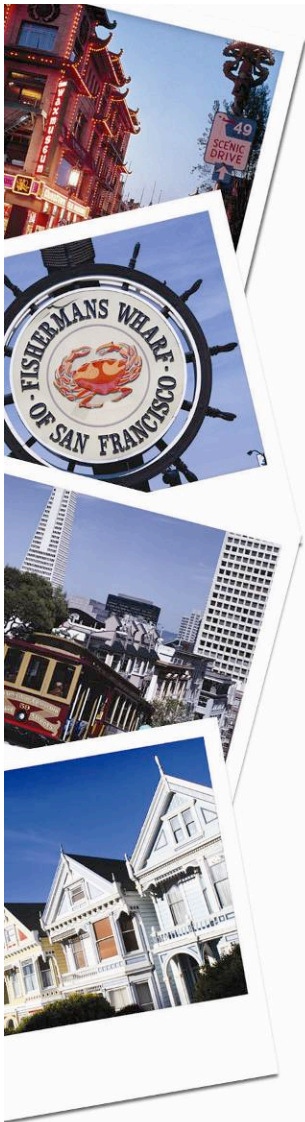


Identity Management Solutions for Supporting Compliance

John Suess
VP of IT and CIO
UMBC

YOUR GOLDEN GATE TO EXCELLENCE



Progress Through Sharing

2008 INTERNATIONAL CONFERENCE

July 6-9 / San Francisco, CA, USA

San Francisco

Identity Management Solutions For Supporting Compliance

- ▶ My background that shapes my perspective on this topic.
 - ▶ In 2000, UMBC launched our initial Identity Management .
 - ▶ In 2003, I authored a section on security architecture for higher education that focused on the role of Identity Management in developing a security architecture.
 - ▶ In 2004, I was named a co-chair of the higher education computer and network security task force.
 - ▶ In 2005, UMBC began participating in the eAuthentication initiative between higher-ed and the U.S. government.
 - ▶ In 2006, UMBC joined the InCommon federation and began supporting federated Identity Management.

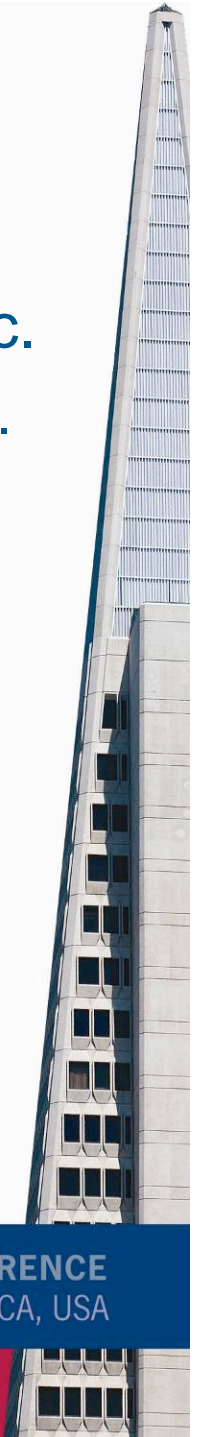


Progress Through Sharing

2008 INTERNATIONAL CONFERENCE

July 6-9 / San Francisco, CA, USA

YOUR GOLDEN GATE TO EXCELLENCE



What I Will Focus On

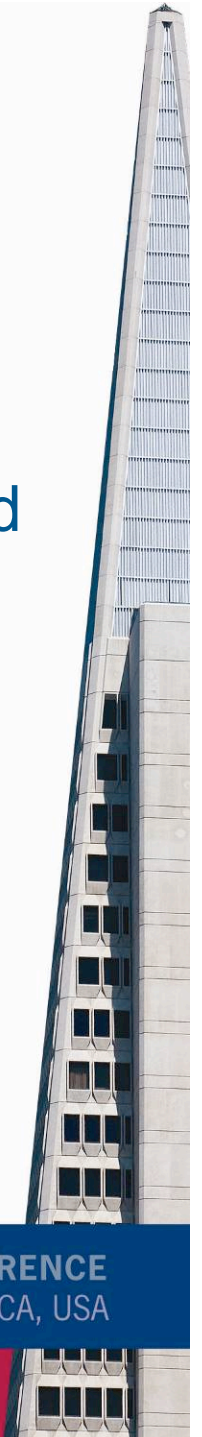
- ▶ An overview of identity management
- ▶ The concept and use of level of assurance
- ▶ The concept and use of federated identity management
- ▶ The crisis in managing and protecting privacy
- ▶ How identity management can help improve security, protect privacy, and ensure compliance
- ▶ The importance of the audit community in working with IT to make this a reality.

Overview of Identity Management Systems

- ▶ What do we mean by Identity Management?
 - ▶ **California State University** definition - An identity management *infrastructure* is a *collection of technology and policy* that enables *networked computer systems* to determine who has **access** to them, what resources the person is **authorized** to access, while **protecting** individual privacy and access to confidential information.

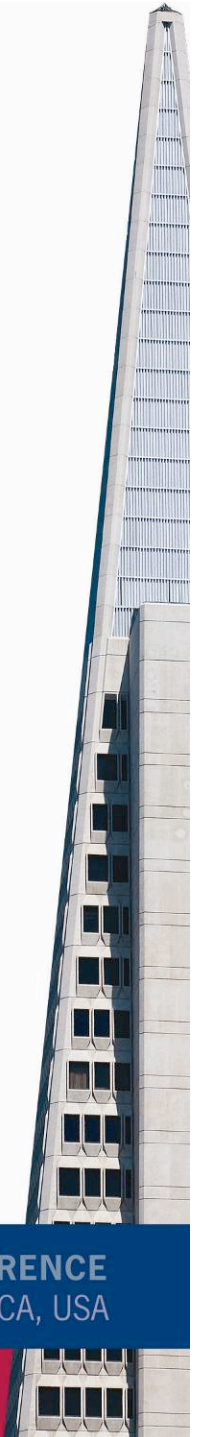
Analyze the Definition

- ▶ **Infrastructure** - software and hardware
- ▶ **Collection** - not just technology
- ▶ **Technology and policy** – policy plays a critical role and is an essential element of the solution
- ▶ **Networked computer systems** - implies distributed technology systems communicating over a network
- ▶ **Access** - Who am I
- ▶ **Authorized** - What can I do
- ▶ **Protecting** - limiting access and protecting information



Another Definition - Identity Management System

- ▶ Suite of organization-wide security, access, and information services
 - ▶ Integrates data sources and manages bio-demo information about people and devices
 - ▶ Establishes electronic identity of users and devices
 - ▶ Issues and validates identity credentials
 - ▶ Uses organizational data and management tools to assign affiliation attributes
 - ▶ ...and gives permission to use services based on those attributes

