A Report on the Identity Management Summit
November 2-3, 2006
Part of the 2006 EDUCAUSE Program Plan

Norma Holland, Fellow, EDUCAUSE
Ann West, Outreach, NMI-EDIT, Michigan Technological University
Steve Worona, Director of Policy and Networking Programs, EDUCAUSE

Background

As part of the EDUCAUSE 2006 Program Plan, EDUCAUSE is holding several summits on topics of importance to higher education designed to bring together thought leaders and experts in the community in order to capture the best strategies and behaviors. The Identity Management (IdM) Summit held in Washington, D.C., in November 2006 was attended by about 50 higher education administrators who hold either an IT or functional role. Sponsored by an NSF Middleware Initiative Award to EDUCAUSE and Internet2, the Summit resulted in a collection of information from a broad higher education constituency who are knowledgeable and experienced in the area of identity management. Using this information, EDUCAUSE and partners are creating a body of knowledge to assist campuses in developing and enhancing their home IdM environments.

Definition

Identity management is an integrated system of business processes, policies, and technologies that enable organizations to facilitate and control their users' access to online applications and resources, while protecting confidential personal and business information from unauthorized users. It represents a category of interrelated solutions that are employed to administer user authentication, access and restrictions, account profiles, passwords, and other attributes supportive of users' roles/profiles on one or more applications or systems.

Speakers

Although the event was focused on discussion, a plenary speaker and a panel helped set the stage for the Summit. George Strawn, CIO, National Science Foundation, gave an overview of IdM and its important to higher education. He emphasized the need to get both IT and non-IT involved in the implementation and the necessity of a consolidated IdM environment on campus. In this model, the technology is managed centrally (commonly by IT), but the distributed authority and stewardship as well as local decision making is retained by the departments involved. In the case of a break in or service failure, policies should be instituted to clearly state who should take charge.

In addition, Strawn stated that IT has evolved from PCs replacing the mainframe, to the Internet replacing disjointed networking, to the current emphasis on information and data. Identification, authentication, and authorization all need to be in place for a trusted system, and privacy is key. Federated identity management is also gaining more use as a trusted connection by organizations needing to authenticate to external entities such as federal e-authentication and other institutions. Identity belongs to the person, not the institution; as people move among higher education institutions, can their identity move with them? This type of thinking is fairly unique to higher education, but Strawn hopes to see pilots up and running in 2007 for FastLane authentication for those involved with federal grants.

Marilyn McMillan, associate provost and CIO, New York University, moderated a panel entitled "The Importance of Identity Management to the Business of Higher Education." Panelists represented diverse communities within higher education and included Mary Anne Mahin, vice president and chief human resources officer, Georgetown University; Karl Heins, director of information technology audit services, University of California Office of the President; Andrew Shaindlin, executive director, alumni association, California Institute of Technology; and David Yeh, assistant vice president and university registrar, Cornell University. The discussion centered on how identity management affects non-IT units on campus and how they can get involved in the IdM strategy. Panelists shared their experiences and offered advice for moving ahead with IdM initiatives on campus.

From the panelists' viewpoint, IdM should be seen as a community rather than an IT issue. Awareness is key, and ensuring that non-IT personnel understand IdM's importance is critical, as they can educate others in their units and their professional associations about it. Yeh wanted to take risks in getting involved in organizational change to move the integration of IdM pilots into his unit. He stressed that department heads need to be responsible and signatory. Mahin reported that the unique ID is a benefit to users and streamlines their services on campus. Heins pushed for a central organization to manage IdM and tie it into the overall security structure for data and applications; auditors typically want to help implement these solutions and need to be involved. Shaindlain stressed the importance of including non-IT people in IdM issues; non-IT leaders must take responsibility for learning about IdM and its benefits (such as protection of donor data) and participate in strategy and prioritization rather than just sending their technical staff to meet with IT. He also suggested that IT staff avoid using technical lingo as much as possible. Both IT and functional staff need to work on the case for IdM on campus. The panelists were appreciative of the opportunity to meet with both IT and non-IT higher education staff to openly discuss IdM implementation issues on campus.

DISCUSSION SUMMARY

Patrick Sanaghan, president, Sanaghan Group, facilitated the two-day meeting and led the group through several topics for discussion.

