UNISYS
imagine it. done.

white paper

Identity Management: A Business Imperative in Building a Trusted Enterprise

The Security Leadership Institute

trusted

Introduction

When the CEO and the Board consider the coming year's corporate and IT budget requests, it is very likely that there are opportunities to:

- Increase productivity
- Improve customer relationships
- Create new business opportunities
- Protect intellectual property and corporate assets
- Safeguard customer privacy
- Achieve regulatory compliance
- Contain costs

To facilitate these and other opportunities, the vehicle is called Identity Management. In the budget request, it may be its own line item. It may be buried within the context of a regulatory compliance initiative. It may be part of the security budget request. In more sophisticated enterprises, identity management will be inclusive in the institutionalization of "trusted" operations. But if it is not somewhere in your plan, it should be; corporate leadership needs to appreciate its potential as well as its cost.

Why? Because Identity Management is about relationship assurance, not just about meeting regulatory minimums for compliance and protecting corporate assets. Identity Management ensures transactional integrity with all relational parties. It is the basis for collaborative trust with suppliers, distributors and customers. In sum, Identity Management not only satisfies regulatory compliance and corporate asset protection, but also leverages that investment to improve the use of technology and associated processes to better serve employees, customers, partners, and suppliers — all of which improve the enterprise's reputation and bottom line.

Realizing the promise of Identity Management requires a broad view of the business enterprise and its associated near and long term objectives. The full benefit of this important undertaking can only be realized when CEOs and their executive teams proactively participate in developing the principles and goals of Identity Management and insure implementation of the program.

The goal of this paper is to assist chief executives and their leadership teams in the creation of a common framework for discussion. It explores the evolving and developing nature of Identity Management by defining its scope, articulating its benefits to the enterprise, and outlining critical steps to develop and implement an effective Identity Management strategy. Finally it gives chief executives and their board's key questions to ask their organizations in order to gather the information vital to developing and prioritizing their Identity Management strategy.

Why Care About Identity Management?

- Assists meeting fiscal responsibilities to shareholders
- Insures you control the deployment, not outside forces
- Crosses your entire organization globally
- Extends your organization making it accessible and secure to trusted relationships
- Creates new business and revenue opportunities
- Ensures transactional integrity
- Protects your intellectual property and knowledge assets
- Enhances your customer's privacy
- Extends your enterprise's reputation and trust status

	CEO View of Identity Management	
	Traditional Thinking	New Paradigm
Productivity Enhancement	—	High Value
Revenue Enablement	—	High Value
Regulatory Compliance	Requirement	Requirement
Cost Avoidance	Ongoing/ Essential	New Opportunities
Improved Mission Achievement	—	High Value
Competitive Advantage	—	Critical Enabler

How is Identity Management Defined Today?

Identity Management's definition can be as limited as "a user authentication application" or as broad as "a business enhancement and expansion program". Today, most organizations view Identity Management narrowly, or as defined below.

At its core, Identity Management is the systems and processes for granting access to corporate assets by entitled individuals. There are four components:

- ASSIGNMENT OF A "TRUSTED IDENTITY" — Is this person, application, or network device trusted and holding the key it will use to prove its identity (e.g., a digital certificate, token, or biometric)? Have the appropriate measures been taken to prove the identity before issuing the "key?"
  - — Policy and process (particularly the enrollment process used to assign identities) come into play as much as technology and help determine the level of trust to be placed in each identity.
- AUTHENTICATION — Can I verify that the entity is who or what it says it is?
  - — Processes (knowledge-based, biometrics or digital tokens) employed to present and validate identity credentials can impact both productivity and security. Shared authentication services can reduce the number of logons and provide consistent methods for credential validation and tracking of authentication events.
- ASSIGNING PRIVILEGES — Where can it go and what can it do?
  - — Policies are based on identity attributes (roles, groups, locations, etc.) or the value of the resource to be accessed. Shared authorization and access control services provide consistent policy interpretation and enforcement.
- MANAGING CREDENTIALS AND PRIVILEGES — Has the relationship changed? Has the policy changed?
  - — Effective processes must exist to reissue or invalidate identity credentials and extend or remove privileges to promote user productivity, enhance security and simplify the introduction of new services.

Glancing at its components, it is understandable why organizations often leave Identity Management to the exclusive purview of IT. Identity Management started as a means to automate the manually intensive IT and HR employee administration functions. It is evolving to become an enabler of new business models. It leverages Internet and mobile technologies to simplify the secure exchange of information and services with customers, suppliers and partners.

Why Is It Increasingly Mandatory?

Over 40% of recently surveyed Global 1000 organizations stated they project eBusiness will generate over 20% of their revenue within 36 months.

In addition, the majority of those same Global 1000 organizations stated, opening back office applications to customers, partners and suppliers would positively impact organizational productivity.