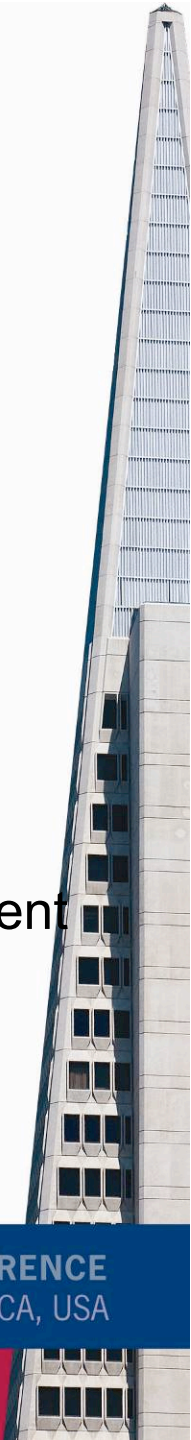
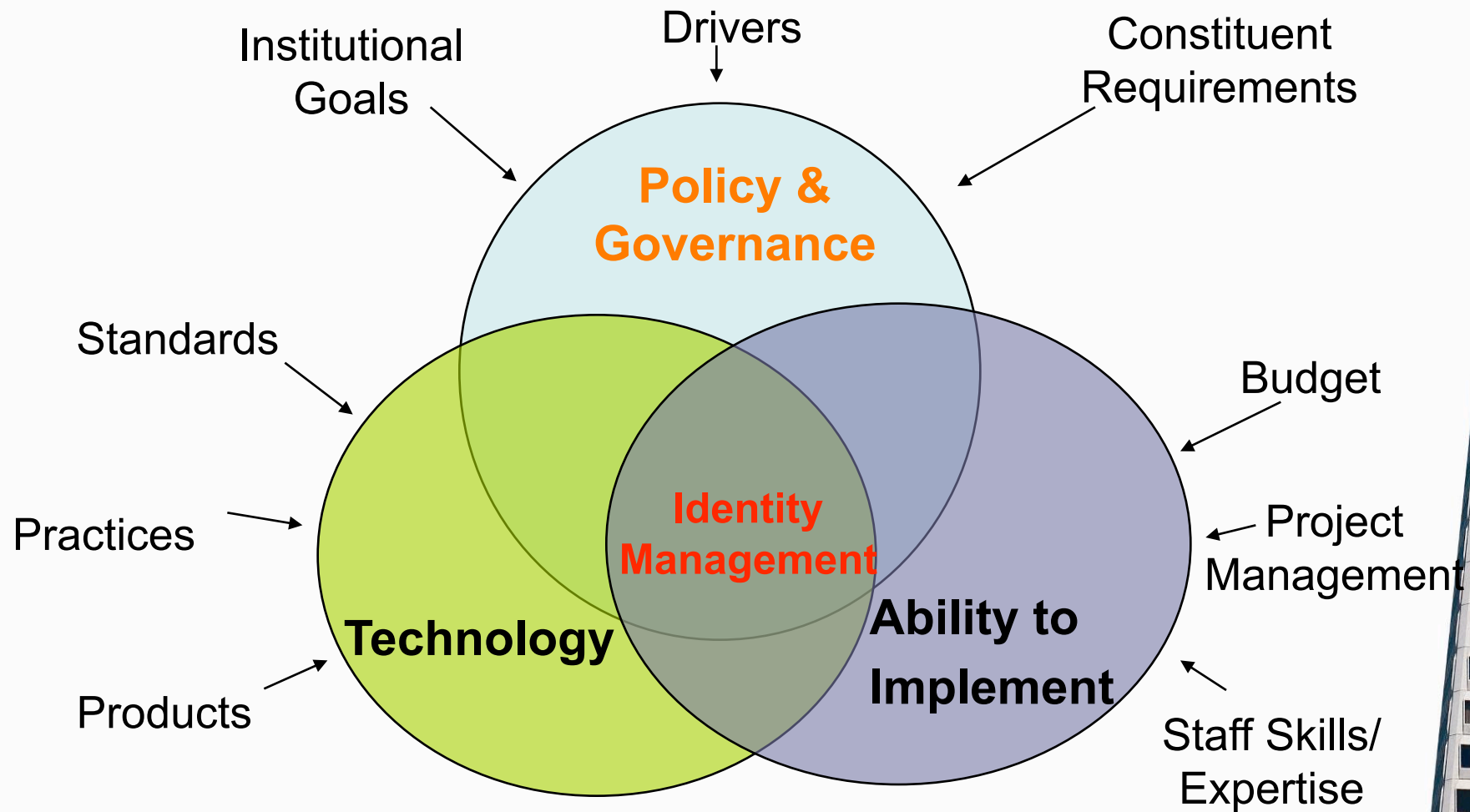


Identity Management and Security

- ▶ I believe the identity management system (IDMS) is a integral component of the organizations overall security strategy and architecture.
- ▶ Historically in my sector, higher education, IDMS has often been developed and managed more as a business enabler than as part of the security strategy.
- ▶ Looking at IDMS success factors we see how much overlap there is with security.



Identity Management Factors



Progress Through Sharing

2008 INTERNATIONAL CONFERENCE

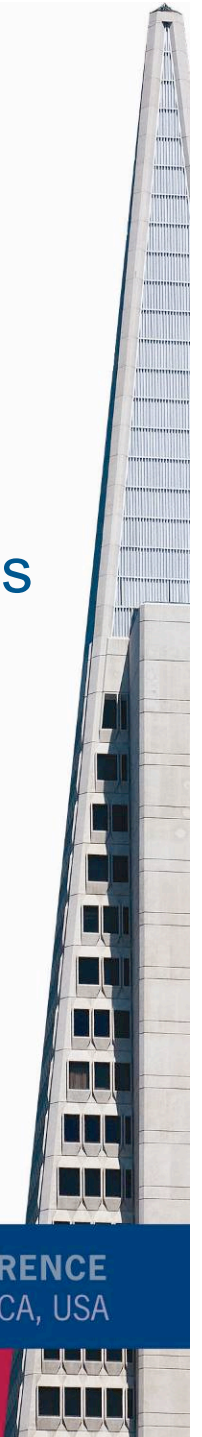
July 6-9 / San Francisco, CA, USA

AIIC - 3 October
2004

YOUR GOLDEN GATE TO EXCELLENCE

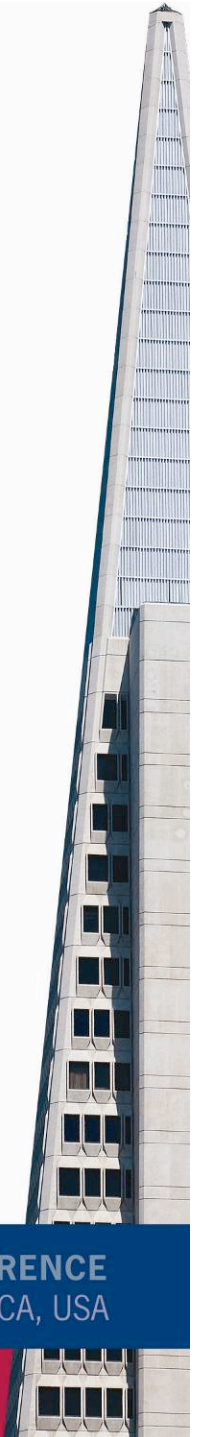
Review of Factors

- ▶ As we find with security, identity management is at the intersection of policy and governance, technology, and people.
- ▶ Amongst these factors, the technology is maturing and is becoming the easiest of the three as vendors develop better cross-vendor solutions.
- ▶ Staffing still requires highly-qualified IT architects that can work across technical and functional areas.
- ▶ Policy and governance – of which audit is a key tool, is the most challenging of the three.

