realtimepublishers.com™

The Definitive Guide™ To

Identity Management

Archie Reed

Copyright Statement

Chapter 6: Identity Management Technologies and Trends

Welcome to the final chapter of *The Definitive Guide to Identity Management*. Before we dive into this chapter, let's review what we've covered so far:

- In Chapter 1, we defined the who, what, where, and when of Identity Management and briefly explored Identity Management standards.
- Chapter 2 began to delve deeper into the components required and available to support an Identity Management initiative, focusing on how Identity Management can help meet most organization's key security requirements.
- By Chapter 3, we had established a common vocabulary and baseline understanding of Identity Management components and concepts, so we moved on to explore Identity Management applications.
- This discussion led smoothly into Chapter 4, which covered Identity Management implementation. As a result of the new and rapidly evolving Identity Management market, there is much flexibility in the terms that vendors use to market their solutions. In this chapter, I discussed how this scope affects the requirements of Identity Management implementations, which will be unique to each organization.
- And in Chapter 5, we built on the foundation of Identity Management standards information that we laid in Chapter 1, focusing on which standards will solve the challenges of your organizations' environment.

This final chapter is intended to provide an overview of the some of the current Identity Management vendors and the technologies they have to offer and are developing. In addition, this chapter provides a concise list of organizations that specialize in the Identity Management space—in particular those organizations that are independent and can help you define and realize the right Identity Management solutions and implementation timelines for your organization.

In this chapter, I'll also explore the trends of the Identity Management market, including likely trajectories and intersections with other technologies. Hopefully, this information will give you insights into the future of the Identity Management market that will help in planning your Identity Management solution. We'll start by exploring the benefits of Identity Management consultants.

Consultants

Although organizations are working to develop standards within the Identity Management space, as we explored in Chapter 5, there is much legacy and proprietary technology still in use and being deployed. This technology makes it a challenge to attempt to integrate the potential Identity Management capabilities available and ensures that such a task is tricky to accomplish without some degree of difficulty. One way to work around this challenge is through consultancy services that are not new to the Identity Management market. Through their expertise and understanding of Identity Management, consultants can assist your organization in rapidly deploying your Identity Management solutions.

Consulting around Identity Management has boomed over the past couple of years and will continue to do so as the industry strengthens and matures. Most IT consulting companies have either established an Identity Management practice or have consultants with specific skills in this area.

Determining which consulting organization to work with during an Identity Management planning and/or deployment exercise is an important task, and, as I stated in Chapter 3, is usually necessary unless you have experienced people on staff. Some companies are very good at assisting you in setting strategy, documenting requirements, and developing business cases to help in the early phases of a project. Others are very good at managing an Identity Management project and/or carrying out the deployment work. Many can carry out both the strategic and deployment functions.

Be aware that many of the specialist companies have strategic partnerships with certain vendors that might influence their product choices. However, this very fact can work to your benefit if you have already chosen a vendor product and want highly skilled expertise focused on that product.

Professional Services

As I've mentioned in previous chapters, careful planning is vital to an Identity Management solution deployment. Developing a comprehensive strategy to evolve your company's Identity Management infrastructure, procedures, and policies will help to ensure that each part of an implementation exists within an overall plan. Some of the well-known companies that offer specialist Identity Management practices include ePresence, Burton Group, PricewaterhouseCoopers, and Deloitte Touche Tohmatsu.

ePresence is an interesting company that originally started out as Banyan Systems. Banyan produced one of the first commercial directory-based OSs. Banyan's gradual disappearance from the OS marketplace had very little to do with the quality of its product (it was a good product) and had a lot to with market penetration and competition from Novell, Microsoft, and Microsoft licensees'. Banyan's senior management team decided to turn its company into specialists in the directory consultancy market and have morphed into the Identity Management market. The company's original staff of highly skilled directory experts has been expanded to include project managers, architects, and people with hands-on skills across a broad range of Identity Management products.

Infrastructure Help

Novell seems to moving in a similar direction to ePresence. Novell have a very good directory product in eDirectory, and through the fairly recent merge with Cambridge Associates, Novell employs a valuable army of consultants. Novell has accepted that directories are commodity products—plumbing for value-added products and services, so it often offers eDirectory as a giveaway. The company is now focusing on meta directory, security, provisioning, and other Identity Management–related products to provide a revenue stream. This effort coupled with the professional services the company can now offer should ensure Novell's survival in the Identity Management arena for some time.

Microsoft seems to have taken an infrastructure-only approach. Having delivered AD as a core service in Win2K Server, Microsoft then obtained meta directory technology through the acquisition of Zoomit, which Microsoft now sells as Microsoft Metadirectory Server (MMS). As I discussed in the Identity Management components section of Chapter 1, Microsoft has so far taken a similar strategy with Critical Path, focusing on core infrastructure components upon which organizations can build their own applications and user interfaces (UIs). In addition, Microsoft offers many extra tools and infrastructure components from which to build solutions, such as Visual Studio, Internet Information Server (IIS), and so forth. Microsoft has recognized that Identity Management, especially at the infrastructure stage, requires expertise, and as a result Microsoft Consulting Services are almost mandated when an organization wants to deploy MMS.

The Risk Management Factor

Many consultancies such as PricewaterhouseCoopers and Deloitte Touche and Tohmatsu have arrived at the Identity Management market as part of their risk management or security practices. This evolution is an important intersection which resonates well with Identity Management. In fact, many other organizations have internal risk management—in particular, but not exclusively, financial, medical, health, and manufacturing organizations.

