



Making Identity Management Work in Your Organization

By E. Eugene Schultz – ISSA member, Los Angeles, CA, USA chapter

This paper describes some of the most significant considerations regarding planning for and implementing identity technology solutions and presents recommendations for approaches and strategies if an identity management effort is to succeed.

Identity management is a wide-ranging administrative area concerned with identifying individuals needing to access systems or applications, controlling user access to system and information resources by assigning user rights in connection with each user identity, and auditing every access to every resource to ensure user accountability. Identity management systems (IDMSs) automate identity management functions such as password reset, password synchronization, single sign-on functionality, access management, provisioning (e.g., for expired passwords), portal services that provide a common, convenient way for users to access applications and other resources, and centralized audit functionality.

Identity management technology is rapidly growing in popularity, due in large part to the fact that this technology offers such a broad range of significant benefits. At a high level, identity management technology typically boosts efficiency within the IT arena by simplifying user tasks such as obtaining and changing passwords, thereby cutting help desk-related and other costs significantly. Additionally, this technology

generally improves data access security and mitigates fraud-related risk. From a more detailed perspective, typical identity management products allow for control of multiple user accounts and access to numerous applications, databases, and so on, provide secure access to information and applications no matter where within a network they are located, provide a consistent strength of authentication and authorization, deliver portal services to users, and make monitoring and accountability easier through centralization.

Despite the many advantages the technology potentially offers, getting identity management efforts to actually work within an organization, particularly within a large enterprise, is often much more difficult than it might superficially seem. Why? This paper describes some of the most significant considerations regarding planning for and implementing identity technology solutions and presents recommendations for approaches and strategies if an identity management effort is to succeed.

Consideration 1

Understanding the nature and purpose

The most fundamental considerations with respect to identity management are understanding what identity management really is, the types of business needs identity management solutions are capable (and not capable) of meeting, and the degree to which these solutions can meet these needs. Among the most important of these considerations is comprehending if, how, and to what degree identity management solutions can meet critical business needs. I fear that too many people become so enamored with identity management technology that they become determined to implement it without understanding how this technology relates to the business interests that information security is supposed to serve. Strengthening identification, authentication, authorization and auditability for the sake of improving security may superficially make sense, but security for security's sake does not. Information security must align with business drivers if it is to contribute genuine value. Information security professionals would be well-advised to heed the lessons learned from dealing with public key infrastructure (PKI) technology, a technology that has faltered because in large part it too often has been embraced and deployed independently of its relationship to business drivers.

Another important up front consideration is achieving a genuine understanding of the fundamental difference between identity management and identity management technology (as exemplified by identity management systems). Identity management includes identification, authentication, authorization, and accountability throughout an entire organization. Technology is almost always an important part of identity management efforts, but equating identity management with identity management technology is a huge misconception. No form of technical control in and of itself comprises a security control.¹ Identity management controls may include identity management technology, but they must also include provisions in information security policy and standards that state and communicate requirements relevant to the scope of identity management controls, baseline technology standards, ownership, roles and responsibilities, and more. Procedural controls that govern matters such as patching and updating IDMSs, safeguarding of sensitive information that IDMSs may store, inspection of audit log data, and so on are also necessary.

Finally, it is important to realize that an identity management effort is good only to the degree that the resulting mechanisms and processes are pervasive. An identity management effort must ideally affect every access to every system, network, application and database – with no exceptions. The more uniformly and universally identity management works, the more effective in terms of both control value and cost effectiveness it is. To put this another way, the more exceptions

An identity management effort must ideally affect every access to every system, network, application and database – with no exceptions.

and exclusions in identity management there are, the more avenues of exploitation and problems that require intervention by technical staff there are likely to be.