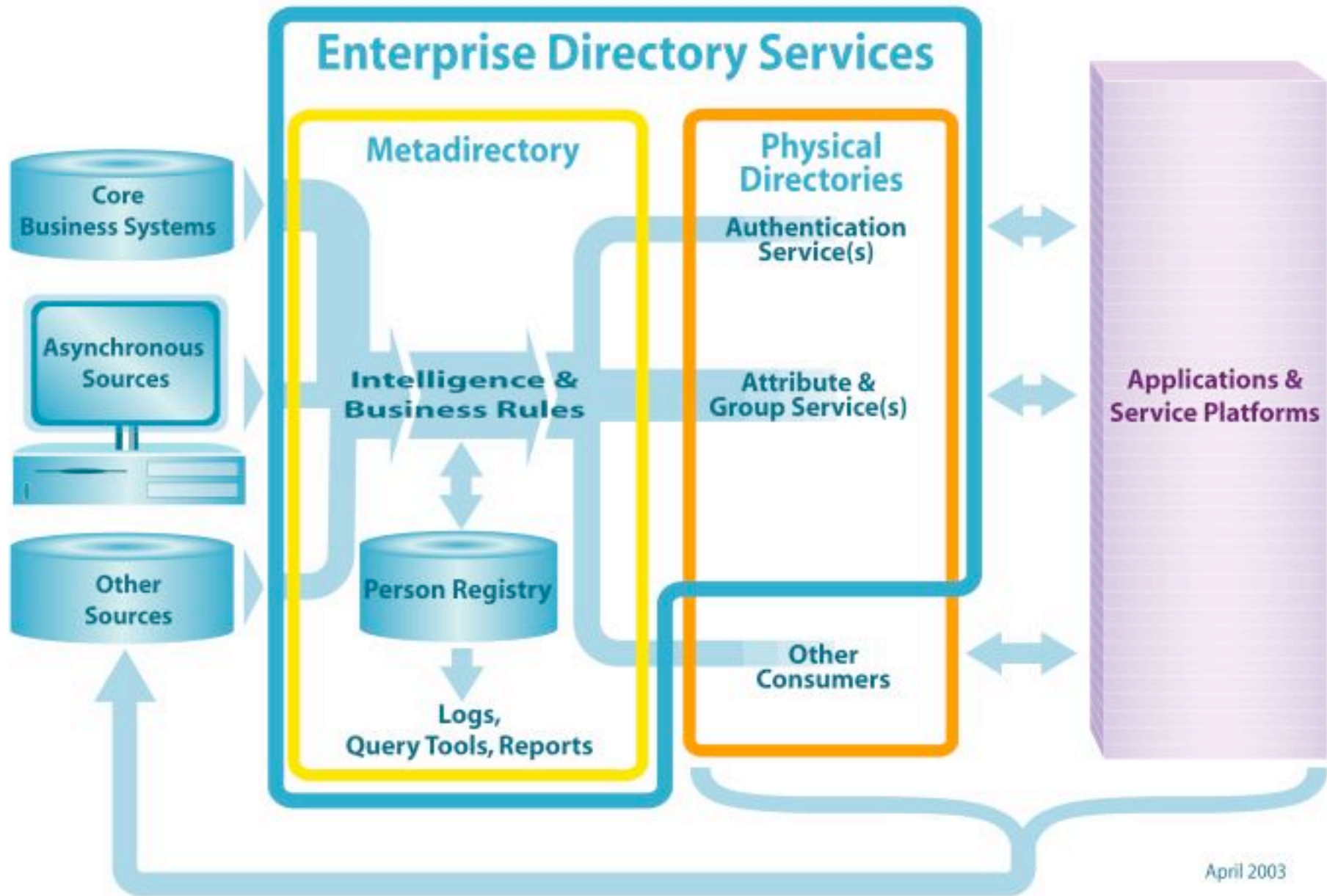


A Model Architecture for Identity Management

- ▶ Identity management systems aggregate information across disparate systems. Requirements include:
 - ▶ High performance – these systems drive all web-facing customer applications and customers (or employees) won't wait.
 - ▶ High reliability – these systems often provide all authentication and authorization services. When down, nothing can occur.
 - ▶ High security – these systems may maintain a large number of person attributes, sometimes including personally protected information.



An Identity Management Architecture



April 2003

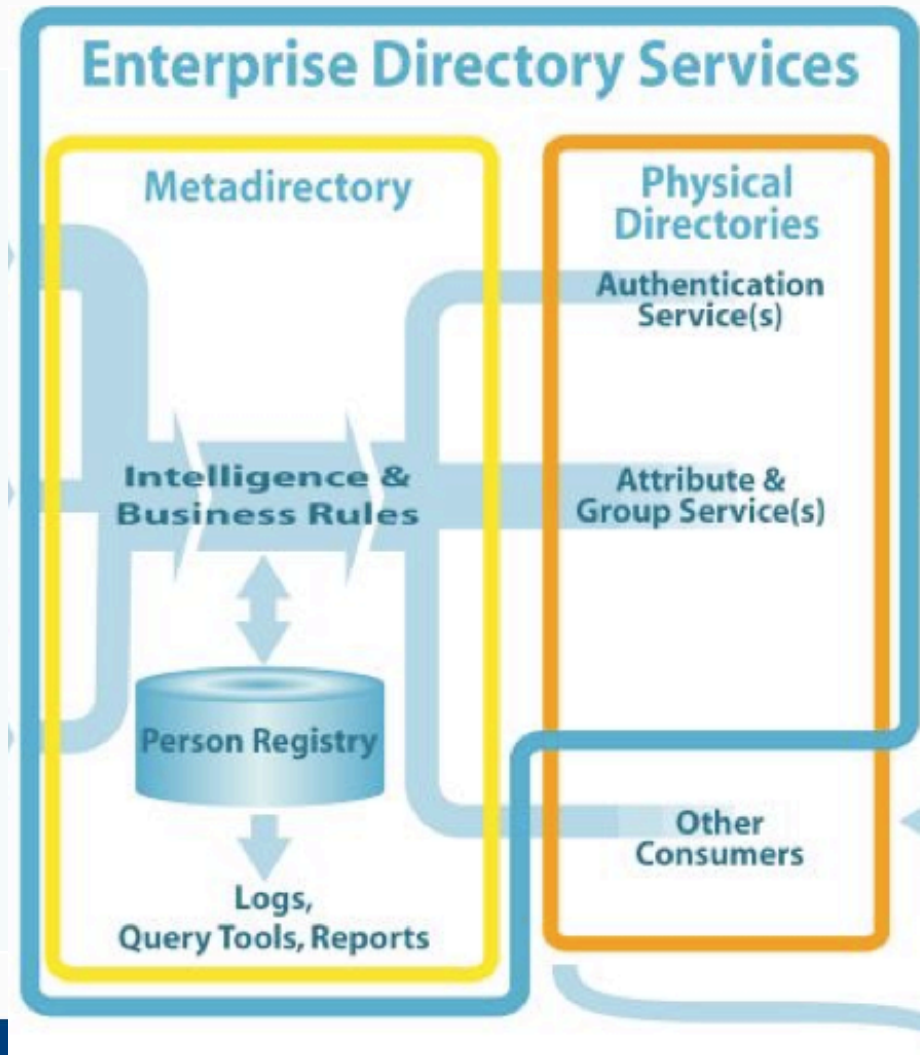
Identifying Authoritative Data Sources

- Authoritative data feeds for the Identity Management system may come in real time or batch from your CRM and/or ERP systems.
- Often you have special population groups kept in systems outside of the ERP or CRM.
- Some systems may provide periodic, or asynchronous updates or be polled for new information.
- For auditors, understanding what data sources are used and the lag time to updating the IDMS system is essential to enforcing policy.




Enterprise Directory Services

- This slide forms the core of an identity management system.
- Metadirectory is usually the IDMS database schema that is updated by the core data sources.
- Physical directories, called LDAP, provide an interface to services.
- For auditors, understanding how to validate that the business rules are implemented and followed is essential.



Applications and Services

- Applications and services are the consumers of an IDMS. Examples include:
 - Authentication - Who am I?
 - Authorization services – What can I do?
 - Portals are often a common application
- Services may reside locally or be provided by off-campus providers through Software-as-a-Service (SaaS) or Service Oriented Architecture (SOA) methods.
- Audit issue is how you validate partners are meeting service requirements and managing data appropriately?