Risk management embraces many strategic, operational, and process components of an organization. Risk management is about trying to eliminate or mitigate potential risks in and to the organization through planning and the deployment of systems and processes. Many of the organizations that come from the risk management background have extensive experience in the risk vs. reward–type scenarios that you will face when looking at the Identity Management market. Remember that although it might seem that your environment grows more secure the more security processes and technology you put in place, there is the risk that you will develop a solution that is too complex to use or too complex to identify possible methods of failure or intrusion.

> ☞ If your organization has an existing risk management team, it would help a great deal if they were identified as a stakeholder in any Identity Management initiative. The experience of risk management teams is not only in identifying risks and in clarifying which are the most important risks to be dealt with, but also in which risks are not very important at all.

The key point to take away from this section is that, for many organizations, an Identity Management solution is part of the resolution of many issues—risk management being another part. The challenges faced by many organizations might be larger than an Identity Management initiative can immediately solve, although Identity Management might form part of the solution.

Solution Vendors

There is a category of consultants called solution vendors. These are vendors of Identity Management–related products that provide professional services that can help you plan and deploy their products into your organization. Some solution vendors might go beyond this scope and help provide general Identity Management strategy guidance as well. Some of the larger solution vendors include IBM, Computer Associates, Sun Microsystems, and Novell, though most of the vendors mentioned in Chapter 3 have some form of professional services and/or consultants available. Consultants who work for solution vendors or trained partners and resellers often have very detailed knowledge of the vendor's products. Although many Identity Management solutions are becoming more integrated and easier to install, the expertise of solution vendors' consultants is still close to a requirement for installing these products. These consultants can help you avoid problems that arise as a result of the complex integration issues across other back-end systems.

To increase exposure and market penetration, many of the vendors have set up strategic relationships with some of the larger consulting firms. Access360, Business Layers, Netegrity, Critical Path, OpenNetwork, and several others have a partnership with ePresence. Vendors such as Oblix, Novell, Sun Microsystems, Waveset Technologies, and BMC Software have a partnership with PricewaterhouseCoopers. These types of relationships help to increase the number of consultants and support personnel that have skills in the Identity Management arena and with specific Identity Management products. In addition, these relationships allow companies that are deploying Identity Management solutions to use consultants with expert knowledge in the Identity Management field and make a choice from multiple products to meet their needs.

Emerging Identity Management–Related Issues

Aside from the consolidation of specific Identity Management functionality that we explored in Chapter 1, the following areas will become more prevalent in the Identity Management market over the next few years. These areas will increasingly become more significant to Identity Management as time progresses:

- Federated identity
- Contexts-sensitive Identity Management
- Identity theft
- Intrusion detection
- Intellectual property management
- Content and digital rights management
- Regulatory and compliance issues
- Identity Management appliances
- Advanced biometric applications

This list highlights the areas of focus that Identity Management solutions will continue to move toward and envelop as well as help drive the development of.

Federated Identity

We have discussed federated identity several times throughout this book, and its importance has led me to include it again in this section. Although federated identity is a definite trend, there has been minimal interaction with the existing infrastructure and solutions already established to support X.509 certificates. The model used for X.509 is based on the X.500 directory model, wherein there is a top-down, mandated structure for information authorities. It appears to many that solutions based on SAML or Microsoft's .NET Passport will avoid much of the complexity of solutions such as X.509. However, both SAML and .NET Passport, as well as similar efforts, will need to be evolved to meet more general requirements as more commercial implementations are made.

This situation is akin to that of LDAP and X.500. X.500 was planned as an all-encompassing, world-wide, solve-everything directory standard; whereas, LDAP was planned as a simple solution that would meet the needs of a small environment (such that it could be quickly implemented and easily used). Although X.500 found favor with large organizations and many national and educational institutions, it did not have widespread commercial adoption. LDAP, however, being quick and easy to implement and, more importantly, designed to work on the Internet-standard TCP/IP protocols, had rapid commercial adoption. As LDAP became more widely used, implementers found many deficiencies, such as limitations with data distribution or replication, large-scale data management, and so forth. Interestingly, all these issues were dealt with in the X.500 standard. This situation parallels that of federated identity—although one solution is less complex, that simplicity comes at the cost of functionality. Sometimes the best and most complete solution isn't necessarily the most popular. As federated identity solutions evolve and replace existing solutions, they might not address every issue but instead will offer enough functionality to allow organizations to move forward with their implementations.

Challenges to Federated Identity

On the privacy front, federation faces many challenges. A major consideration is the complex relationship between federated identity and legality. The sharing of information between organizations may be governed by local or national laws or international agreements. The issue is compounded when laws contradict each other about what information can be shared. Since its launch in 1999, .NET Passport has been under much scrutiny from public and private organizations. For example, from .NET Passport's launch through 2001, the Electronic Privacy Information Center (EPIC) along with numerous other consumer advocacy groups raised privacy issues with the United States Federal Trade Commission (FTC) concerning .NET Passport, which in turn led to the FTC to investigate .NET Passport. The European Commission has asked similar questions about .NET Passport. Most issues focus on the following concerns:

- Unclear privacy policies that make it difficult to determine what will happen to personal data once it is provided
- The process of securing the collection and storage of personal information
- Particular concern about protection of data relating to children
- Potential transfer of personal data beyond organizations with which a relationship was established
- Potential transfer of personal data across state or national borders, potentially breaking established laws either locally or internationally
- The lack of ability to delete an account

Much work has been done to deal with the policy issues, making them clearer and more restrictive about how personal data is handled.