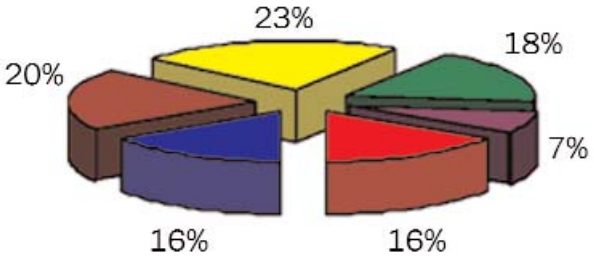
Central to their ability to realize the benefits of margin improvement and productivity enhancements across the supply chain is establishing the appropriate levels of trust. Trust not only in the identities with which they are interacting, but also in the process by which they collaborate.

Security and privacy are no longer an add-on to corporate operations. It is an integral part of the supply chain.

With Identity Management, security steps into the role of business enabler. It is fundamental to an organization's ability to open its doors to deeper collaboration with customers, partners and suppliers.

Projected Revenue e-Business 2-3 Year Initiatives

>5% 5-10% 10-20% 20-30% 30-40% >40%
Percentage of Respondents



Source: Ponemon Institute Research, October 2003

Identity Management is also a critical component to regulatory compliance because it allows organizations to:

- Track an individual's use of applications which delivers the needed audit trail for Sarbanes-Oxley compliance.
- Authenticate who they are interacting with and share information with other private or public sector entities to detect suspicious activity for compliance with the PATRIOT Act, Transportation Security Act, or similar legislation from other jurisdictions.
- Provide audit and forensics data to assure consumers of the protection of their personal health and financial information as required by HIPAA (Health Insurance Portability and Accountability Act) and the Gram — Leach — Bliley Act in the United States.

Beyond Security And Compliance

Approached proactively, Identity Management is a powerful business strategy that delivers improved quality management, workflow process and risk management, and it enhances relationships by driving down the risk associated with trust. In essence, Identity Management enables increased intimacy with customers, suppliers, and business partners, which in turn, reinforces the perception of a brand's quality and creates an unparalleled competitive advantage.

One of the challenges organizations face as they work to embed security into their overall strategy, is that there is an inherent tension between security and other stakeholder groups. Security's mission is to protect the organization. Yet, in this increasingly global and virtual world, organizations must open their systems and applications if they are to sustain their competitive positioning. This balancing act requires the organization to make constant trade-off decisions.

This is particularly difficult because security language tends to be wrapped in networking language. This obscures the business aspects of security impacting initiatives. Identity Management may end up viewed as yet another security drain on already tight budgets. As a result, the funding parameter becomes an impatient, what's the bare minimum we can do to comply?

The Security Leadership Institute believes that organizations need to evaluate Identity Management through a variety of different lenses – those of each stakeholder group. This multi-functional view is enlightening. The following table illustrates a few of the benefits a proactive approach to identity management delivers by vertical.

VERTICAL	STAKEHOLDERS BENEFITS
Bank	**Customer Service** — enables a broader products and services to be delivered via multiple media at lower risk. **Compliance Officer** — provides an additional aid in identifying suspicious transactions.
Defense Contractor	**Program Managers** — delivers greater protections and controls of intellectual assets and classified activities. **Contract Officers** — provides the ability to integrate subcontractors more more completely.
Government Agency	**Operations** — enables eGovernment initiatives that support services delivered directly to the public.
Major Medical Institution	**Operations and Doctors** — allows productivity enhancements across the entire organization from records through prescriptions.
Automotive Manufacturer	**Operations** — delivers reduction in costs due to ability to deliver dealer and service center network real time inventory management.
Chemical Manufacturing	**Marketing and HR** — reduces risk of harm to the company's physical and human esources and loss of reputation. Security — enhances logical and physical access control.

As illustrated, an appropriately deployed Identity Management strategy drives benefits through the entire organization:

- Customers can have direct access to a personalized view of purchasing systems and their history. Their loyalty and trust are significantly enhanced due to their ability to identify their own employees and to manage their access privileges. This self management also delivers significant support cost savings.

- Supply chain partners can view inventory, purchasing patterns and service histories to proactively manage and automate procurements for just in time delivery of products and services.
- Strategic business partners can collaborate electronically in real time to review customer demand, develop integrated product roadmaps, or evaluate and revise engineering schematics.

A pharmaceuticals company is collaborating with a competitor on the development of a new drug. To facilitate collaboration, the two companies are working across corporate intranets. By mapping the authorized interaction, this collaboration can occur while assuring that no other proprietary data is accessed by the competitor's employees. Identity Management mitigates risk of data theft and security compromises and insures access rights and activities are clearly monitored. Finally, it ensures the protection of intellectual property.

