



How to Tackle Identity and Access Management

At many companies, when it comes to IT security, the weakest link is identity and access management.

by Sari Kalin | Mar. 15, 2006 | CIO Magazine

A chain is only as strong as its weakest link. And at many companies, when it comes to IT security, the weakest link is identity and access management. Ideally, a company would have an automated process for doling out application access—and for yanking that access once an employee leaves. Employee identities would be synchronized across all systems, and technologies would enable companies to trust the identities of suppliers, business partners and other outsiders who need secure access to their systems.

But the reality in most companies is far from ideal: Terminated employees may still have access to sensitive systems for weeks because the system admin never saw the termination e-mail from HR. Employees burdened by having to remember multiple passwords write them on sticky notes and slip them under their keyboards.

CIO Executive Council members met in August to share advice on ironing out policies and processes for identity-management projects, prioritizing their efforts and how to get funding. Here are some of their tips.

1] Make the case with hard and soft benefits. Be prepared to educate business partners about identity and access management—what it is and why it is important. "It's a very nebulous area to someone outside IT," says Bruce Metz, CIO of Thomas Jefferson University. "One challenge is to have people understand what you're trying to do. Then, the second question is, 'Why does it cost so much?'"

Members who've successfully secured funds for their identity- and access-management projects say the secret is in staying away from the nitty-gritty details of single sign-on, smart cards and other elements of security infrastructure. "Keep this from becoming a techie exercise," says Keith Glennan, VP and CTO at Northrop Grumman. "Anytime you're doing something that's essentially an infrastructure project, you have to explain clearly what you're trying to accomplish in business terms."

Steve Strout, CIO at Morris Communications, advises peers to walk through processes and rules related to identity creation and resource access before hardening those processes into code

His strategy for dealing with the [IdM Product] uncertainty: "Build processes in a standardized way." That way, if he has to move to a new technology, he'll minimize the amount of re-architecting that he needs to do.

Glennan made his case by showing that new ID-management systems would reduce IT administration and help-desk costs (by reducing the manual hassles of resetting passwords and assigning application access). Security would improve (no more sticky notes with passwords under the keyboard), and so would user productivity (since users wouldn't have to repeatedly log in to multiple systems). And Glennan points out a soft yet exceedingly important benefit: being better prepared to enforce compliance with regulations and demonstrate that compliance to Sarbanes-Oxley auditors.

2] Pilot the processes, not just the technology. CIO's who've begun identity-management efforts say that business-process issues present bigger hurdles than the technology. Steve Strout, CIO at Morris Communications, advises peers to walk through processes and rules related to identity creation and resource access before hardening those processes into code: Who is able to create, modify and view employee IDs? What is the trigger for giving a new employee (or an employee changing jobs) access to systems—and for revoking access when an employee leaves or changes roles? "We spent a lot of time walking through the logic behind why we were doing things a certain way," Strout says. His project team (which included representatives from HR, IT and finance) created a new business process: When a user successfully passes the company's mandatory drug test, it serves as the trigger for creating and then enabling systems access.

3] Plan on customization. To achieve the full benefits of ID- and access-management tools, Strout says, most IS shops will have to do some customization, especially if they want to enable automated provisioning and single sign-on to legacy systems, homegrown apps, software from small startup companies and other nonstandardized systems. "The security designs aren't necessarily the same, so you just have to tackle each one as they are," Strout says. In some cases, it may not be cost-effective to do automated provisioning to a nonstandardized system, especially if it has few users; it could make more sense simply to generate an automatic e-mail to an admin requesting systems access and have the admin manually fulfill the request.

4] Protect yourself against industry consolidation. While Strout was evaluating vendors for his identity-management initiative, the industry consolidated right before his eyes. Netegrity was bought late last year by Computer Associates. And earlier this year, after Strout had committed to buying an identity-management suite from Oblix, Oblix was bought by Oracle. "We're predominantly a Microsoft shop," Strout says, and he wonders if future iterations of the Oblix ID-management suite will remain Microsoft-friendly.

His strategy for dealing with the uncertainty: "Build processes in a standardized way." That way, if he has to move to a new technology, he'll minimize the amount of re-architecting that he needs to do.

Logic Trends, Inc.

Atlanta

1050 Crown Pointe Pkwy
Suite 1580
Atlanta GA 30338

office: 770.551-5050
fax: 770.551.5055
info@logictrends.com

Branch Offices:

- ❖ Tampa
- ❖ Cleveland
- ❖ Dallas

