing with IdM. Institutions reporting a more aggressive technology adoption strategy also had a higher mean capability score than those with less aggressive strategies. For example, respondents describing their institutions as innovators in technology adoption had a mean 3.13 capability score (std. deviation = 0.695), while those describing their institutions as technology laggards had a mean capability score of 2.29 (std. deviation = 0.619).

We found a similar relationship with institutional IT goals. Those who described their institution's IT goals as creating competitive advantage had higher capability scores on average than those whose

goal was to provide reliable IT services at the lowest cost. More aggressive technology adoption strategies and IT goals were also associated with higher reported resource sufficiency for IdM.

Conclusion

Though the agendas of our respondents were crowded with activity, it would be more accurate to say that we found most of them standing at the threshold of identity management rather than practicing it. Interest in IdM is very high, and respondents acknowledge the importance of the benefits that it delivers. But reported rates of fully operational IdM technologies are generally low, use of federated identity is restricted to a narrow slice of mostly doctoral institutions, and network authentication technology remains a conservative domain. Resources are constrained, and most institutions will enter the next three years with modest central IT funding (at best) for IdM initiatives. "Don't know" rates that were often a substantial factor in our findings about plans and approaches suggest that many institutions are taking a wait-and-see attitude IdM issues.

An advance guard of mostly doctoral and large institutions is engaged in large-scale and sophisticated IdM projects that will greatly help the rest of the higher education community bring IdM and associated best practices into the mainstream. But the constraints that most institutions face in funding, staffing, and crowded IT agendas are a reality that is unlikely to go away.

We believe that institutions confronted with these challenges will have to approach their IdM plans with an eye on flexibility and agility, putting limited resources where they will do the most good. Improving data integrity, looking for small victories that demonstrate value, embracing standards, building the policy foundation for IdM, and improving senior management understanding and support will go a long way toward helping institutions achieve their IdM ambitions.

As key enabler of almost all online transactions and many desirable new services, IdM will almost certainly justify investments beyond the modest amounts we found among most of our respondents. Institutions will have to prepare the ground, however, by showing IdM's concrete benefits and ultimately by transforming virtual identity from a parochial IT concern to an institutional priority.

References

Kvavik, R. B., & Goldstein, P. (with Voloudakis, J.). (2005). *Good enough! IT Investment and business process performance in higher education* (Research Study, Vol. 4). Boulder, CO: EDUCAUSE Center for Applied Research. Available from http://www.educause.edu/ecar/

Maltz, L., DeBlois, P. B., and EDUCAUSE Current Issues Committee. (2005). Trends in current issues, Y2K–2005. *EDUCAUSE Quarterly*, *28*(2), 6–23.

Ronald Yanosky (ryanosky@educause.edu) is a Research Fellow with the EDUCAUSE Center for Applied Research.

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