Applications &
Service Platforms

Level of Assurance in IDMS

- ▶ IDMS systems have often been business enablers for connecting customers or external business partners.
- ▶ Questions?
 - ▶ Do all account holders have access to all services and generate the same level of risk?
 - ▶ Do you have the same level of confidence that the identity associated with an account is who they purport to be for all your account holders?
- ▶ If you answered no, you might look at integrating level of assurance into your IDMS.

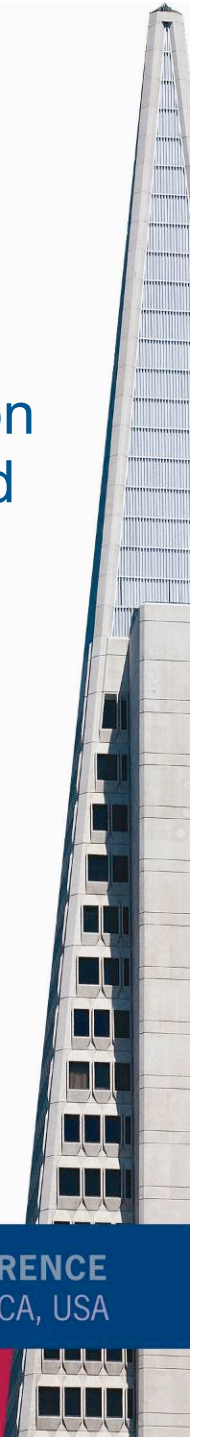


Overview of Level of Assurance in IDMS

▶ Two distinct uses

1. For a **service provider**, the level of risk to the application or organization if an incorrectly identified user is allowed to access the application or perform a transaction. This can happen if someone compromises an account password.
2. For an **identity provider**, the risk that the person is not who they claim to be – in this case the person has legitimate credentials that they acquired fraudulently

- ## ▶ Organizations often perform both functions and must look at both risks.



U.S. Federal Government eAuthentication Initiative

<http://www.cio.gov/eauthentication/>



Today's Date is: 24-June-2008

[Home](#)

[Key Personnel](#)

[Federation Applications](#)

[Federation Links](#)

[Federation Members](#)

[Newsroom](#)

ANNOUNCEMENTS

GSA's HSPD-12 MSO wins Outstanding Issuing Organization Award

The HSPD-12 MSO won the 2008 Smart Card Alliance Outstanding Issuing Organization award at the CTST 2008 Americas Conference and Exhibition currently taking place in Orlando, Florida. The HSPD-12 MSO won for its role in personalizing and issuing the federal government's Personal Identity Verification cards for more than 65 federal agencies and departments; the PIV is a common, government-wide smart card credential for both physical access control and information security that is being issued to all federal government employees and subcontractors. [For more information...](#)

Background on E-Authentication Solution and the US E-Authentication Identity Federation

US E-AUTH IDENTITY FEDERATION

- Membership Documents
- Technical Architecture
- E-Authentication Portal
- Interoperability Testing
- Approved Product Vendors
- **FIDCS Acquisition Information**

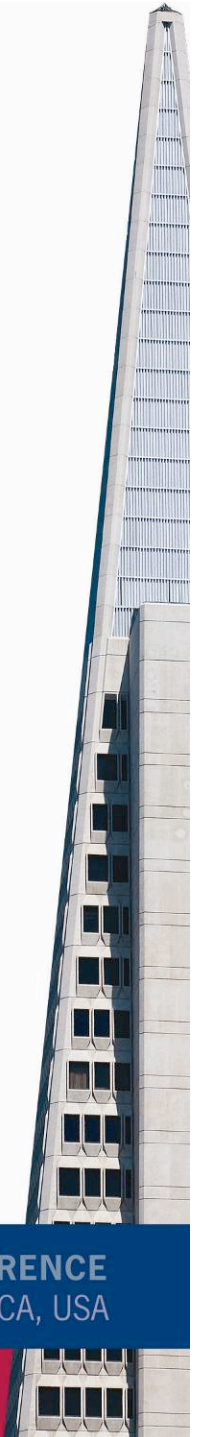
POLICY

- Guidance for Federal Agencies
- NIST Special Publication 800-63
- X.509 CP for E-Governance CA's

FOUR GOLDEN GATE TO EXCELLENCE

Assurance as an Identity Provider

- ▶ A combination of assurance that the person presenting their credentials is who they say they are AND they are the person presenting the credentials.
 - ▶ The degree of confidence in the vetting process; and
 - ▶ The degree of confidence that the person presenting the credential is the person you issued the credential to
- ▶ Level 1 – little or no assurance
- ▶ Level 2 – some confidence
- ▶ Level 3 – high confidence
- ▶ Level 4 – very high confidence

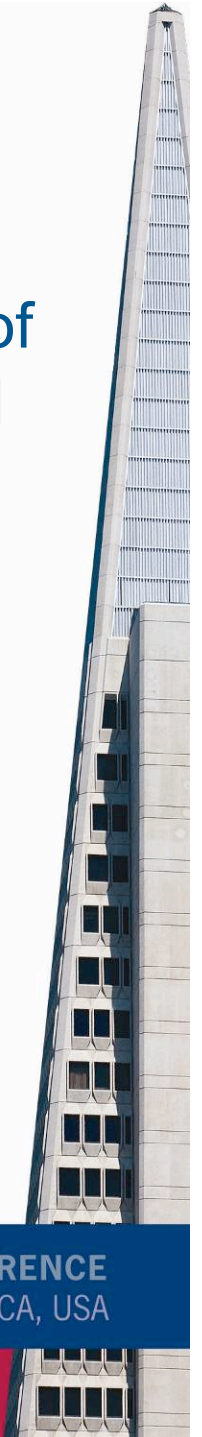


Assurance as an Identity Provider

- ▶ eAuthentication guidelines require that everyone is identity proofed.
- ▶ We define another group – level 0. Level 0 has no assurance the person is who they say they are. These are guests that assert their identity and want a portal account. We have no way of verifying they are who they say they are
- ▶ Audit plays an important role in assessing and validating the procedures for initial identity proofing. We do this when issuing our ID card.

Assurance of Credentials

- ▶ The second component of assurance is the assurance of the credential as presented by the person it was issued too.
- ▶ Traditional authentication focuses on password management. Level 2 is the highest assurance a text-based password can achieve.
- ▶ For level 3 or 4 assurance eAuthentication requires two-factor authentication. The second factor must be some token that is issued to the user. The US government is moving to smart ID-cards under the auspices of HSPD-12.



Credential Assurance

NIST 800-63 guide provides excellent framework for managing credentials.

The entropy spreadsheet is a great tool for reviewing password practices and looking at how subtle variations in policy practices change the strength of the credentials.

This is a great tool for auditors!

