Trends in
Identity & Access Management Solutions
in Higher Education Institutions

Spring 2012

Abstract

A telephone survey of higher education institutions was conducted. A variety of IT professionals were contacted at all levels within the technology organizations of willing universities and colleges. The survey focused on the drivers for IAM technologies, the challenges related to the broad application of Identity and Access Management (IAM) technologies, the satisfaction of current IAM solutions and the impact of emerging technologies on IAM. Results showed that most organizations are using single sign-on (68%), just over half are currently using password management and directory services (53% each). Provisioning / deprovisioning and federation are in use at just over a third (36% and 35% respectively). The following report is a detailed analysis of IAM technologies as they relate to college and university business drivers and challenges; strategic approaches towards IAM technologies; and the effects of emerging technologies on IAM infrastructure.

Issues

Identity management remains a top concern and focus for colleges and universities. However, the identity management software market has changed dramatically in the last few years, especially for higher education organizations. Vendor disruption has come from acquisitions and mergers creating an opportunity to innovate that emerged from the quickly advancing open technologies.

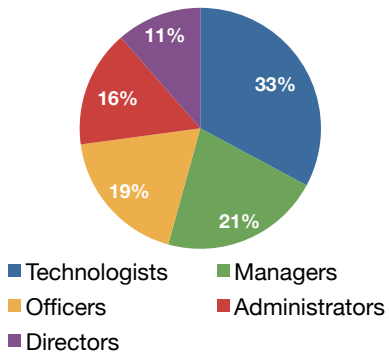
Change is also occurring in the needs to serve students, faculty and staff on college campuses. Consumerization and mobility, virtualization, cloud technologies, and privacy are all evolving issues. The legacy solutions available for managing identity, access, and directory data have been retrofitted to adapt. But new technologies are emerging with contemporary solutions to best fit those needs. So, what are the modern drivers and concerns on campuses related to identities, access, directories and the technologies that support them? This study was commissioned to understand the current state of identity management solutions, needs and gaps of today's higher education leaders.

Identity and access management technology in higher education is nearing a second decade. Early adopters have aging technology while others' home-grown solutions are taxed and proving difficult to adapt to the changing needs, especially the rapid expansion of mobilization, virtualization and cloud technologies. The purpose of this study is to discover the state of existing identity and access management solutions in higher education institutions, including how well they are meeting the needs of those campuses and whether changes are imminent.

Aegis Identity brings 8 years and over 60 implementations of identity management in the higher education market. We understand the unique requirements faced by colleges and universities, including Student/Faculty Lifecycle Management, Password Management, Federation and Single Sign On. Aegis Identity Software commissioned this survey to better understand these emerging market trends.

The survey was conducted by an independent research firm with the goal of providing insight for higher education executive level management into the trends of their peers at the dawn of an evolution in identity management practices and technology. The survey targeted all levels of the IT organization including CIOs, CISOs, Directors, Managers, Network Analysts, and System Administrators.

Profile of respondents



Survey Methodology

Overview: This survey was conducted by Michigan based IMTS, Inc. between Jan 1, 2012 and Mar 15, 2012. A total of 8,432 phone calls were placed to institutions of higher education across the United States and Canada. This outbound calling effort resulted in 165 live calls and 96 fully completed surveys.

Accurate results are presented below. In some cases, only responses considered "important" or "very important" are statistically analyzed while responses such as "no" or "don't know" are removed to illustrate more meaningful results.

Detailed survey results are available upon request to Aegis Identity Software by sending an email to info@aegisidentity.com, subject line: survey responses.

