

Identity and Risk Management

Preparing for a new world

ABOUT THIS PAPER

When it comes to identity and risk management, the days of business as usual are over. The increasing speed with which Web 2.0, cloud computing and mobile now govern business operations demands as much.

Organizations need to think anew if they are to maintain their critical edge. It is no longer enough for them to view IT issues such as security as purely technical matters. A true, lasting approach to identity and risk management can only come from the top, with leadership that understands—and metes out—a solid governance approach to meet the “many-to-many” environment now upon us.

This paper discusses how leaders can prepare for a new world of multi-channel, multi-device access to improve their security posture and best mitigate risks.

Identity and risk management holds more than a few new challenges for government and commercial organizations. Yet many organizations are still working as they did 10 years ago. Gone are the days when business interactions could effectively be governed by a “one-to-many” relationship, with a standard user ID and password on a local network as the norm. Today, a shift is underway toward a “many-to-many” environment through the Internet.

In this complex new landscape—fueled by Web 2.0, cloud computing and mobile services—business partners, service providers and customers are often scattered throughout the world. At the same time, organizations’ internal data face increasing susceptibility to breaches, as well as questions about the identity of third parties with whom they now partner for data.

Because of these new challenges, few organizations can afford to engage in business as usual. Nor can they continue to view issues of security, especially identity and risk management, as purely technical matters.

Identity and access management: Facing a new reality

Various industries face this new reality.

Take healthcare for instance. In the past, health professionals had access to patient information within one healthcare facility. Today, through electronic health records, these professionals have ready access to information on patients who are not even their own—with or without the patient consent, depending on the jurisdictions.

Or consider public utilities. Public services companies such as Orange in France now accept the public profile of customers, such as through Windows Live, Google or Yahoo, into their own federated identity environment. This represents a vast departure from the days when private customer databases were the standard.

Then there’s government. In most governments, information sharing and cybersecurity, with a corresponding focus on identity, authentication and access management, are hot button topics. Government agencies are increasingly preoccupied with finding ways to validate identity on a recurring and interoperable basis. The U.S. FICAM (Federal Identity, Credential and Access Management) initiative illustrates that preoccupation.

This many-to-many shift across industry lines demonstrates the need for a new approach to identity and risk management. Whereas in the past an organization could provide a one-time password token, such as a secure ID, to secure the access of a user to his or her network, the process of verification now takes on a new level of complexity and enables validation of one’s identity before giving access to an organization’s information assets and data.

Identity governance framework: Lead from the top

Addressing today's identity and risk management challenges begins with instituting an identity governance framework.

Executive leadership must understand that they, not their technical department, are ultimately accountable for an organization's informational assets and data. Far too often, however, an organization plunges head-first into a technical solution using the popular product of the moment without waging an appropriate business analysis first. This approach often undermines efficiency and cost.

As much as 80 to 90 percent of any successful identity and access management approach centers on business strategy. The identity piece requires procedures, processes and legal background, which only can begin with a strong identity governance framework, shaped by executive leadership, that's compliant with the legislation, regulations, standards and practices of one's industry.

Ultimately, a governance framework determines which individuals require identification and strong authentication. If, for example, an organization is dealing with non-proprietary or non-sensitive information, it will not require strong authentication. If, however, the organization is focused on such areas as health or criminal information, a well-plotted governance framework is essential. An effective governance framework must refer to legal requirements or asset categorizations to determine the level of confidence required of third parties to access information assets and data. Once the governance framework is configured, the organization then applies its identity and authentication management framework.

Web 2.0, mobile, cloud: Know the Challenges

Any effective framework must address challenges on three fronts: Web 2.0, mobile and cloud computing. Sooner or later, an organization is likely to leverage each of these services, making it imperative that it also understand the value of identity management within each of these environments.

With Web 2.0 (social media, in particular), an organization can easily fall victim to identity theft or data leaks—and not only through technically sophisticated means. Such theft can result from criminals simply using “friends of friends” to access privileged or sensitive information.

If you're a government or enterprise executive, beware the ease with which your employees can be identified on any major social media website—and, by extension, the ease with which that same person can be used to get information on your company's intellectual property or organizational strategy.

For example, the mere mention by an employee on his or her Facebook page or a friend's page that he or she works for a law enforcement agency could jeopardize the outcome of any given police operation. This vulnerability, which can apply to any organization, makes it essential to implement a consistent framework for the use of social media within your company or government agency. The framework should

DEVELOP AN IDENTITY GOVERNANCE FRAMEWORK

The establishment of an identity governance framework is critical to best address today's identity and risk management challenges.

This type of governance framework requires executive leadership involvement, and it includes a clear definition of roles and responsibilities via an accountability model and a clear line of sight about which individuals require identification and strong authentication.