Consideration 2

Proper planning

The scope of identity management (including the identity management technology used) is usually so far reaching and broad that developing a strategy or an architecture that specifies the major elements (both technical and non-technical) that will be involved is also necessary. For example, Windley argues that an identity management architecture that includes a process architecture, data architecture, and technical reference architecture, all of which fall within interoperability and policy boundaries constraints, needs to be developed.²

Finally, planning for ways to measure the success of an identity management effort needs to begin early in such an effort. One of the most important steps in this endeavor is developing suitable metrics and discussing them with senior management and the information security steering committee to ensure that there is agreement and buy-in. Among the metrics that can be used to demonstrate the worth of identity management are:

- Time and costs related to creating, deleting, or suspending user accounts
- Help desk costs related to user authentication and authorization problems
- Time needed to inspect and evaluate user access records and associated costs
- Costs of security incidents in which authentication or authorization controls have been circumvented or defeated

Consideration 3

Developing suitable requirements

Developing requirements is one of the most important considerations in any project, and identity management is by no means an exception. Matching identity management requirements to business needs is the most important part of requirements formulation. Keeping abreast of current and soon-to-be-initiated business initiatives is thus essential. If,

¹ Information Systems Audit and Control Association, *CISM Review Manual 2008* (Rolling Meadows, IL: Information Systems Audit and Control Association, 2008).

² P. Windley, *Identity Management Architectures and Digital Identity* (Sebastapol, CA: O'Reilly, 2005).

Scalability is a “sleeper” waiting to rear its ugly head.

for example, several new business applications that require high strength of authentication but little effort on the part of users are being implemented, identity management requirements should be gauged accordingly.

The requirements phase will almost inevitably include requirements for selecting an identity management product. Typical requirements such as cost, functionality (especially when it comes to identification, authentication, authorization, and auditability functions), stability, impact on ongoing operations, quantity and quality of documentation, vendor reputation, responsiveness, and reliability, and more need to be included. However, three requirements, *usability*, *scalability*, *compatibility* with the existing IT environment, and *complexity* are particularly important in the identity management arena in that they can and do “make or break” identity management efforts within organizations.

Usability

Usability is so critical that without adequate levels of it, user resistance can easily doom an identity management effort to failure. Although virtually every vendor claims that its product is extremely “user friendly,” some IDMS products are far superior to others in this regard. Carefully formulating usability requirements and assigning extra weight to them is thus imperative.

Scalability

Scalability means ability of an IDMS product to work regardless of the extensiveness of the environment in which it is implemented. This requirement is in many respects a “sleeper,” one waiting to rear its ugly head at a later point in time if those who are drafting IDMS requirements are not aware of just how critical it is. Many IDMS products have very obvious scalability limits. They work just fine when they are deployed in settings in which there is a limited number of users and in which only one or two networks that are reasonably physically proximal to each other exist, but do not work well when there are many users and applications, and when there is a huge enterprise network that spans massive physical distances. Other products work well in traditional network environments but break down in others such as wireless network environments. Weird and disruptive breakdowns such as failure to apply changed entitlements to subsequent resource access attempts, user authentication failures due to timeouts not caused by users, and failures of password changes to “take” can and do occur when a product’s scalability limits are exceeded. It is thus extremely essential to ensure that scalability requirements are included and also that they are weighted disproportionately.

Compatibility with existing IT environment

Because the pervasiveness of identity management is so critical, compatibility with the existing IT environment is yet another “show stopper” requirement in identity management. Your organization should not have to make extensive modifications to its business processes and IT infrastructure when identity management solutions are rolled out. Given the fact that almost every IT environment lacks a certain amount of orderliness and uniformity, however, meeting this requirement is often the most difficult of all. Diverse operating system platforms, applications, network devices, and so on are a reality in IT environments today, something that makes compatibility of identity management technology with these environments an even greater challenge. In general, the more a product is compatible with the range of technology, especially the most critical technology from a business perspective, the more desirable that product is.

Compatibility of IDMS products with existing authentication and name space schemes is a very critical consideration. Some IT environments use LDAP, others use Kerberos, and still others depend on other protocols. Still, there may be some points of compatibility between seemingly incompatible protocols. A Kerberos Key Distribution Center (KDC) can, for example, be made to use LDAP for storing its data.

Compatibility with applications is yet another potentially huge problem. No single IDMS product of which I am aware is compatible with every existing application, nor is any such product ever likely to be. In general, the greater the degree of compatibility of IDMS products with existing applications, the more suitable that product is.