IAM Technology utilization / plans: The survey questions were organized to gain insight into the use of, or plans to implement, five key IAM technologies:

1. Single sign-on
2. Provisioning / deprovisioning
3. Federation
4. Password management
5. Directory services

Business Drivers: Respondents were asked about their implementation plans for these technologies and the business drivers motivating those plans. Seven business drivers were explored asking the respondents to indicate the degree of importance of their implementation or need to implement the technologies:

1. Speed of provisioning and deprovisioning
2. Cost containment (Help Desk / Productivity)
3. User convenience (Single sign-on)
4. Reduce complexity and increase manageability
5. Migration from obsolete or ineffective solution
6. Compliance (HIPAA, GLB Act, FERPA etc)
7. Other

Challenges: To quantify those responses related to business drivers. The survey explored the challenges to each of these drivers. Using a slightly different question to isolate consistency in the information obtained. Questions were asked related to ROI and security as well as a scale measuring the level of challenge or satisfaction that was experienced in:

1. What challenges does your organization face in pursuing identity and access management? (Lack of acceptable ROI, Lack of ownership of identity management by a Central Group, Readiness of current systems for implementation, Developing campus policies and procedures, Others)
2. How many significant security incidents related to user identification, authentication or authorization has your institution experienced in the past 2 years?
3. How challenging is it for your institution to manage passwords?

4. How challenging is it for your institution to give prompt network / email / application access to your employees, students and faculty?
5. How much do you agree with the following statement? "My institution is getting the value we expected from the money spent on identity management projects"

Institutional support, identity solution delivery, and value: The last sections of the survey asked for insight into perceived senior management and institutional support related to identity management, the institution's thoughts on delivery and acquisition of IAM technology as well as their perceived value of solutions currently being used on their campuses.

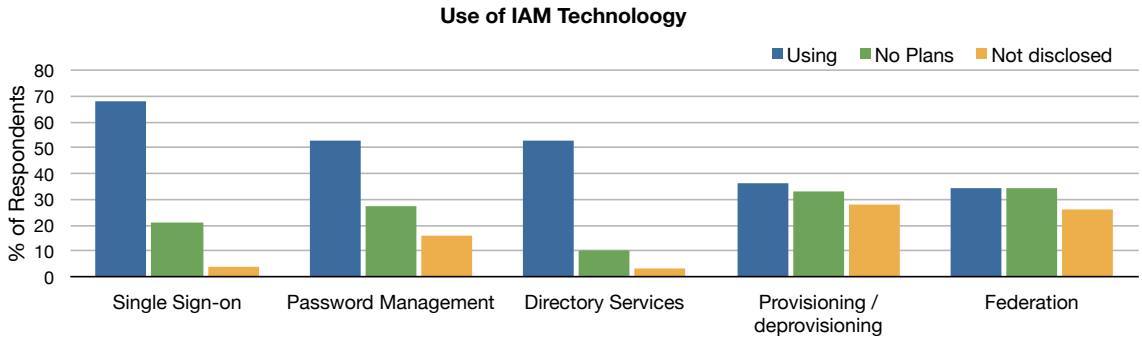
1. My institution is getting the value we expected from the money spent on identity management projects [so far]
2. My institution's senior management understands the benefits of investing in identity management.
3. My institution's senior management understands the costs of identity management.
4. My institution's senior management is willing to address the policy issues related to identity management.
5. My institution is providing the resources needed for identity management.
6. 8. Which BEST describes your institution's current thinking about identity management solutions? (Blend solutions using in-house-developed or open source software with commercially available solutions, Use Best of the Breed commercially available solutions, Use a Suite of Solutions from a Single Vendor, Use SaaS or Cloud solutions, Others)

Emerging technologies. Finally respondents were asked about the degree challenge perceived related to emerging technologies as they relate to identity and access management.