AUTHENTICATE FOR THE FUTURE

Three critical trends lay ahead in addressing identity management challenges:

1. **Provisioning** to manage user identity (employee, subcontractor, third-party and so on) and access to and across systems, applications and resources
2. **Authentication** to have the means to provide credentials—and manage them easily—to prove that identity, and for use in standard web environments as well as Web 2.0, mobile and cloud computing environments
3. **Strong authentication and digital signatures** to ensure accountability of third parties accessing sensitive information and digital signatures to provide non-repudiation of online transactions

make it explicitly clear that an employee cannot disclose any information, however inadvertent, within a social media setting.

Mobile devices also pose security challenges. With devices such as the iPhone, iPad and BlackBerry, critical company information is often just a screen-touch away. While the anytime, anywhere access of mobile devices fuels a mobile workforce, that same flexibility can also lead to negative business consequences if the same device is lost or stolen with unprotected critical information inside. As a result, it's critical that an organization not only identify the person using the device but also identify and, if needed, localize and disable the device itself.

Cloud computing presents its own security imperatives, particularly in industries such as healthcare where health information can be housed in the cloud. How does an organization know where any given person accesses their critical information? And through which information network? An organization must ensure an extra layer of authentication that goes beyond the days when information was simply housed in an internal system.

A step in that direction is ensuring that the provider complies with industry standards. For example, it's important that the site where the information is kept in a cloud model meets generally recognized standards, such as SAS 70 Level 2 compliance for data centers and a SaaS architecture with a maturity level 1 to 4, corresponding to the business needs of the organization. A provider must be in a position to demonstrate that it has complied with the security and maturity levels required.

Identity management: Be aware of the trends ahead

Three critical trends lay ahead in addressing identity management challenges: provisioning, authentication and the use of strong authentication and to ensure accountability of third parties accessing sensitive information and digital signatures to provide non-repudiation of online transactions.

Provisioning will be required when an individual becomes an employee, provider or business partner of an organization. For example, if a company hires subcontractors on a regular basis, it must ensure they're provisioned—and at the right time.

Provisioning is a critical step in the midst of the continued push toward decentralizing data. Quite simply, an organization's data could be anywhere on the planet in a cloud computing environment. If an organization gives a third party the task of keeping information confidential, it must ensure that no other entity—except the people the organization authorizes—is able to access that information.

Authentication will require an organization to have the means to provide credentials—and manage them easily—for use in standard web environments as well as Web 2.0, mobile and cloud computing environments. If an organization wants to ensure that the person is the right person before issuing any credentials, then it must either use an authoritative data source, such as a government data source pertaining to identity. Or it must meet the individual in person, gather ID information and, in some specific environment, take their fingerprints, for example.

ABOUT CGI

At CGI, we're in the business of satisfying clients. A leading IT and business process services provider, CGI has 31,000 professionals operating in 125 offices worldwide.

Working in partnership with clients for more than 35 years, CGI has extensive experience in all aspects of IT management, from consulting and systems integration services to the full management of IT and business functions (outsourcing).

This know-how puts us in a unique position to help clients successfully implement identity and access management solutions that manage and mitigate risks.

To learn more, visit us at www.cgi.com or contact us at info@cgi.com.

When an organization authenticates the person in question, it must require that they use renowned credentials with a sufficient security level. Strong authentication can include a digital identification certificate coupled with a second or multiple authentication factors as required by the nature of the information assets and data an organization wants to protect. If an organization uses a digital identification certificate in the background, it can then be sure that any person using it will be held accountable for their deeds and actions and will also be irrecoverably linked to documents they sign based on that identity.

Authentication is especially important as organizations continue to open their databases to additional parties—for example, shared health information among health networks. In opening its organization's "trust domain" to others, an organization must be able to authenticate individuals who have access to that information. Additionally, if individuals are providing information to feed a given database, an organization must ensure it's the right person with the proper authorization providing the right information.

Lastly, the use of strong authentication and digital signatures (credential management solutions) will only grow in the midst of new identity and risk management challenges. Hastening this need is the increasing virtualization (dematerialization) of transactions. If a contract is signed digitally, it must be accompanied by an ability to authenticate (and retain, in electronic form) the identity of the signer, such as a doctor administering an e-prescription or a policeman signing an e-report.

Identity management: Look beyond legacy systems

Both the legal and healthcare sectors have successfully introduced identity management in their business area. Underpinning that success has been this critical best practice: to look beyond proprietary or legacy security systems for a more effective identity and risk management approach. Looking ahead, the lessons are clear: Go to the standards, stick with them and avoid too much personalization.

Knowledge is also key. Industries such as healthcare and banking are developing their own governance models. An organization must have the means to comply with standards, use them and integrate them into its governance framework and environment. By contrast, when an organization has a legacy system that can't address new standards, it must find ways to interface those systems so that they meet or, in some cases, comply with those standards.

Those lessons learned are particularly relevant to government agencies. Many still have mainframes and old technology in the background that can't be replaced in the short term. In such cases, they would do well to externalize the authentication and, as required, the authorization processes for those applications. And they should use a standard interface to authenticate and authorize people to have access to those legacy applications.