Complexity

Finally, it is important to realize that some of today’s identity management technology are extremely complex to the point that they are downright difficult to properly install, configure, and maintain. Ease of maintenance is particularly important – a few IDMS products require gargantuan amounts of personnel time and effort to properly maintain. At the same time, however, identity management technology that offers more functionality is by nature more complex, so viewing complexity in terms of cost versus benefits is a more realistic approach. Identity management technology that is unnecessarily complex can readily become an “orphan” technology within an organization, so considering complexity during requirements formulation is also especially significant.

Consideration 4

Selecting an IDM product

The preponderance of identity management efforts requires choosing an identity management product. A few organizations have developed in-house identity management software, but there are usually substantial limitations (particularly in terms of cost overruns and failure to sufficiently meet requirements) associated with such efforts. The require-

Viewing complexity in terms of cost versus benefits is a more realistic approach.

ments criteria discussed in the previous section should be matched to the capabilities of each candidate product, with extra weight assigned to usability, scalability, compatibility, and complexity.

In theory, the selection process for identity management products should be basically the same as for selecting any other product. In reality this is not quite true, however, because when candidate products are selected for in-house trial evaluations, it is not feasible to test them very completely against certain requirements criteria. Consider scalability, for example. A valid and robust test of scalability would require testing a candidate product with more and more users and applications to determine the so-called scalability limit for that product. Involving tens of thousands of users and hundreds of applications in a scalability test is by no means practical. The result is that organizations are instead likely to be forced to turn to testimonials by individuals from organizations that have used the product in question. Unfortunately, vendors almost always provide the names of customers who are satisfied with the products they sell and omit the names of dissatisfied customers. Consequently, it may not be possible to obtain valid information about an IDMS product's scalability. The same applies to compatibility.

Finally, during the selection phase a considerable amount of usability testing involving a diverse sample of users needs to be conducted. All that glitters is not gold, and many flashy user interfaces in IDMS products (as well as other products) are in reality deficient in terms of their usability. Given that identity management solutions must be as pervasive as possible if they are to be successful, determining the real degree of usability that each candidate product offers is essential.

Consideration 5 Implementation

As with anything else, planning comprises a critical path on the road to success, and planning for implementing an identity management solution or project is no exception. One of the keys to success is testing all aspects of the identity management solution that has been chosen in a non-production environment before it is implemented in the production environment. A phased implementation, one in which only a certain percentage of users and applications are migrated to the identity management solution that has been selected at any one time, is also imperative because it greatly lessens any negative operational impact that may result.

Certain aspects of implementation are likely to be especially difficult, and integrating applications into an identity management solution is likely to be one of them. I recommend

devoting a considerable amount of effort to identifying the interfaces that each application supports, and then determining the types of integration protocols and services (such as LDAP) that work in connection with each interface. Some applications are likely to be incompatible with the selected IDMS; in these cases attempting to at least include these application's identity information in a common directory or exploring other, more generic integration methods may be the best available solution.

The operational phase

Once an identity management solution has been implemented, the next phase is operations, something that involves both technical procedures (making regular backups, inspecting and verifying settings, installing vendor-supplied patches and upgrades, and so on) and updating and expending administrative/procedural elements. Ensuring that resources necessary for the operational phase are available and that the operational procedures that are in place are being carefully followed are two of the most important considerations during this phase. Additionally, metrics must be measured and communicated to entities such as senior management and the information security steering committee during this phase.

Conclusion

The future of identity management technology looks very bright. At the same time, however, planning for, implementing, and maintaining this technology are often not anywhere as easy as it might seem. Putting into practice the principles and recommendations presented in this paper can make the difference between success and failure.

A final thought concerns weak links in identity management technology. One thing that should greatly concern information security professionals is the fact that today's IDMSs generally have much to offer in terms of security-related functionality, yet they sometimes have security-related limitations that negate much of the value of this functionality. Some IDMSs, for example, work only in connection with static password-based authentication, a form of authentication that has over the years proven itself to be severely deficient. Identifying weak links early in the identity management life cycle and avoiding them or at least working around them to the maximum degree possible is thus also critical.

About the Author

Eugene Schultz, Ph.D., CISM, CISSP, is the Chief Technology Officer and Chief Information Security Officer at High Tower Software, a company that develops security information and event management software. He has written/co-written five books and over 120 published papers and is an associate editor of three information security journals. He is a member of the ISSA Hall of Fame can be reached at eeschultz@sbcglobal.net.