This factor is an important consideration if you plan to do business with international partners or customers, whether they are other organizations or individuals. It is in situations like these in which an organization that has already worked through these issues becomes valuable. The effort that Microsoft is putting into .NET Passport is one example of an organization that is attempting to find a balance between the benefits of federated identity and legality. Visa, Master Card, and American Express also provide a model wherein these issues have been dealt with, such that the correct and legal exchange of identity information can occur. These companies have established a trusted network in which to exchange information and a formal membership model for the distribution and usage of credit cards as the identifier for undertaking transactions. The trend with federated identity will be based on these models. A company known as PingID provides a new version of these models specifically for the use of identity in federated environments.

As defined on its Web site. "Ping Identity Corporation was established to meet the growing demand for solutions that manage the emergence of Identity Federation—the linking and movement of identity information between two or more organizations." For more information about the PingID network and corporation, check out http://www.pingid.com.

Context-Sensitive Identity Management

Another area of Identity Management that will become increasingly important is context. For example, most current OSs employ a form of the concept of allowing logon at specific times of the day or to specific resources, such as remote access. The consideration for many organizations is that unless all your resources are protected by the same access control mechanism, such as an SSO solution, you cannot apply the same policies across many different types of resources.

Time-based restrictions are an example of basic context-based controls. The following list offers other context-based information that could be used to control access to systems as well as determine the identity of the access requester (generally consider an individual, but could also be an application or service that needs access to other resources):

- Location of the access requester—Is the access requester accessing the resource from a controlled environment (an intranet, extranet, or VPN), or is the access requester trying to gain access from a remote location (unencrypted dial-up, DSL)? Can the location be determined and validated by an outside source?
- Location of the resource—Is the resource within a physically secure environment?
- Authentication method—Is the authentication method an account and password, token, or biometric?
- Access method—Is the access requester trying to access resources via fixed connection, wireless connection, or other? What type of connection is being used—wireless and WiFi, Bluetooth, infra red?
- Access device—What device is the access requester currently using—laptop, desktop, handheld device, or other?

These as well as additional pieces of information help define the context of the situation and can allow a system to change the level of access a user may have. This functionality can help ensure that secure data is only accessed over a secure (for example, encrypted) connection. In addition, there are more extensive sets of context information closely related to biometric challenges such as whether the access requester is under stress—is the access requester’s blood pressure, body temperature, or pulse rate outside of scoped limits. Certainly, these types of methods might seem far-fetched or beyond the needs of many organizations. However, there is a growing niche for such context-sensitive information, and these types of solutions are already available in high-end security solutions that will become more prevalent as well as cheaper over time.

In addition, context expands the ability of an Identity Management solution to provide dynamic profile information to applications—profiles are extended through context information. A profile is a set of characteristics that relate to an identity, including data about that identity ranging through the following:

- Name
- Addresses/locations
- Age
- Identifying references
  - Passport Number
  - Student number
  - USA Social Security Number
- Application preferences
  - Color schemes

Although Identity Management is generally thought of as dealing with the identity of individuals, another context of Identity Management solutions is that of systems and applications that need access to each other. In some cases, this might be an application that needs access to another to enact changes on behalf of a user. Thus, context provides the dynamic aspects of the profile, allowing for very complex scenarios (applications acting on behalf of users, for example) to be automated.

Identity Theft

Identity theft is when somebody gains information about, or the identifiers of, someone else, and uses that information to masquerade as the person whose identity has been stolen. Because identity is based on key pieces of information about a person (for example, date of birth, address, and so on, many identity solutions base their validation on those pieces of information; in some cases, making the assumption that an individual in possession of that information must be the same individual to whom they belong. In these situations, a thief can establish a bank or credit card account with some basic address information. It is difficult to protect against such criminally fraudulent behavior, but by placing controls around how information is exchanged we can mitigate the risk.

There are many ways identity theft can occur in the real world, such as:

- Pickpockets and purse snatchers—The classic theft that traditionally nets cash is now used more and more to obtain credit card, driver's license, and other personal data that can be used to obtain additional credit at a later date.
- Swiping—Thieves use swipers (small electronic card readers) to capture credit card details that can be uploaded to a computer at a later time. These thieves often "employ" staff in heavy tourism areas and upscale restaurants in which credit cards are often used. Cards might not even be used for some time after the theft, meaning that tracking where the incident took place can be extremely problematic.
- Mail theft—Much identity theft today is through simple theft of physical mail from a mailbox. This type of theft focuses on credit card approvals (that is, pre-approved credit card offers), payments (utilities, car registrations), and so forth. The goal is to gain as much personal information about individuals, or alternatively, to gain a person's actual credit card, license, or otherwise such that the thief can easily pretend to be that person. This theft affects domestic as well as business mail.
- Trash or dumpster diving—Similar to mail theft, thieves can obtain information about an individual or organization by searching through trash either at home or near a business. Thus, the need is very high to shred any paperwork that contains personal information.
- Insider access—Unfortunately, insider access to data is a growing concern wherein employees of organizations that deal with personal data (for example, a Human Resources staff person or customer service representatives) exploit their position.
- Private data on second-hand computers or similar electronic devices—Thieves may obtain old computing resources from individuals or organizations and attempt to recover information from the devices. Corporations should ensure that all data on old computing devices is thoroughly wiped before selling or giving them away. Ideally, the hard drive should be removed and destroyed prior to the machine being moved on.
- Redirection—Thieves might use a change of address or similar method to redirect mail to an address that they control.
- Internet—There are many potential risks in exchanging information over the Internet. Although there are common methods for encrypting data between clients and providers, primarily SSL, there is still a danger in how the data is stored and that the data might be compromised in any number of ways.

