Nelson Cicchitto

THE 10 PHASES OF IDENTITY AND ACCESS MANAGEMENT

As one of the fastest growing industries, gaming & hospitality organizations rely on technology solutions that can keep pace with the speed of business and rely on information technology infrastructure for the delivery of positive customer and employee experiences. This makes automating identity management (IdM) - the processes for creating, maintaining and deleting user IDs, passwords and privileges - essential to a successful gaming enterprise. By automating identity management, gaming organizations will save money, enhance operational efficiency, better manage risk and ensure compliance with internal and external regulatory requirements.

While most large organizations have begun implementing IAM projects, few have fully deployed IAM across the enterprise nor have they deployed IAM at its most advanced capabilities. IAM has ten stages, or layers, of capabilities that can be successively deployed. Most companies attempt to implement several phases at once with limited success or complete failure.

Ten Stages of IAM Deployment

What, exactly, does identity and access management entail? Identity management involves administration and policy creation, while access management entails enforcement of those policies. Together, IAM is a hierarchical collection of security practices and technologies, each new stage building on the prior one. The ten phases of IAM are:

Phase 1: Password Management

It's an oft-quoted fact that 30% of all helpdesk calls involve password problems. So the first phase of IAM is aimed at automating that 30% of calls. This first stage is password management -- an automated solution for managing password assignment and resetting passwords via phone or desktop. It enables users and customers to do limited self-service management of their accounts without bothering IT. For instance, they can reset passwords if they've forgotten them or as passwords expire. Because a password management system is fairly easy to cost justify to a CEO (that 30% reduction in help desk calls translates into hard payroll dollars), it represents the "low hanging fruit" of IAM and should be implemented before moving on to other phases.

Phase 2: Password Policy Enforcement

Every organization needs security rules, including rules about how passwords may be created, used, reset, and so forth. In phase two, you need to create policies that will protect passwords from being stolen or guessed by outsiders, but which don't over-burden users. An automated policy manager will enforce those password policies, for instance by not allowing a user to put his user name as the password, or create a password of less than seven letters, or use common words and names. Easy-to-guess passwords are extremely vulnerable to exploitation by outside thieves, so ensuring the enforcement of corporate security rules is critical to network security.

Phase 3: User De-Provisioning

Once you've got password management and password policy enforcement in place, you're now in a position to move up to a de-provisioning solution. De-provisioning is much more than simply pulling the plug on a user ID. It involves terminating access to multiple accounts across various systems, archiving mailboxes and directories that may be required in case of an audit, and deleting the account from the system. It eats up time the IT staff could use for other projects and, conversely, if left undone exposes the system to access by disgruntled ex-employees. Automating the de-provisioning process increases security, takes one more administrative burden off of the IT department's shoulders, and complies with accepted best practices in the gaming industry.

Phase 4: User Provisioning

This involves the automating of account creation across multiple systems and platforms. It's a big step up on the ladder, because this is the first stage that requires you to define user naming conventions, roles for employees, and what levels of access to various systems each role requires. However, the benefits of automating this level are significant, because once you've defined the roles, you no longer have to manually provision each new employee. You can simply assign them a role or job code and the provisioning software will handle the rest. No more guessing if the new HR assistant is supposed to be able access individual payroll information or not, or trying to remember which printer is closest to the new persons' desk. Conversely, some products allow you to simply select and copy a source user to a target account. For organizations that cannot afford to reap the benefits of User Provisioning and do not have the time to define roles, this option works well.

Phase 5: Self-Service Role Matrix and Rights Management

This stage is even more dependant upon systems your organization must have in place prior to deploying this type of solution. In this phase the concept of automated self-service password management is taken one step further, to enable your end users to request access to specific systems and accounts and have the authorization handled automatically by a predetermined workflow. For instance, an assistant accounting representative might submit a request for access to a sensitive system such as payroll, or to certain restricted functions such as the ability to change data or tables. The employee request is then forwarded, based on the preconfigured workflow, to managers authorized to approve such access. This also enables new employees to self-provision themselves, by inputting their name and job code and getting the necessary approvals to access whatever systems are part of his or her job code. Existing employees also benefit because they will have a self-service method for updating their employee contact info.