THE E-AUTHENTICATION CREDENTIAL ASSESSMENT SUITE

- [Guide to Preparing for a Credential Assessment](#)
- [Certificate Credential Assessment Profile](#)
- [Password Credential Assessment Profile](#)
- [Credential Assessment Framework](#)
- [Entropy Spreadsheet, v2.0.0](#)



Progress Through Sharing

2008 INTERNATIONAL CONFERENCE

July 6-9 / San Francisco, CA, USA

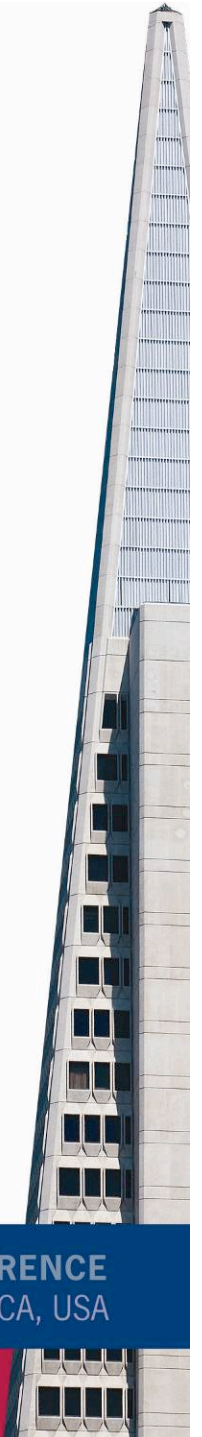
YOUR GOLDEN GATE TO EXCELLENCE

An Example – Password Resets

- ▶ Forgotten passwords are often amongst the most common call to the helpdesk.
- ▶ Creating a self-service method to reset your password often is essential for improving customer service and reducing helpdesk costs.
- ▶ However, this creates an opening for attacks to compromise accounts. We are integrating level of assurance into our process.
 - ▶ The 10% of total account holders that have LOA of 2 have a different process than the 90% with LOA of 1.

Assurance for Service Providers

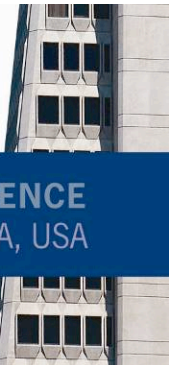
- ▶ Service providers follow traditional risk management approaches such as NIST 800-30 to assess the risk associated with an authentication error:
 - The potential harm or impact, and
 - The likelihood of such harm or impact.
- ▶ Potential categories of harm include: reputation, financial loss, organization harm, release of sensitive information, risk to personal safety, and criminal or civil violations.
- ▶ Ratings use values of low, moderate, or high.



Setting Level of Service Assurance



Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High



Progress Through Sharing

2008 INTERNATIONAL CONFERENCE

July 6-9 / San Francisco, CA, USA

YOUR GOLDEN GATE TO EXCELLENCE

Role of Audit

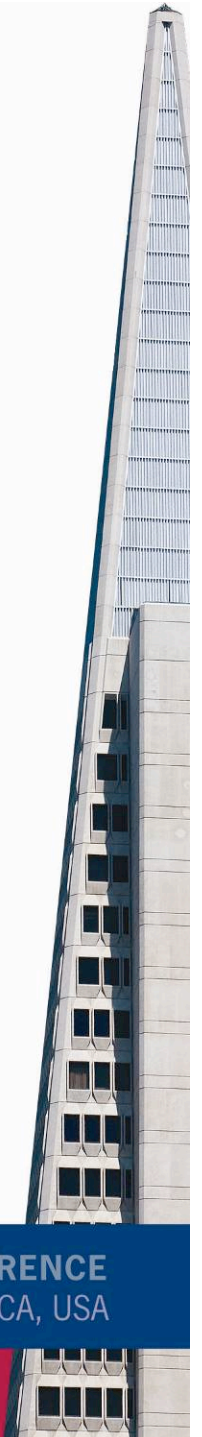
- ▶ Audit should be playing a critical role in helping the organization set assurance levels and validating that practices and policies properly support the assurance granted.
- ▶ Beyond just validating practices and policies, audit has full access to the entire organization and can help shape organizational practices and policies to be better aligned for compliance when these practices cut across organizational boundaries
- ▶ We will discuss the role of audit more when we discuss federations.



Federations and Identity Management

► Federations – definition

- *Dictionary.com* - a federated body formed by a number of nations, states, societies, unions, etc., each **retaining control** of its own internal affairs.
- *Incommon.org* - A federation is an association of organizations that come together to exchange, as appropriate, about their users and resources in order to enable collaborations and transactions.



InCommon Federation – An Example

www.incommonfederation.org

- ▶ Presently about 85 members, approximately 59 higher education institutions, 4 government agencies or non-profit laboratories, and 22 corporations (public and non-profit) representing 1.7 million individuals.
- ▶ Entities agree to a common participation agreement that allows each to inter-operate with the others.
- ▶ InCommon sets basic practices for identity providers and service providers. The primary focus has been technical and focuses on campus identity management procedures and attributes.



InCommon Federation – How is it Used?

- ▶ InCommon uses a technology called Shibboleth (shibboleth.internet2.edu) that uses the security access markup language (SAML) to exchange information.
- ▶ A student at my institution can access external content providers and request information. When they do this the user is directed to authenticate at UMBC and UMBC provides some agreed upon attribute to the content provider validating access (or not).
- ▶ Shibboleth is designed so that you can release the minimal amount of information as necessary.

Benefits of Federations

- ▶ For organizations, without a federation, organizations that want to share information must enter into bilateral agreements. These agreements are difficult to achieve and greatly complicate the work of insuring compliance if each has slightly different terms.
- ▶ For individuals, without a federation, individuals must establish a relationship with each organization, often providing duplicate information to multiple organizations.

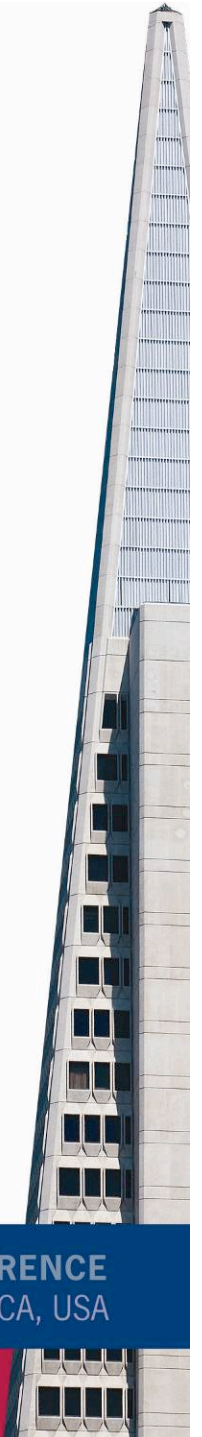
InCommon Federation

- ▶ It has taken three years to reach this point. Recent interest from Microsoft, Google, and Apple will dramatically increase membership.
- ▶ We anticipate that InCommon could double in size every 6 months for the next 3 years, when it could ultimately reach 1000 universities and represent at least 10 million individuals.
- ▶ We are adding new categories for members that need greater security. “Silver” membership will require higher level of assurance for credentials and require an annual audit of practices.



The Evolution of Federations

- ▶ As I look at InCommon I can see the possibility of InCommon supporting many different “Levels.”
- ▶ As the broad use of federation becomes more commonplace we envision that across our users there will be range of applications available through the federation that require different levels of assurance.
- ▶ As a result, managing compliance requires validating each identity is managed appropriately and assigned the proper level of assurance and managed appropriately.



Using the IDMS for Managing Roles and Security

- ▶ Universities are complex – we have systems for student housing, finance, human resources, grants management, student records, admissions, alumni, and library – often to name just a few of the major systems.
- ▶ It is very rare to have a single vendor provide solutions to all of these areas and so we have many different vendors. In many cases we have a different vendor for each major system.
- ▶ In addition, application security is getting much more complex making it staff intensive and difficult to audit for compliance.