Identity theft over the Internet is an area of focus for the Identity Management arena. It is an organization's responsibility to not only protect identity information, but also to ensure that the organization is able to help in the event that the information is compromised in some way—for example, by ensuring that organizational perimeters are secure and monitored along with being able to provide forensic evidence (log files, audit trails, and so on) should the need arise.

Recent research by students at the Massachusetts Institute of Technology (MIT) found that in a surprising number of cases important and confidential data is not correctly or sufficiently erased from storage before it is released into the public domain. Although non-conclusive so far, the anecdotal evidence is alarming. To undertake their study, the researchers purchased 158 disk drives for less than $1000. Of the 129 functional drives, there had been little or no attempt to erase information on 28 of these. Many contained a great deal of personal data, including confidential emails. Alarmingly, one of the drives had come from an ATM machine, one contained a year's worth of financial transactions, one contained more than 5000 credit card numbers, and yet another contained confidential medical records.

The Keys of Identity

One way to sidestep potential identity theft is to not use standard information as key identifiers or account names. Many organizations, particularly in the United States, tend to use common social information as identifiers. Almost ubiquitous is the Social Security Number (SSN), assigned to every resident. Arguably, the SSN is in such widespread use that to use it as a sole identifier is at least questionable. Worse still, many online organizations use the SSN as a logon identifier. Interestingly, this situation makes a variation of brute-force hacking quite easy, such that hackers can determine the validity of an SSN.

> ✎ Brute force methods of hacking attempt to overwhelm a system by trying many different types of entry. For example, the most common brute force attack is to obtain an account name on a system and use a dictionary of possible passwords to try and "guess" the correct one. This hack works when the system is made unsecured by not setting password lockouts as well as the fact that most people still use common words for their passwords. Consider an ATM card. In this case, the equivalent to a password is a Personal Identification Number (PIN). In most cases, the PIN is only four digits, equaling a *potential* 10,000 possible combinations. If it were achievable, you could try all 10,000 possible combinations; however, ATM machines protect against this scenario by "eating" or "swallowing" the card after a set number of unsuccessful attempts (usually three). The ATM model uses two-part authentication. Essentially, the ATM solution combines "something you have" (the ATM card) and "something you know" (the PIN). Either factor is weak by itself as cards can be stolen and PINs can be guessed (or worse still, written down by the card holder). When combined correctly, however, the solution is less prone to attack.
>
> The introduction of smart cards and further advances in the capabilities of readers (ATMs and similar) will help to eliminate such brute force attacks. Fingerprint and other biometric information will form part of the process as well.

In the case of an organization using SSN or similar for their account identifiers, hackers can attempt to work out "which number works," as in the following case. On March 6, 2003, it was announced that the University of Austin was compromised by hackers who made off with approximately 59,000 names and SSNs of current and former staff and students.

What this means is that increasingly, organizations that use such identifiers will become increasingly targeted. The question many of these organizations face is whether to spend the money changing their identification, authentication, and authorization processes now or bear the brunt of being compromised. Of course, the answer should be that an organization spends the money now, but many organizations play the risk game to their and their customers' detriment. Of course, the impact on the integrity and perception of the institution will take a significant beating as the result of such a scenario, as the message posted on the University of Texas Web site attests (the message follows and can be read at http://www.utexas.edu/datatheft/). It is important to understand the implications of the entire message, as it serves as a severe warning to the importance of secure management of identity data:

> The University of Texas at Austin regrets that one of its administrative databases was breached by a deliberate attack through the Internet. Since the security breach was discovered Sunday evening, March 2, the University has devoted all available resources to identifying the origin of the attack and recapturing the data before they could be misused or transmitted. Through this Web site and other means, the University seeks to inform the University community and the public about the University's response as well as the status of personal data exposed in this incident.
>
> The University is grateful for the prompt and expert response of the Travis County District Attorney's Office, the U.S. Department of Justice, and the U.S. Secret Service. In particular the University wishes to call attention to the March 6 statement of United States Attorney Johnny Sutton, "... it does not appear at this time that the information that was obtained from the University database has been disseminated, nor has it been used to the detriment of the persons to whom it rightfully belongs." This statement followed execution of a search warrant on the two residences identified as the source of the attack.
>
> Although the U.S. Attorney's statement is reassuring, the University does not seek to minimize the concern raised by this incident. Accordingly, through this Web site the University makes available several communications mechanisms for concerned individuals, as well as a set of resources for monitoring credit records and protecting your identity.
>
> If you are unfamiliar with the basics of this incident and the University's response, see "Initial Report."
>
> The "Am I Affected" page lists the three ranges of Social Security numbers that were used to attack the University System. A total of 2,670,797 SSNs fall in this range, whereas only 55,200 SSNs were exposed from the University database. If you have had no affiliation with the University, it is highly unlikely that you are affected, even if your SSN falls within range.
>
> If you believe you are affected, or might be affected, we encourage you to complete the online form at "How To Contact Us" so that we are assured of an up to date postal mail and e-mail address for you. The University intends to contact every individual whose Social Security number was exposed by this unfortunate incident.
>
> This Web site will be updated whenever the University is made aware of new information about the progress of the investigation by law enforcement authorities as well as when the University can clarify when and how it will communicate with affected individuals.