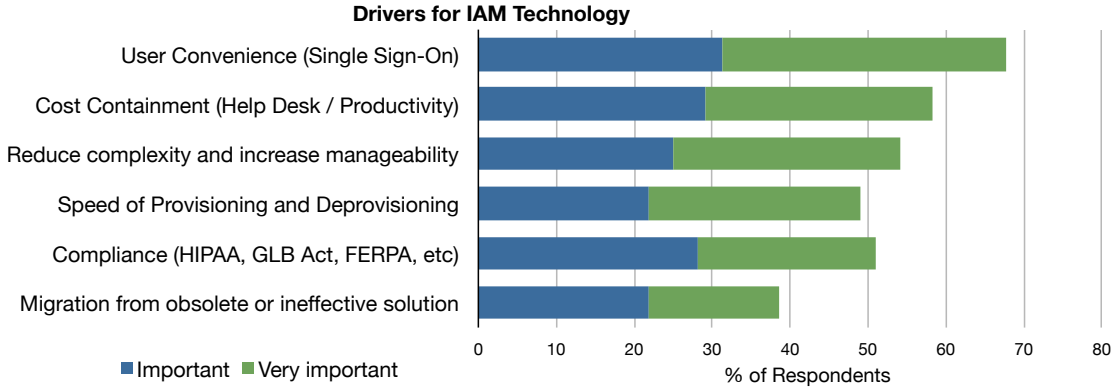
1. Cloud Access
2. Mobility
3. Social networking
4. Virtualization
5. Bring your own device

Key findings

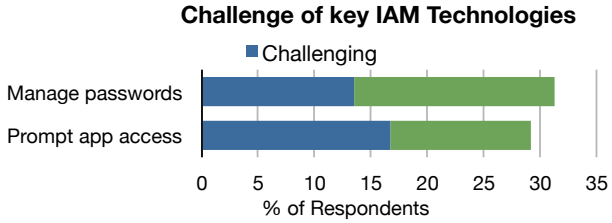
Overview. The first part of the study evaluates the state of use of identity and access management technologies and, for those using or implementing IAM the key drivers associated with the use or need to implement.



Single Sign-on is the most used IAM technology with over half of the schools already using SSO as well as password management and directory services. A minority of the schools is using provisioning and federation technologies with a third having no plans to implement them.



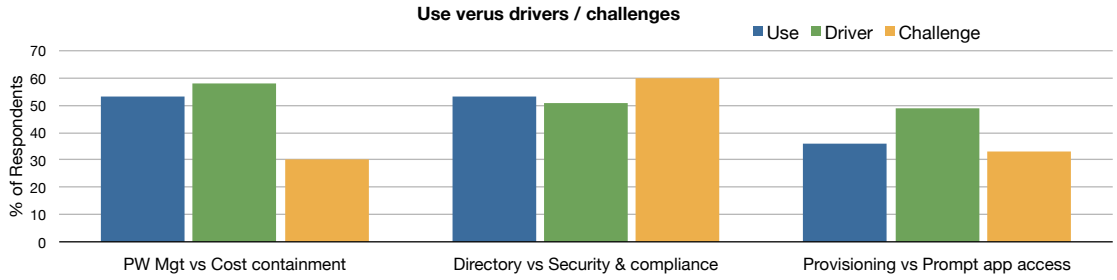
User convenience, cost containment and the reduction of complexity are the primary drivers of IAM technology. Still, compliance and speed of provisioning are drivers in nearly half of the institutions in the study while a third desire to move off of obsolete or ineffective solutions.



Managing passwords and prompt application access were challenging on a third of the campuses.

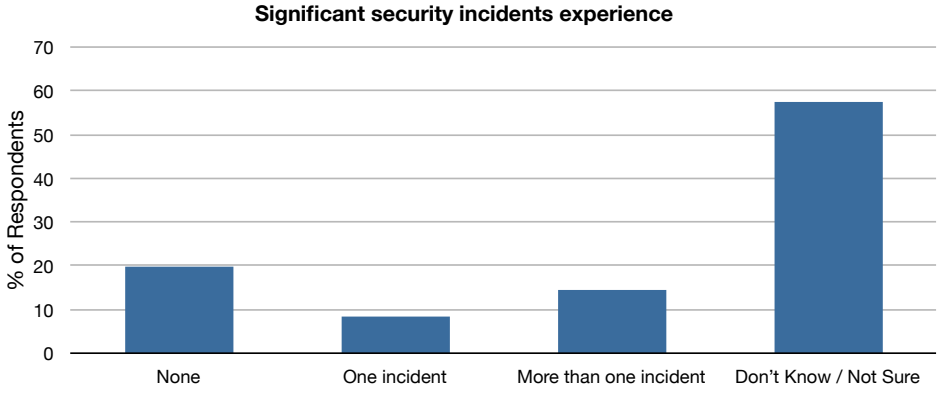
Implications. Not surprisingly, SSO and Password Management are already used in over half of the schools in the study with their chief benefits being user convenience and cost containment as the top drivers.