[VIEW A PDF
OF THIS ARTICLE](#)

A Security Checklist for ERP Implementations

A study of ERP security issues produced a checklist that shows institutions what to look for while letting vendors know what campuses consider important

By **Joy R. Hughes** and **Robert Beer**

Enterprise resource planning (ERP) systems are often the single most expensive software system that a CIO will ever implement. When all costs are considered—hardware, software, network upgrades, staff time, training, and consultants—an ERP system can cost \$10–\$50 million to implement. Millions of dollars can be spent just to provide the same level of management information that the hundreds of reports designed to work with the old system provided. Unsuccessful implementations and huge cost overruns are not uncommon and can lead to legal action by the school against the ERP vendor or consultants when the project fails during implementation. Although lawsuits are uncommon, they bring considerable notoriety to an institution and add strength to the mythology of the career-ending ERP implementation.

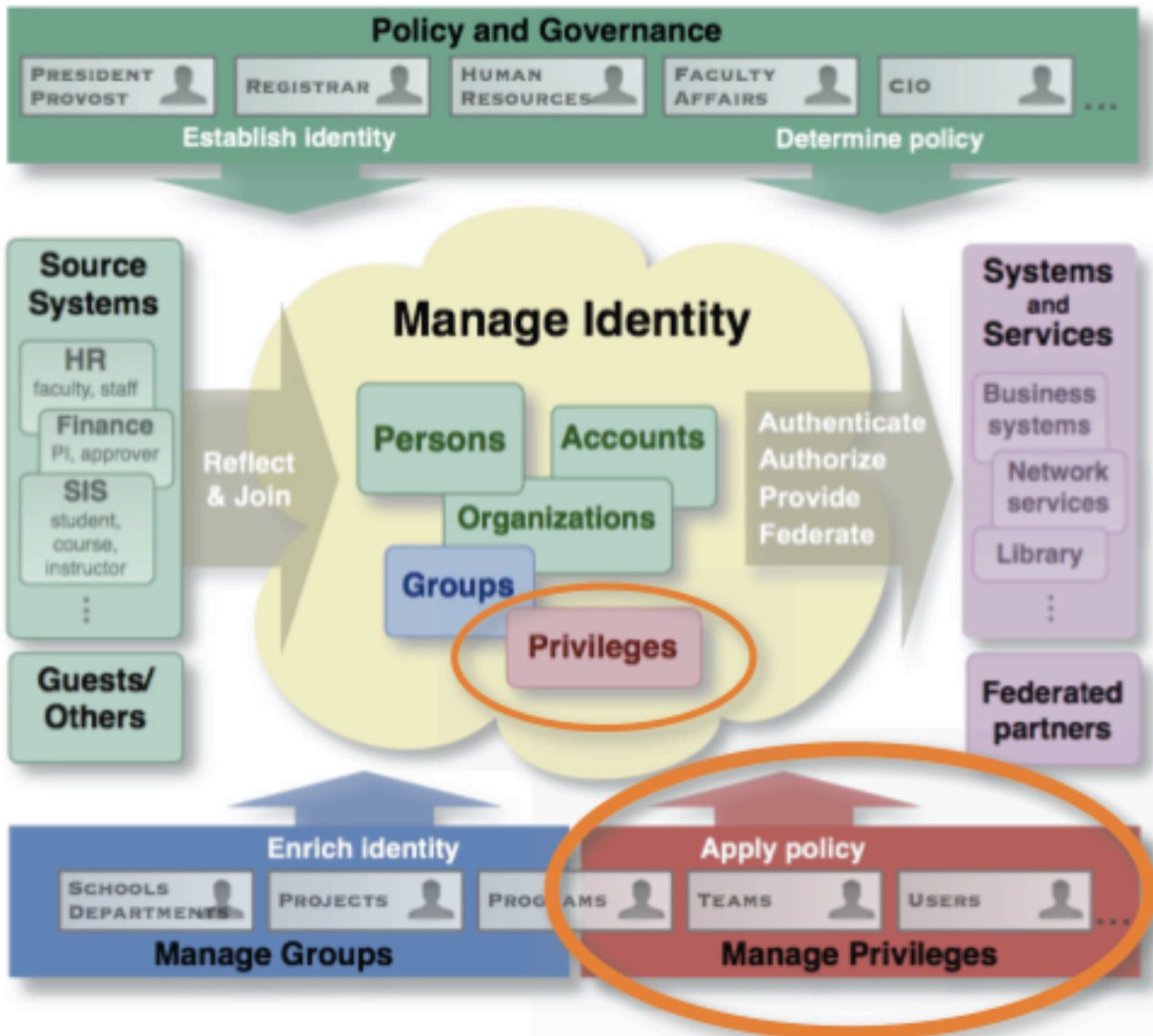
ERP Security Checklist for Vendors

- ▶ The article is from my former co-chair, Joy Hughes.
- ▶ The focus of the article is to highlight the challenges CIO's face in certifying systems are secure. It highlighted 5 areas vendors need to improve.
 - ▶ Reports for managing roles and responsibilities
 - ▶ Password and account management
 - ▶ Insuring data standards and integrity
 - ▶ Automated process documentation
 - ▶ Managing and controlling sensitive data
- ▶ <http://connect.educause.edu/Library/EDUCAUSE+Quarterly/ASecurityChecklistforERPI/45535>

IDMS – Managing Roles and Application Security

- ▶ Internet2 has launched a project called Signet to allow security roles to be managed centrally and have these update the application security.
- ▶ The process is define a security model, assign roles and responsibilities in the IDMS for functions (e.g. approve payroll) and then have a specially developed connector update the security in the application based on changes in the IDMS.
- ▶ The benefit is that as an employees status changes you can make the change in one place and propagate to all systems.





Signet's Role in the Identity and Access Management (IAM) Model

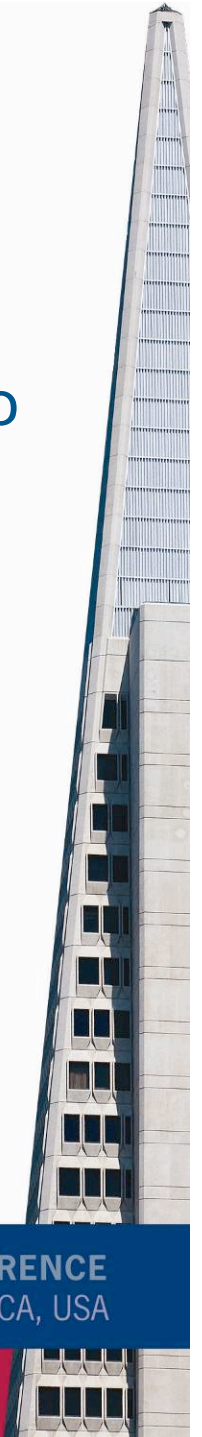


Key Elements of SIGNET

- ▶ Provide a single point for managing authorization without consolidating control. Business owners have a web interface for managing who has access.
- ▶ Allows centralized IDMS services to be leveraged for business applications and security, such as when a person leaves the organization or changes roles.
- ▶ Helps enable business groups and users through a consistent approach to security

Vendor Solutions for Managing Application Security - Oracle

- ▶ Oracle has purchased a number of the leading companies in the middleware space – Oblix and BEA to name a few and has a well thought out plan.
- ▶ Oracle's Fusion Middleware product is moving to redefine the way that security is provisioned in Oracle Fusion applications. There will be mechanisms for provisioning non-Oracle applications



Oracle Middleware

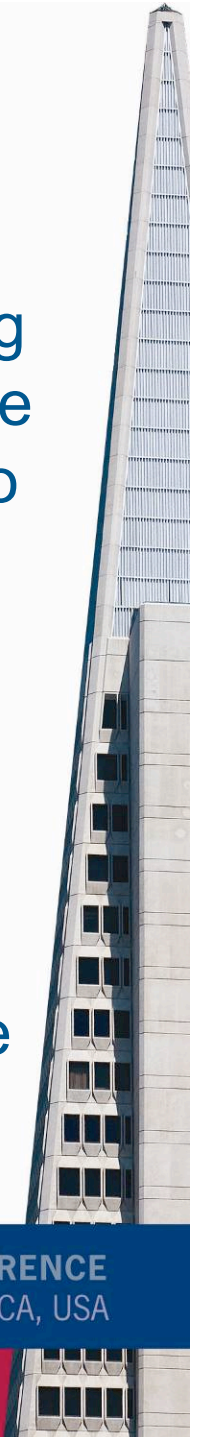
Oracle has one of the most comprehensive set of IDMS solutions among vendors. It is quite complete but also quite complex and in my opinion requires strong technical resources to implement.