Intrusion Detection

As we have just discussed under the identity theft heading, one of the Identity Management–related issues faced by many organizations is determining whether your system is under attack. Commonly today, an intrusion detection system monitors network communications and, using profiles or thresholds, attempts to determine whether a hacker/cracker is attempting to break into a system or cause a Denial of Service (DoS) attack. If the determination is made that intrusion is being attempted, the system might send out alerts (email, SMS, SNMP, page, and so on), log the attack (syslog, NT event logs, custom log file), and/or try to modify the operating parameters (configuration, port numbers, communication speed, and so forth) of the system being monitored in order to prevent or alleviate the attack.

It is important to remember that attacks can come from inside or outside your network. Although many studies say that a majority of attacks or security breaches come from within the organization by insiders, the increasing reliance on the Internet ensures that more connectivity is in place and more doors are being opened to the world outside your network. The question your organization must ask is whether the doors are being secured correctly? The importance of Identity Management to intrusion detection is to help minimize the scope of potential damage in any unauthorized use of a system.

Intellectual Property Theft

Protecting intellectual property is a goal of most Identity Management solutions, even if it is not advertised as such. Intellectual property is defined by the World Intellectual Property Organization (WIPO) in the following way: “Intellectual property refers to creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce.” Intellectual property is essentially intangible assets or resources. Business processes, staff and customer lists, sales data, and research and development activity are all examples of intellectual property. The trend is that Identity Management provides additional security and process around the protection of intellectual property in addition to assets and resources.

Throughout this book, the Identity Management framework has been presented as largely managing resources that are under your direct control. One trend today is that organizations are increasingly concerned with management of resources or assets that go outside of their control, often referred to as proprietary technology or intellectual property.

Granting access to an organization to utilize services or data is a common reason for initiating an Identity Management solution. However, there is the consideration of what happens if the consumer of that data is able to take it outside of the controlled environment. There exists today many mechanisms and standards for the protection of intellectual property, including copyright, trademark, and patent registrations as well as Digital Rights Management (DRM) technologies. The basis of these protections are a cultural acceptance of what these registrations mean in legal terms, and what the results are should the law be broken.

Interestingly, these protections are primarily what would be referred to as out-of-band solutions. That means that the protection is not a part of the actual product or resource that is being used, but rather relies on an almost separate agreement, conducted outside of the transaction that actually takes place. This is the role of contracts such as an End User License Agreements (EULAs) associated with most software sales. The issue with this type of solution is that there is no guaranteed control over the intellectual property unless unauthorized use is detected. Instead, the solution's use is based on trust and belief that the user of the resource will do so in a valid way because of a perceived level of honor, or more likely the potential threat through other means (legal ramifications that can have significant financial and social consequences).

The rise of technology, and specifically the Internet, has created new opportunities for rapid exploitation as well as rapid enforcement or protection of intellectual property. The issues surrounding this are that intellectual property in electronic format (such as documents, music, video, and so forth) are now easily transferable via electronic mechanisms in an unchecked manner—there are many more people who are now able to abuse the out-of-band agreements. Truthfully, it is not so much these agreements that protected intellectual property, but rather the cost of acquiring the intellectual property in a useable format.

The rise of peer-to-peer (P2P) networking solutions has been popularized by both Instant Messaging and file sharing networks. The growth of file sharing has created several identity challenges. Napster provides a perfect example. Although Napster was shut down as a result of legal proceedings, similar solutions have sprouted in its place (Gnutella, OpenNap, FastTtrack, and more). Users identify themselves to these networks and connect to other users to download files (primarily copyrighted music and video formats), but there is no real control over the process. Users can define their own name, alias, and so forth, making the tracking of who is using the system more difficult. Ultimately, of course, these users must reside on the Internet somewhere, have an IP address, and have a physical presence that can be tracked. ISPs have recently been subpoenaed to provide logs in order to allow the Recording Industry Association of America (RIAA) to correlate an IP address with a real-world user.

How is this important in the Identity Management market? For many years, organizations have had the goal of protecting assets in isolation. Solutions have evolved through software encryption or license enforcement requiring license keys to unlock and physical security devices such as dongles shipping with a product. To protect documents from unauthorized use or copying, a number of companies have introduced software and hardware solutions to do so, such that the rights of the creator are tied to the asset and can be enforced by tools that want to access or make use of that asset. Essentially, this is known as persistence and is embodied in DRM.

For example, Adobe has introduced protection into its Acrobat solution. Acrobat is a software solution for creating and reading documents. Adobe includes incorporates in this solution basic document protection within the framework for protecting content from copying, printing, and so forth.

In addition, vendors of portal products, document management solutions, and similar are incorporating DRM and SMS principles into their core products in response to enterprise customers asking for “good enough” security at more manageable costs. This natural consolidation of security technology into content servers and document repositories is a significant trend that will brighten IT budgets and dim the fortunes of secure content management systems suppliers. The key is that DRM solutions are also being driven by regulatory compliance (HIPAA and GLBA) and ultra-high-value intellectual property such as product design plans with limited user communities. Each layer of the stratification builds upon previous layers.

Authenticated self-service download of a PDF document over an SSL session provides an audit log of restricted access to content that cannot be easily modified after delivery. Recipients are trusted not to share passwords or abuse the trust relationship.

Secure messaging provides a cryptographically protected push capability to designated recipients with tighter audit capability and tighter desktop security. Implementations consist of software to transparently encrypt and decrypt messages, manage license keys, and allow organizations access when passwords are forgotten.