Sharpening the Focus

The benefits of a proactive Identity Management program and implementation are many. In fact, the deeper an organization looks into its operational areas, the more benefits emerge, to the point it can become overwhelming. And therein lays the crux of why Identity Management implementations tend to be a microcosm of the ideal. The ideal feels like trying to solve world hunger.

The challenge, then, is to develop an Identity Management deployment strategy that prioritizes an implementation into more manageable pieces, without losing sight of the whole. As with any large scale staged implementation that is easier said than done.

Success Requires CEOs Focus on Three Critical Steps

1. Develop Your Own Foundation

Identity Management is the foundation for realizing a new and improved way of doing business. Organizations are faced with more risk; more technology choices with greater integration challenges and the tendency for individual business units to stove pipe their operations. Achieving the benefits of Identity Management requires an organization to think differently. CEOs must understand what their organizations are doing today, as well as challenge them to apply new, more productive, operational models. CEOs must internalize this new, broader view, of identity management and apply it to their organizations. Changing the paradigm must involve all of the stakeholders. It cannot be limited to the executive team, or the board. All stakeholders must understand Identity Management delivers:

- Central coordination of information which is a necessity by virtue of new regulations for privacy and data protection
- An integral and consolidating vehicle for an organization's responsible information strategy and enterprise architecture. It is not an add-on.
- Proper identification and authentication of users which is no longer a luxury. It is a fundamental cost of doing business. Stakeholders must recognize that the lack of control over Identity Management can have a direct impact on an organization's reputation and competitive viability.

The world's leading developer and supplier of advanced plant genetics to farmers worldwide wanted to build new business by giving its sales force the ability to deliver real time regional data regarding weather, growing cycles and plant yields. It further wanted to enhance its customer service by giving field the ability to collect and access detailed personal customer information. The challenge was to create an easy to use solution that reassured a community typically suspicious of technology. Designing with the business objectives in mind, the IT organization developed a solution leveraging wireless PDAs and Identity Management technologies to deliver the ease of use the sales force required, coupled with the assurances that the farmers required their personal data was protected. The quality of data the field collects improved. The value added services the field provided improved customer loyalty. The solution is now one of the company's major competitive differentiators.

2. Assess the Organization & Develop the Strategy

It is likely that within discrete departments processes may appear to be working well. It isn't until functional groups attempt to collaborate that the broken processes surface. Unfortunately, more often than not, rather than solve the broken linkages, organizations develop Band Aids to solve the specific problem. The result is a hodgepodge of redundant spending and one-off solutions with no consistency or audit ability. More importantly, the existing processes may make external collaboration cumbersome and cost prohibitive, significantly impacting the organizations competitive viability.

Therefore, it is essential CEOs canvas their organizations to uncover the broken linkages and improvement opportunities. This includes far more than IT functions. The review must also include such areas as: policy development, privacy, contract administration, regulatory compliance, HR functions and customer/partner relationship systems.

Once CEOs have a clear understanding of their organizations' gaps, opportunities for improvement, new risks, new value equations, they can develop proactive identity management strategy which insures the organization is able to reach out to each stakeholder group in a simple manner, while ensuring intellectual property protection, privacy, and recoverability.

An organization with over 20 separate CIO organizations, each with its own set of databases, user directors and applications was chartered with developing common interoperable authentication to improve the customer ease of doing business and overall productivity. However, the project was not given a separate budget. The leadership felt there was already enough funding allocated to IT to support the effort. The key to a project's success in securing reallocations from the CIO organizations was establishing an effort to look across the units for redundant investments. They were able to secure — $25m in funding.

3. Commit the Resources and Remain Engaged

In order for Identity Management to have any chance for success it must be viewed as a non-negotiable and fundamental component of an organization's business strategy. Identity management is central to both an organization's risk management and external collaboration strategy.

A truly robust Identity Management strategy requires a level of cross-functional cooperation and collaboration that does not come easy to organizations. Ultimately, it may require transfer of power between functional groups. It will mean headcount and budget reallocations. Inevitably it will be viewed as a zero-sum game where some groups win while others lose. Success requires that progress against the plan is attached to performance reviews and compensation from executive levels through to system administrators. CEOs must remain engaged, but also be aware of becoming potential bottlenecks.

Another critical element to successful enrollment and initial deployment of a core system is establishing centralized funding. Organizations that buy into Identity Management as a business strategy most often fail in their implementation because funding models create an "opt in" environment. Successful initial deployment requires corporate-level investment and forceful central corporate leadership.

Management must be continuous. CEOs and Boards, under Sarbanes-Oxley, are held responsible for operating within a strategy that is consistent with the law and best practices for their industries. It is simply not enough to establish solid polices and business processes. They must be monitored.