So why would a significant number of institutions have no plans for provisioning when almost a third find timely access to applications challenging? And why are a third of the institutions finding managing passwords challenging even though they are using some kind of password management technology?



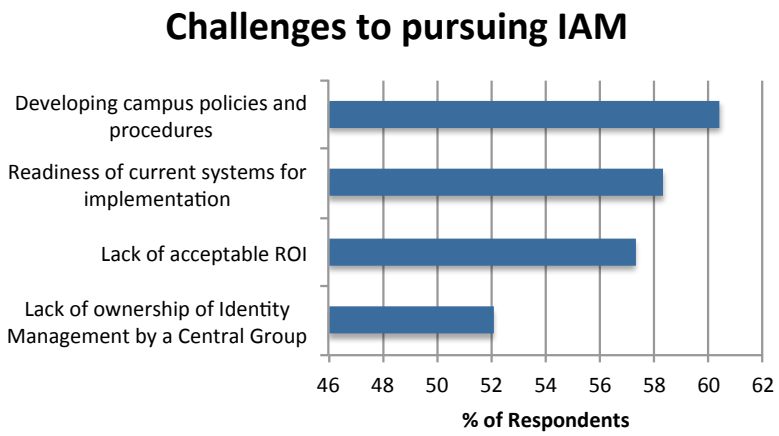
The graph above shows that fewer institutions are utilizing password management and provisioning technologies as compared to the drivers to implement those technologies (the blue graph is shorter than the green one). Furthermore the challenge associated with compliance (the orange graph associated with directory) indicates that peripheral benefits of provisioning, or more specifically, deprovisioning and password management would also be gained by implementation of these two key, but underutilized IAM technologies. Deprovisioning insures that users who should no longer have access, most importantly those with potentially threatening access, are removed from the system while a good password management solution will insure against users sharing passwords with unauthorized users.

Significant security incidents experience



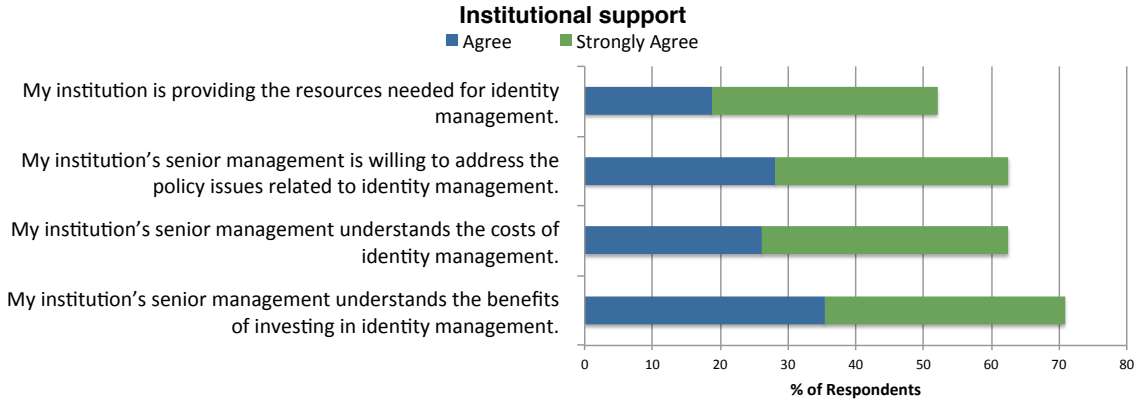
Security incidents are not insignificant in the study with 23 percent of the institutions experiencing one or more incidents and 57% not sure or unwilling to share their experience.