DRM enforces policy and restricts an end user’s ability to save local copies, print hard copy, electronically forward content, and copy and paste to lift information into another body of work. The implementations involve maintaining a user registry, setting policies for stored content, managing distinct license servers, and providing technical support to business partners. This trend has had a sobering impact on the bottom line for vendors of DRM and secure email products. Consumer-oriented content providers jumped off the DRM bandwagon, while enterprises pulled up short on assuming the extra overhead burdens of complex security systems to limit what business partners can do with online content.

Content and DRM

As well as attempting to control software piracy, electronic copyright protection extends to many other forms of electronic media, such as music, video, and electronic books. Protecting content can take two main forms. The first and most simplistic is to encrypt the source to ensure that it can’t be copied from one place to another, or if it is copied, ensure that it cannot be decrypted elsewhere.

For example, a music CD could be encrypted to prevent it from being copied onto a PC and copied elsewhere or downloaded to MPEG players. The second method of controlling access to copyrighted material is to embed some form of access control into the media itself. This option is designed to allow the material to be copied freely but only accessed if a particular individual has the appropriate access. Access control implies knowledge of the identity of an end user of some form.

> ✎ *“Digital Rights Management (DRM) systems restrict the use of digital files in order to protect the interests of copyright holders. DRM technologies can control file access (number of views, length of views), altering, sharing, copying, printing, and saving. These technologies may be contained within the operating system, program software, or in the actual hardware of a device.”*
>
> **—DRM & Privacy, Electronic Privacy Information Centre, January 2003**

There have been several attempts over the past few years to set standards around DRM systems. The Trusted Computing Platform Alliance (TCPA) was formed by some of the larger vendors who had been working independently on copyright controls. The vendors are Microsoft, Intel, IBM, Compaq, and Hewlett-Packard (the latter two having now merged).

The most concrete and controversial DRM system to be outlined as a part of the trusted computing push is the Microsoft Palladium initiative—now known as Next-Generation Secure Computing Base (NSCB). This initiative is a combination of controls deployed in hardware and in the OS itself. Although this initiative is still in the early stages of development, there are plans to include features such as virus and spam controls as well as an Identity Management store of some form and DRM controls.

Some of the main players in the DRM space have been the music industry, movie producers and distributors, and online book distributors. These players have a desire to protect the intellectual property of the material they offer. They want to capitalize on the broad reach of the Internet without having their products freely copied between third parties. They have formed partnerships with vendors such as Microsoft and worked through the political system to have bills approved to protect their intellectual property.

Regulatory and Compliance Issues

The increasing set of regulatory and compliance challenges have already been discussed throughout the book. Expect these pressures to increase.

Paradoxically, expect privacy issues to both support as well as resist the rollout of Identity Management solutions, primarily in the case of extending Identity Management beyond the organizational perimeter. This is why organizations such as PingID, which, as I mentioned earlier, provides a non-proprietary network through which identity information can be exchanged within a legal framework, will be increasingly important to mediate these issues and support your own rollouts.

Identity Management Appliances

The goal of appliance-based solutions is to offer a secure and focused solution implemented on a system based on a single-purpose appliance architecture. This prevents the possibility that holes in the underlying general purpose OS could compromise the entire system.

Appliances have seen an increasing role in supporting businesses. For example, firewalls are a very prevalent example, wrapping multiple but specific functionality into a black box. This feature appeals to numerous organizations that do not want to spend time implementing specific functionality for their general environments.

Identity Management appliance-based solution vendors also provide authentication services, DNS, DHCP, mail and calendar, and directory stores through appliances. Examples of authentication services include:

- SafeNet's iGate—The iGate combines authentication and encryption capabilities. This functionality lets you manage users' access via a secured browser-based application through the use of a USB-based token, or iKey, and a PIN.
- SingleSignOn.Net Practical PKI and Least Privilege—These solutions offer role-based access control on a dedicated appliance running a hardened OS.

Expect the trend to continue with more Identity Management-specific appliances becoming available over the next few years that offer role-based access controls, provisioning, and so forth.

When looking at these types of devices, one of the common indications that the solution is secure is certification such as FIPS-140 (http://csrc.nist.gov/publications/fips/) or ANSI X.9F (http://www.ansi.org/). FIPS-140 is a United States government standard (also recognized by the Canadian government) that describes the security requirements for cryptographic hardware and software modules (the most recent and current version is FIPS140-2). ANSI, through the related financial services committee X.9F, is drafting several standards that embrace FIPS-140 to support financial solutions.

Software Licensing Enforcement

As the software industry has grown, there has been an increasing requirement to protect the intellectual property of the software developers. Most products have licensing schemes and enforcement of some form. For example, the open source community has the GNU General Public License (GPL). In order to enforce licenses, there is a need to identify who licenses the software, which is where Identity Management is and will become increasingly important.

Advanced Biometric Applications

An improving area of biometrics focuses on cases in which the user isn't aware of the scan. For example, an airport might have a facial-features scanner designed to trigger based on known terrorists. Equipment could be installed under the floor in order to discover people according to their gait, or even weight, as they walk over them (such systems can distinguish among multiple people walking simultaneously). Body odor and DNA can be extracted from a persons "thermal plume" as they walk under a sniffing system.

Biometrics introduces a huge privacy debate. For the first time, it provides the government with a means to track its citizens in a manner that the citizens cannot avoid. This functionality gives totalitarian governments the ability to tightly control their populations. At the same time, it provides businesses equal opportunity to invade their employees and customer's privacy.

Biometrics is considered to be based upon a single, unalterable identity. A private key, for example, can be destroyed in case it is compromised (through key revocation). However, the features detected by biometric technology are with you for life. Today's authentication is usually through pseudonyms that are only roughly related to who you really are.