Drivers for Identity Management

IdM is needed on campus for multiple reasons, including mitigating the risk to institutional reputation, complying with federal regulations, fostering competition with other institutions, enabling ease of use for users and efficiency of administration, customizing data and access, allowing for the portability of credentials, and establishing accountability. If an institution does not have an IdM plan, there is little or no recourse if confidential data is compromised. Benefits of IdM include encouragement of cross-breeding among departments and roles, collaboration with external agencies, coordination and integration of ERP Web applications and stand-alone applications, uniform standards for privacy and confidentiality, participation in federated identity systems, access to federal granting agencies, risk reduction, and the opportunity to offer tailored and affiliation-appropriate services from cradle to endowment. The institution must ensure the process is easy and secure and that staff and data custodians are properly trained to respond to data incidents promptly and accurately to protect intellectual property and safeguard the institution from bad PR. Institutions must quickly accommodate these needs for IdM and maintain a secure environment. Several highly publicized security breaches have highlighted awareness about the importance of IdM. Compliance drivers will require institutions to have a solid IdM infrastructure in place. The cost/benefit of implementation varies among institutions, but a PR nightmare resulting from a security breach must be considered and avoided.

Institutional Ownership/Governance

Institutional ownership must come from the top, as IdM cuts across many organizations, and requires a high-level champion who views this as an institutional priority. In many institutions a central office is responsible for IdM with collaboration of cross-functional units. Thus, the central office provides IdM services to the consumers. Boards and regencies must understand this ownership issue and establish a governance committee to ensure that IdM is implemented and maintained on campus.

Policy Considerations

IdM policy must be considered in the context of other policy issues and address privacy and institutional values. It should clarify and define roles, responsibilities, and accountability, and document guidelines and requirements. A balance of open access and security is needed in higher education. Compliance is a factor, and institutions must be held accountable. Policy must be managed within the established governance structure and enforced by executive leadership. Policy must be publicly documented with a feedback mechanism, approved, and communicated institution-wide.

Risk Management and Assessment

Institutions must undertake risk assessment and risk management in order to evaluate the impact of embarrassment, loss of trust and integrity, and financial risk. Not being adequately positioned with IdM infrastructure poses legal risks. Institutions have dealt severely with those in charge of securing sensitive data on campus when such data have been compromised.

Assessing risk is based on a cost/benefit analysis. There are costs involved in doing nothing versus being totally prepared for any incident. Thus far, campuses have not seen stringent legal sanctions imposed on them. Some feel that their risk is low, and it is difficult to quantify losses or avoiding losses. Risk management should be an ongoing exercise handled at the enterprise level with departments involved. Communication should be consistent tie into the enterprise.

Communication and Education

Communication and training are both key to achieving success with any IdM implementation. Benefits and stories from other institutions can be shared. Simple ongoing messages, free of technical jargon, are best. This should be a shared responsibility, not an IT responsibility, integrated into established channels of communication on campus. Legal counsel should be involved. Different audiences need customized messages that communicate the positives as well as the negatives aspects of IdM. Campuses might consider including IdM training as an annual requirement for users.

Implementation and Operational Issues

The foundation of IdM is the core infrastructure that must be implemented in order to make it all work. This is the technology part of the overall institutional initiative and should be based on community practices and standards to ensure interoperability, both with local applications and in federated environments. In many institutions, this is considered not very exciting and not generally seen as an institutional priority. Some motivation such as an incident or a new system might be the key to moving ahead. The campus needs to understand the negative consequences of not doing anything. Non-IT business associations can help spread the word. There needs to be a standing group of the right stakeholders to champion IdM as a priority. New systems, whether vendor (incorporate IdM standards into RFP), developed in-house, or community source, need to incorporate IdM and ensure integration with other systems.

A Business Case for Identity Management

A business case for identity management on campus needs to be made to upper administration (presidents, provosts, boards, associations, CFO, et al.). Key points in the business case should include risk mitigation (include stories from other institutions), compliance with external mandates, collaborative opportunities, and elimination of duplication of efforts and inefficiencies to ensure better services to users. The balance among security, privacy, and ease of access needs to be clear. National leaders in this area can be referenced to demonstrate the need.

This is *not* an IT issue, and the CIO alone should not be making the case. A range of stakeholders are involved, including auditors and general counsel, security officer, controller, and risk management. Some institutions bring in an external entity to explain the need. Executive summaries preceding a full discussion can be helpful.

If the reception is negative, this initiative should be started anyway, and the business case should be revised to address concerns and resubmitted. If the reception is lukewarm, then perhaps it is time to declare victory and get started. It may not necessary to wait for a response in order to get started, or perhaps all that is needed is an FYI describing what is happening. Continuous communication and follow-up on questions and concerns are critical.

Preparation, policy and business practices are needed early on in order to be ready to begin. This is the difficult part. Technology should not lead.

Next Steps

The Summit ending with EDUCAUSE asking the group for suggestions on follow-up activities, which include collecting best practices; developing brochures, articles, and presentations at various events; having non-IT people spread the word at their associations and on their campuses; forging new relationships between technical and functional staff on campus; and maintaining a listserv/blog for continuing dialogue.

Those attending the Summit described it as a valuable experience where they could concentrate exclusively on this topic in a meaningful way, engage in excellent discussions among knowledgeable colleagues, and establish relationships with others challenged by the same issues.