However, this phase is impossible to achieve without an organizational chart, defined roles, and for some products a high level workflow design in place prior to rollout.

Phase 6: Metadirectory

Many organizations believe they need a single directory that contains identities of all of their disparate directories. Metadirectory is, as it sounds, a combined directory of the metadata on all enterprise data located on all of the organizations' servers. It sounds like this phase could be fairly automated, however that is far from the truth. To bring all of these identities together on a scheduled basis requires someone to manually check identity mappings of critical identities as well as monitor the automated process. For very large environments with and several unique identity repositories this technology does not scale well.

Phase 7: Enterprise Reduced Single Sign-On (SSO)

From a user perspective, it's considerably more convenient to sign on just once for access to all applications and databases, rather than having to log on to each system separately. Enterprise reduced SSO is a phase that can help boost user productivity by reducing security-related tasks. But just like the prior phases, this phase requires even more preparation by your organization before it can be successfully deployed. Prior to deploying any SSO technology you must identity the app you want to enable, record the logon process of each app, test SSO, determine who you should distribute the app to, and maintain the SSO process as interfaces to web apps change. Additionally, it is best to rollout SSO applications from the easiest to most difficult. The easiest apps includes recording the logon macros for your internal web applications; next easiest application to tackle are your external web applications (such as Expedia, Partner sites, and other web sites); moving on the third is to automate your Windows 32-bit applications; and fourth phase requires automating legacy or java applications.

Phase 8: Authentication Services

For highly security conscious organizations, authentication is a key element of identity and access management. As the traditional "Who you are, what you know and what you have" saying illustrates, a user ID and password are only two of three possible ways to make sure the correct person is gaining access. The third, required along with the first two, is some hardware element – a smart card or dongle or VPN—that determines which applications will be accessible to you. Many organizations never get this far up the security ladder, and many don't need to. However, if you do decide to implement this phase be prepared for even more planning and a disruptive change to existing authentication procedures.

The 10 Phases of Identity and Access Management

Phase 1:
Password Management

Phase 2:
Password Policy Enforcement

Phase 3:
User De-Provisioning

Phase 4:
User Provisioning

Phase 5:
Self-Service Role Matrix and Rights Management

Phase 6:
Metadirectory

Phase 7:
Enterprise Reduced Single Sign-On (SSO)

Phase 8:
Authentication Services

Phase 9:
Enterprise Access Management

Phase 10:
Federated Identity Management

Phase 9: Enterprise Access Management

Enabling restricted access to web applications is the primary goal at this phase. In this phase you must identify which web apps and end users you want to provide restricted access to, enable those apps, test restricted access, monitor access of resources, and distribute the restrictions to end users.

Phase 10, Federated Identity Management

Few organizations have implemented the last phase, federated identity management. Like phase 6, the majority of firms don't really need this phase for better security or work efficiencies, and it can be both expensive and problematic to implement.

Federated identity management gives users the ability to log onto one network and be able to then access all trusted networks. While all of the prior phases of IAM provide elements of federated management, full federated identity management also entails access to networks of trusted partners, and their access to your network. The complexity of enabling partners to access internal systems is enormous. It requires not only technology for ensuring secure and automated access by outsiders, but also requires negotiation and agreement between the two organizations first. There are liability issues to be considered, contracts that must be drafted, and, finally, the technical details how the partners will access systems, what level of access they will be granted, and what their responsibilities are in the event an employee loses a password, leaves the firm, etc. For most organizations full federated identity management is unnecessary. However, for those that engage in constant data exchanges with highly trusted partners, it may become a necessity.

The Long-Term View

Labor intensive, high turnover industries like gaming are ideal candidates for automated identity management. The ability to securely and efficiently automate the management of user identities is a "must have" to reduce costs, increase operational efficiency, manage risk and achieve regulatory compliance. Regardless of whatever IAM phase your organization happens to be at, the long-term strategy should be to regularly evaluate your security needs and decide how well the current IAM technologies are meeting those needs.

Nelson A. Cicchitto, a career information technology leader, joined Avatier Corporation in 1995 as chairman and CEO. He has over 20 years of experience setting information technology for fortune 100 companies such as Chevron and Pacific Bell.