The key to biometrics is that they cannot be forgotten; many companies are adopting biometrics as a cost-saving issue because lost passwords are becoming a leading problem in IT departments. Biometric features cannot be passed on from one person to another and are considered extremely difficult to forge. However, biometric verification hardware isn't currently difficult to fool. In fact, several fingerprint readers have been fooled with something as simple as a piece of gelatin.

> ☞ For more information about this fingerprint-reader experiment, check out http://www.counterpane.com/crypto-gram-0205.html#5.

Even worse, biometrics has a number of other problems. The first is that biometric measurements get worse over time, such that there are no guarantees that biometric measurement are permanent. For example, signatures can and do change over time. An injury can change fingerprints or ocular characteristics. Voice recognition systems fail when people have a cold, and biometric technology doesn't always account for those who don't have the requisite physical features. Over time, weight can change and medical changes can significantly alter measured biometrics. Thus, the future of biometric solutions must ensure that biometric solutions can adequately deal with these sorts of issues. The processes to manage the lifecycle issues of biometrics could therefore be considered as complex as those faced by PKI and certificate lifecycle management, where the issues reside around certificate lifecycle of issuance, renewal, updates, revocation, and removal.

Identity Management Resources

As you dive into planning and deploying an Identity Management solution for your organization, you will benefit from research. Table 6.1 provides areas of interest that relate to Identity Management and where you can find more information about these topics.

Area of Interest	Company/Organization	Web Site
Digital identity commentary	Digital Identity World	http://www.digitalidworld.com/
Electronic privacy	Electronic Privacy Information Center (EPIC)	http://www.epic.org/
	Platform for Privacy Preferences (P3P) Project	http://www.w3.org/P3P/
	Privacy Rights Clearinghouse	http://www.privacyrights.org/identity.htm
DRM	Internet Digital Rights Management (IDRM)	http://www.idrm.org/
	Microsoft Corporation Digital Rights Management site	http://www.microsoft.com/windows/windowsmedia/drm.aspx
	Trusted Computing Platform Alliance (TCPA)	http://www.trustedcomputing.org
Software licensing/activation	Microsoft Corporation Software Piracy site	http://www.microsoft.com/piracy/basics/activation/
Identity theft	U.S. government's central Web site for information about identity theft—maintained by the Federal Trade Commission (FTC)	http://www.consumer.gov/idtheft/
	Fight Identity Theft	http://www.fightidentitytheft.com/
	Federal Citizen Information Center	http://www.pueblo.gsa.gov/cfocus/cfjuly2000/focus.htm
	Identity Theft Resource Center (ITRC)	http://www.idtheftcenter.org/
	Cross-border Econsumer.gov—e-commerce complaints	http://www.econsumer.gov/english/

Area of Interest	Company/Organization	Web Site
Information security	Computer Security Institute	http://www.gocsi.com
	The Encyclopedia of Computer Security	http://www.itsecurity.com
	The SANS Institute Online	http://www.sans.org
	The Software Institute’s CERT Coordination Center (CERT/CC)	http://www.cert.org
	The World Wide Web Consortium (W3C) Security FAQ	http://www.w3.org/security/faq/www-security-faq.html
	Information Systems Security Association (ISSA) organization	http://www.issa.org
	Information Systems Audit and Control Association and Foundation	http://www.isaca.org
	Internet Security Alliance	http://www.isalliance.org
International privacy resources	Privacy Commissioner of Canada	http://www.privcom.gc.ca/
	The European Union Online	http://europa.eu.int/
	Internet Users Privacy Forum Web site	http://www.iupf.org.uk/
	New Zealand—Office of the Privacy Commissioner	http://www.privacy.org.nz/
	Ontario Information and Privacy Commissioner’s Web site	http://www.ipc.on.ca/english/index.htm
	Isle of Man Government Office of Data Protection Registrar	http://www.gov.im/odpr/
	Italian Data Protection Commission	http://www.garanteprivacy.it/garante/navig/jsp/index.jsp
	French Data Protection Authority Web site—Commission Nationale Informatique et Libertés	http://www.cnil.fr/uk/index.htm
	The Office of the Privacy Commissioner of Australia’s Web site	http://www.privacy.gov.au/
	Swiss Federal Data Protection Commissioner (SDPC)	http://www.edsb.ch/
	Berlin Data Commissioner’s Web site	http://www.datenschutz-berlin.de/

Area of Interest	Company/Organization	Web Site
	Hong Kong Special Administrative Region of the People's Republic of China Government Information Center Web site	http://www.info.gov.hk/eindex.htm
	Web site of the Office of the Privacy Commissioner for Personal Data, Hong Kong	http://www.pco.org.hk/
	Web site of the United Kingdom Information Commissioner	http://www.dataprotection.gov.uk/
	Web site of the Data Protection Commissioner of Ireland	http://www.dataprivacy.ie/

Table 6.1: Identity Management resources.

Summary

In conclusion, Identity Management should be part of any organization's current and future framework, even if it is not specifically identified yet. Identity Management intersects with security as well as other parts of the infrastructure and business processes, although it is its own discipline. The desire to quickly and securely deliver new information, capabilities, functionality, and services to customers, partners, suppliers, contractors, and employees is a significant goal and deserves recognition in the technology and budget tables.

The following section summarizes the functional aspects and key steps to be taken toward an Identity Management deployment. In addition, this content restates the value that can be gained from an Identity Management initiative for your organization. Figure 6.1 illustrates the Identity Management components that we've explored in this book as well as relates the business value and the complexity of the components.