The current business environment is such that Identity Management will become mandatory; driven either by regulations or shareholder mandate. Proactively implementing Identity Management programs now, insures CEOs control their business operations. Waiting for external mandates may relinquish that control.

Gathering the Right Intelligence and Knowledge

When evaluating and prioritizing an effort as extensive as Identity Management, it is essential to go beyond conventional justifications, and challenge the functional groups to think beyond their own spheres of influence. The CEO and board should be examining the business implications of an Identity Management strategy to corporate processes and initiatives across the entire organization.

A truly proactive Identity Management strategy should enable organizations to achieve a balance between security and productivity; and should meet the expectations of its customers, suppliers and partners for privacy and enhanced access.

ORGANIZATIONAL OBJECTIVE	CRITICAL QUESTIONS
• Position Identity Management in your overall "trusted enterprise" strategy. • Baseline your current Identity Management policies and practices. • Measure their scope and effectiveness against the opportunities and risks that emerge from your own organization.	• Does your program maximize operational risk management and mitigation organization wide? • Do our security policies provide the level of protection that inappropriate for our knowledge assets and customer information globally? • How have they been benchmarked against best practices and tested? • How do we ensure that our Identity Management processes balance the benefits of improved information protection against authentication complexity for system users?
• Define your Identity Management improvement opportunities and their relative priorities. • Commit the people and resources necessary to address the improvements and protect against the risks.	• What risks and opportunities emerge when we examine the organization's Identity Management practices as a whole rather than by each business unit? • What impact do the identified risks and opportunities have on our top 3 strategic initiatives? • What resources (skills, competencies and funding) are required? • Where is there redundant Identity Management spending/effort? • Where are the skills necessary to support this program successfully?

ORGANIZATIONAL OBJECTIVE	CRITICAL QUESTIONS
• Anticipate and mitigate risk.	• Are we proactively scanning the horizon for new risks? • What incidences and alerts are we dealing with today? • How could we have avoided them? • If we were to have an information security breech, what is the anticipated impact to our reputation or brand in the marketplace? • Where is we most exposed? • Do we have the mechanisms and forensics in place to complete a post mortem? • How long would it take before being able to notify harmed parties? • How long would it take to make a realistic assessment?
• Continually monitor the program to capitalize on new opportunities across the organization (customers, employees, business partners, suppliers).	• What are our top 3 strategic initiatives over the next 3 years across all business units that touch our most strategic assets? • What opportunities exist to further improve our operations?
• Build awareness throughout the organization to proactively address regulatory compliance, new business opportunities, productivity improvements and customer satisfaction opportunities.	• How are we building awareness at all levels of the impact of their actions on the protection of our assets and customer privacy? • Are we anticipating regulatory compliance requirements? • Have we reviewed both current and pending legislation and rule making to understand their implications on our operations? • Are we integrating compliance into our business plans and strategic investments?

The confluence of strategy, process, and technology represented by Identity Management is long overdue. Today's global environment presents greater risks to our nation, our economy and our personal safety. It also represents unprecedented opportunity to expand our reach. Capitalizing on that opportunity requires organizations to also protect against the risks. A well thought out Identity Management strategy and deployment plan establishes a solid foundation upon which to build.

About the Authors

The Security Leadership Institute (SLI) is a forum of nationally recognized security experts from business and government that provide insight into emerging security issues and best practices to organizations worldwide. A goal of the SLI is to help both business and government leaders to see "beyond the horizon" and gain security insights that can become key factors in their long-range business strategy.

SLI Members:

General Michael P.C. Carns
USAF, retired; vice-president of Privasource, a software firm that specializes in securing large, sensitive databases.

William P. Crowell
Security consultant and former deputy director of the National Security Agency.

James J. Flyzik
Partner, Guerra, Kiviat, Flyzik and Associates, a consulting firm; former CIO, U.S., Department of Treasury.

Norman D. Inkster
Partner, Growlings Consulting; former commissioner of the Royal Canadian Mounted Police and former president of INTERPOL.

Dr. Lawrence A. Ponemon
Chairman and founder, Ponemon Institute, dedicated to advancing ethical information and privacy management practices.

John C. Reece
Consultant; former CIO of the U.S. Internal Revenue Service.

Thomas L. Sheer
Authority on corporate investigative strategy; former assistant director of the FBI New York office.

Dr. Eugene H. Spafford
Executive Director of the Center for Education and Research in Information Assurance and Security.

For more information, please visit our Website at:
www.unisys.com/public_sector

Specifications are subject to change without notice.

© 2005 Unisys Corporation.

All rights reserved.

Unisys is a registered trademark of Unisys Corporation. All other brands or products referenced herein are acknowledged to be trademarks or registered trademarks of their respective holders.

6869 5436-000

Printed in U S America 10/05