Challenges to the pursuit of IAM technologies



The challenges to pursuing IAM may provide some explanation as to the low adoption of provisioning and improved password management technologies. Over half of the schools found one or more of these challenges when pursuing IAM projects.

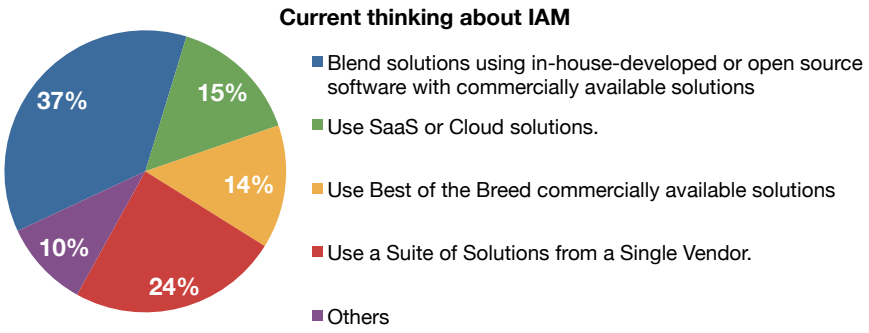
Institutional support



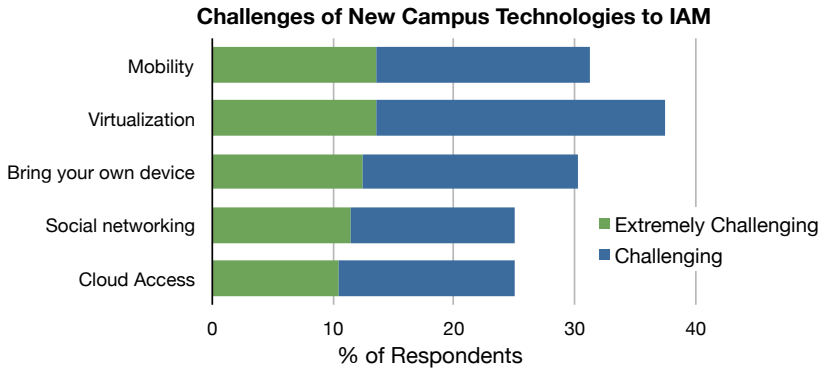
Respondents indicated that institutional support from management is not an issue with a majority responding that senior management understands the benefits and costs and have a willingness to address the policy issues. Over half felt that the resources they need are being provided.

Therefore it appears that addressing the challenges of IAM project pursuit, most specifically the establishment of campus policies and procedures, will go a long way to reaping the benefits of provisioning and password management.

Other research. The study also gives some indication into the thought leadership and new campus technologies as they relate to identity and access management on college and university campuses. The majority of institutions prefer to blend solutions with in-house developed or open source software with commercially available solutions.



Challenges of new campus technologies as they relate to IAM



Nearly 40% of schools felt that virtualization presented a challenge while a solid one-third found mobility and BYOD challenging. Clearly new technologies on campus are having an impact on IAM projects in these institutions.

Recommendations for action

Even though IAM has experienced a degree of maturity in higher education, this study demonstrates that there is an immediate need for colleges and universities to adopt available technology advancement in IAM. Specifically, there is opportunity to reap the benefits of improved security and compliance, productivity with faster access to applications for new students, faculty, and staff, and simplification of the process of password management; all in the context of new campus technologies including mobility, cloud and virtualization. Furthermore a significant number of institutions need to migrate from obsolete or ineffective solutions. These opportunities lie in the adoption and implementation of new or improved password management and provisioning technologies. Schools will have to overcome the challenges of developing the campus policies and procedures and make current systems ready. Most schools, by far, prefer to use a blend of solutions using in-house developed or open source software with commercially available solutions. Institutional and leadership support is strong to take advantage of these technologies and reap the benefits of cost containment while addressing the priorities of the campus community.