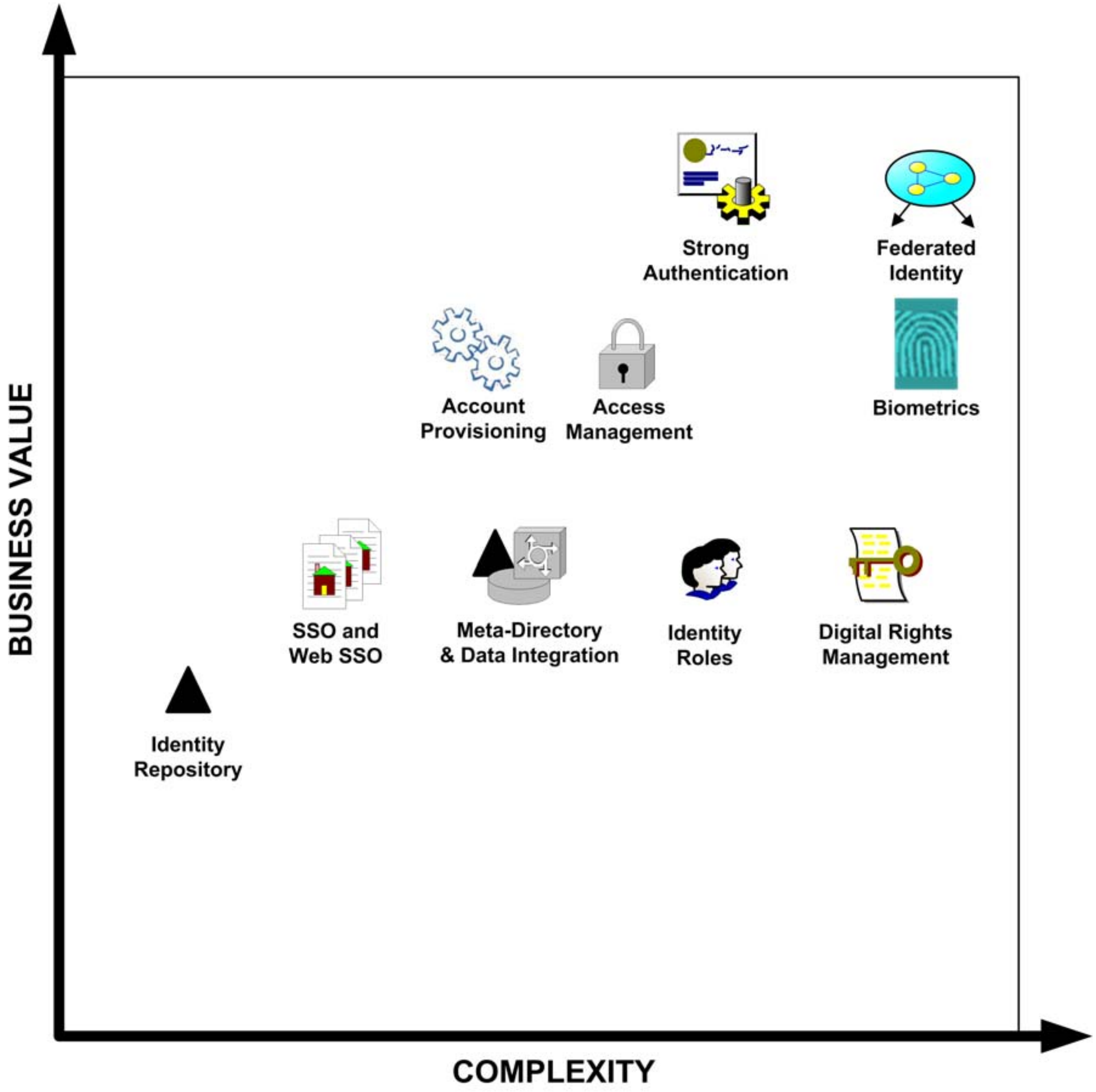

Figure 6.1: The incremental value components of an Identity Management initiative.

As you can see, much can be gained in business value through steps toward a complex but effective Identity Management solution. However, remember that you will benefit only if your infrastructure is useable enough that you can take advantage of the functionality of a complex Identity Management solution.

Although many of the currently available Identity Management solutions claim support for the existing Identity Management standards, and will likely support new standards as they arrive, the clear driver for most organizations is to support and embrace their legacy or heritage applications within an Identity Management framework. Doing so might make it difficult to realize the benefits of the improved standards and solutions as they become available.

As I've stated throughout this book, the following factors are key to the critical success of your organization's Identity Management initiative. During the planning phase and throughout the deployment, you will need to evaluate the process to ensure that your organization meets the following requirements for your Identity Management solution:

- Address core security solutions and key elements
- Ensure management processes are included in the solution
- Manage privacy issues ahead of implementation
- Identify key deliverables such as TCO and ROI
- Identify existing processes and flaws when dealing with management of personal data and related applications and services that require provisioning

We also explored the requirements of implementing your Identity Management solution. The process necessitates people, methods, and focus, as the following list of requisite components highlights:

- Dedicated teams—part time resources do not work
- Methods and tools—the team needs to know what to do
- Tools and enablers—enable efficient implementations

A successful implementation means more than a functioning technology, it requires:

- Organizational alignment
- Process and people integration
- Data integration
- Technical integration
- Roll out and maintenance approach

I hope that the information in this book helps start your organization on its way to a successful and useful Identity Management implementation. Good luck!