▲ ORACLE IDENTITY MANAGEMENT SOLUTIONS

- ➔ [Oracle Access Manager](#)
- ➔ [Oracle Adaptive Access Manager](#)
- ➔ [Oracle Identity Manager](#)
- ➔ [Oracle Role Manager](#)
- ➔ [Oracle Identity Federation](#)
- ➔ [Oracle Internet Directory](#)
- ➔ [Oracle Virtual Directory](#)
- ➔ [Oracle Web Services Manager](#)
- ➔ [Oracle Enterprise Single Sign-On Suite](#)
- ➔ [Oracle Entitlements Server](#)
- ➔ [Oracle Management Pack for Identity Management](#)
- ➔ [Oracle Identity & Access Management Suite](#)
- ➔ [Oracle I&AM Suite for Mid-Sized Businesses](#)
- ➔ [Oracle Authentication Services for Operating Systems](#)

Vendor Solutions for Managing Application Security - Microsoft

- ▶ Microsoft has been building a solid system by leveraging its investment in Active Directory. Microsoft released the Microsoft Identity Management System a few years ago and in higher education we see increased adoption.
- ▶ Microsoft has recently announced the Microsoft Identity Lifecycle Manager 2.0 (ILM) system. This builds on the prior system and adds much better provisioning, credential management, and support for some of the emerging web-services standards. Groups making heavy use of Windows Server and/or Sharepoint will be targeted.





Identity Lifecycle Manager "2"

Identity Management is about to get a lot easier

ILM "2" Feature Highlights:

Policy Management

- SharePoint-based console for policy authoring, enforcement & auditing
- Extensible WS-* APIs and Windows Workflow Foundation workflows
- Heterogeneous identity synchronization & consistency

Credential Management

- Heterogeneous certificate management with 3rd party CA support
- Management of multiple credential types, including OTP
- Self-service password reset integrated with Windows logon

User Management

- Integrated provisioning of identities, credentials, and resources
- Automated, codeless user provisioning and deprovisioning
- Self-service user profile management

Group Management

- Rich Office-based self-service group management tools
- Offline approvals through Office
- Automated group and distribution list updates



Progress Through Sharing

2008 INTERNATIONAL CONFERENCE

July 6-9 / San Francisco, CA, USA

YOUR GOLDEN GATE TO EXCELLENCE

Web Services – Service Oriented Architecture

- ▶ Service oriented architecture (SOA) leverages the web to provide services. The goal of SOA is that as the web becomes the application delivery platform there will be components done elsewhere that you want to integrate into your application.
- ▶ There are a set of standards (multiple) that define how web services will interoperate and manage authorization and access to these web services.
- ▶ Ultimately, for the promise of web services to be realized there will need to be solutions that reside outside of the application as part of an overarching IDMS system.



Web Services Standards Overview

Interoperability Issues



Standard Bodies

Business Process Specifications



Management Specifications



Presentation Specifications



Metadata Specifications



Reliability Specifications



Security Specifications



Transaction Specifications



Resource Specifications



Messaging Specifications



SOAP



XML Specifications



Dependencies

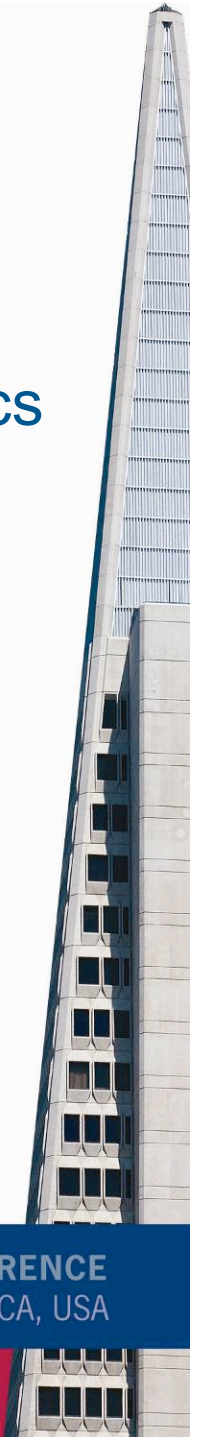


innoQ Development GmbH
 innoQstraße 11
 D-6880 Pirmasens
 Phone: +49 7109 31100-400
 info@innoq.com - www.innoq.com

innoQ Service Desk
 Dienstleistungs IT
 68440 Darm
 Phone: +49 6154 9000-10

Longer Term Approaches

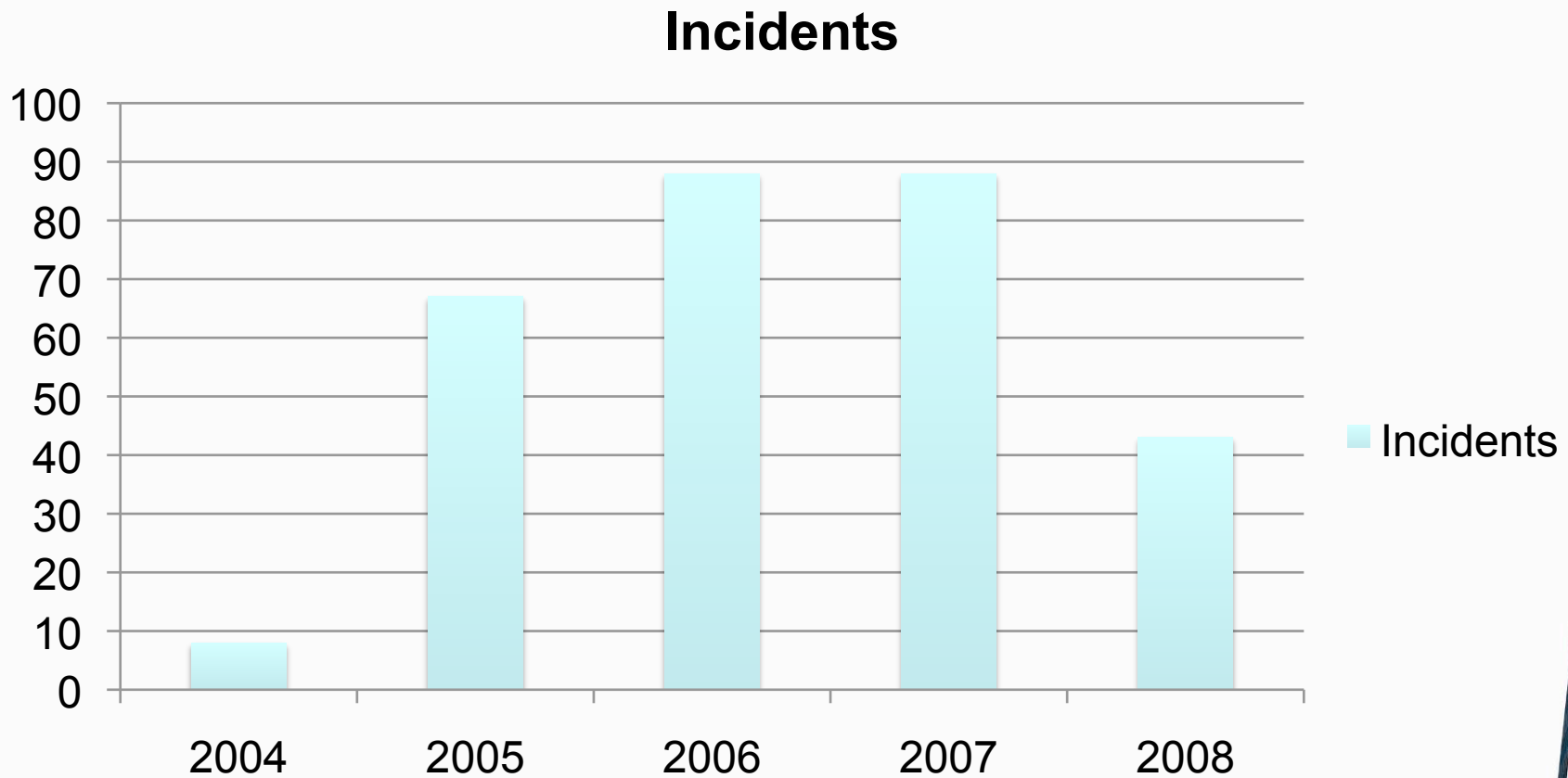
- ▶ The WWW consortium (W3C) is working on standards for autonomous policy engines that take policy heuristics in an XML format and exchange and manage them across independent groups.
- ▶ There seems to be momentum in moving to SOA and that will ultimately drive standards and direction as applications emerge that support business innovation.
- ▶ Companies may initially have two approaches, one for internal desktop applications and the other for extranet applications.



Managing and Protecting Privacy

- ▶ My sector, higher education, has had a large number of non-public information (NPI) data releases. Primarily this is associated with our past heavy use of social security numbers.
- ▶ Privacyrights.org lists 184 releases in first 6 months of 2008, 43 were universities.
 - ▶ Higher education's total is lower in 2008 than in 2007 and we seem to be making some progress in that our overall percentage of releases is going down.

Higher Education Data Security Incidents



Progress Through Sharing

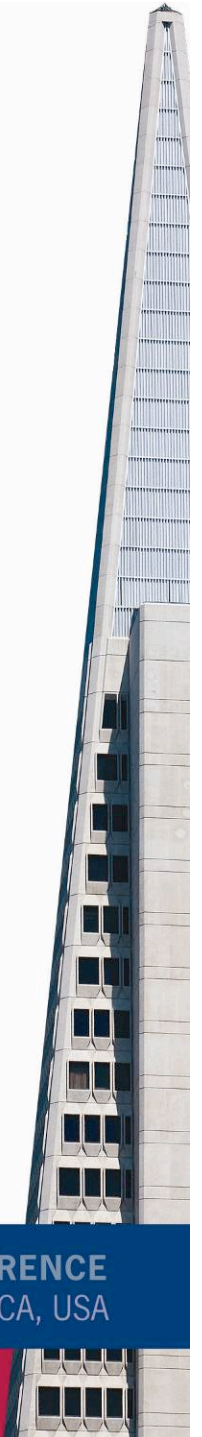
2008 INTERNATIONAL CONFERENCE

July 6-9 / San Francisco, CA, USA

YOUR GOLDEN GATE TO EXCELLENCE

Interesting Statistics

- ▶ Data as of July 2007
- ▶ Higher education was responsible for 5.8 million of the “official” 140 million identities that had been released.
- ▶ The median size of a data release in higher education was 4719.
- ▶ 5% of the incidents accounted for 2.7 million of the 5.8 identities that were released (47% of the total).
- ▶ 20% of the incidents accounted for 80% of the identities released (4.8 million)



What Do These Statistics Imply?

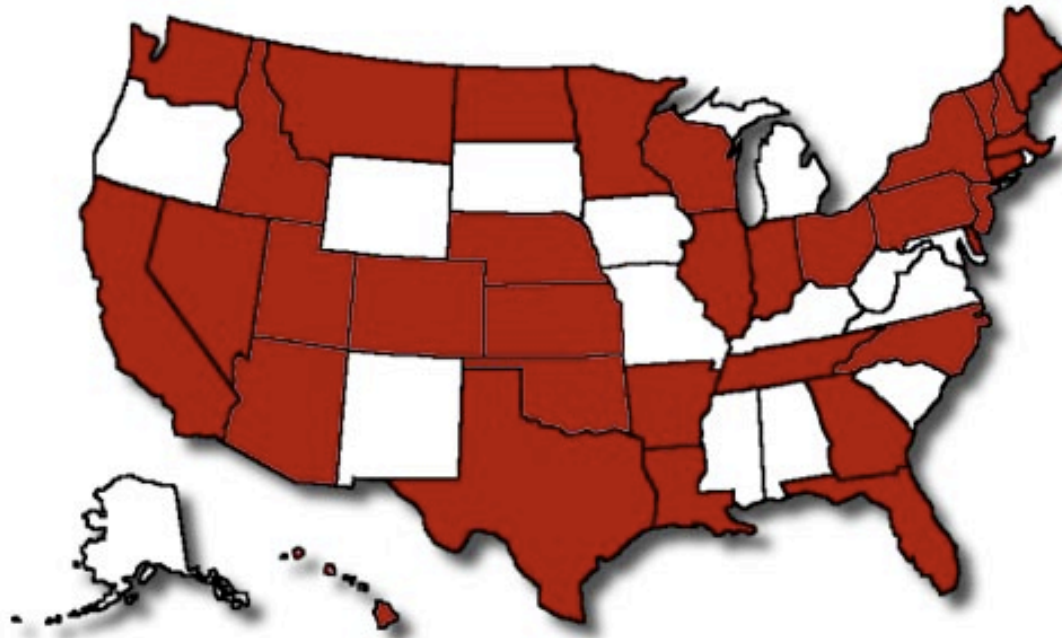
- ▶ Small incidents dominate the statistics.
- ▶ Many of the incidents revolve around individuals having access to data that had sensitive information (NPI) and not taking adequate security procedures.
- ▶ Data management – knowing who has access to sensitive data, and then taking appropriate measures, is a key aspect of protecting that data.
- ▶ Large incidents often revolve ancillary business systems that are run outside of central IT.



States With Disclosure Notification Laws (Courtesy U. Georgia.)

State Security Breach Notification Laws (as of October 1, 2006)

State Security Breach Laws are requiring businesses, nonprofits, and state institutions to notify consumers when unencrypted "personal information" may have been compromised lost, or stolen. So far, 34 states have passed this law.



Identity Management and NPI

- ▶ At UMBC, our Identity Management system was instrumental in remediating our use of SSN across different business systems. We integrated our ID card into the system and did away with the using SSN as a primary identifier.
- ▶ We built better tools for identity lookup, including presenting the ID picture to validate the person, through the Identity Management system. As part of this effort we built in strict controls on who has access to view someone's full or partial SSN.



Future Directions for Identity Management and NPI

- ▶ At UMBC, we have purchased a tool, Asarium, that allows us to track whether NPI is on a device.
- ▶ We want to integrate data management privileges into our IDMS and use the IDMS to verify who has gone through formal data management training and who has NPI on their machine.
- ▶ We will then use the IDMS to show us who is and isn't allowed to have NPI on their machine and use that to inform our compliance efforts – either removing the NPI or making certain that compliance training has occurred.

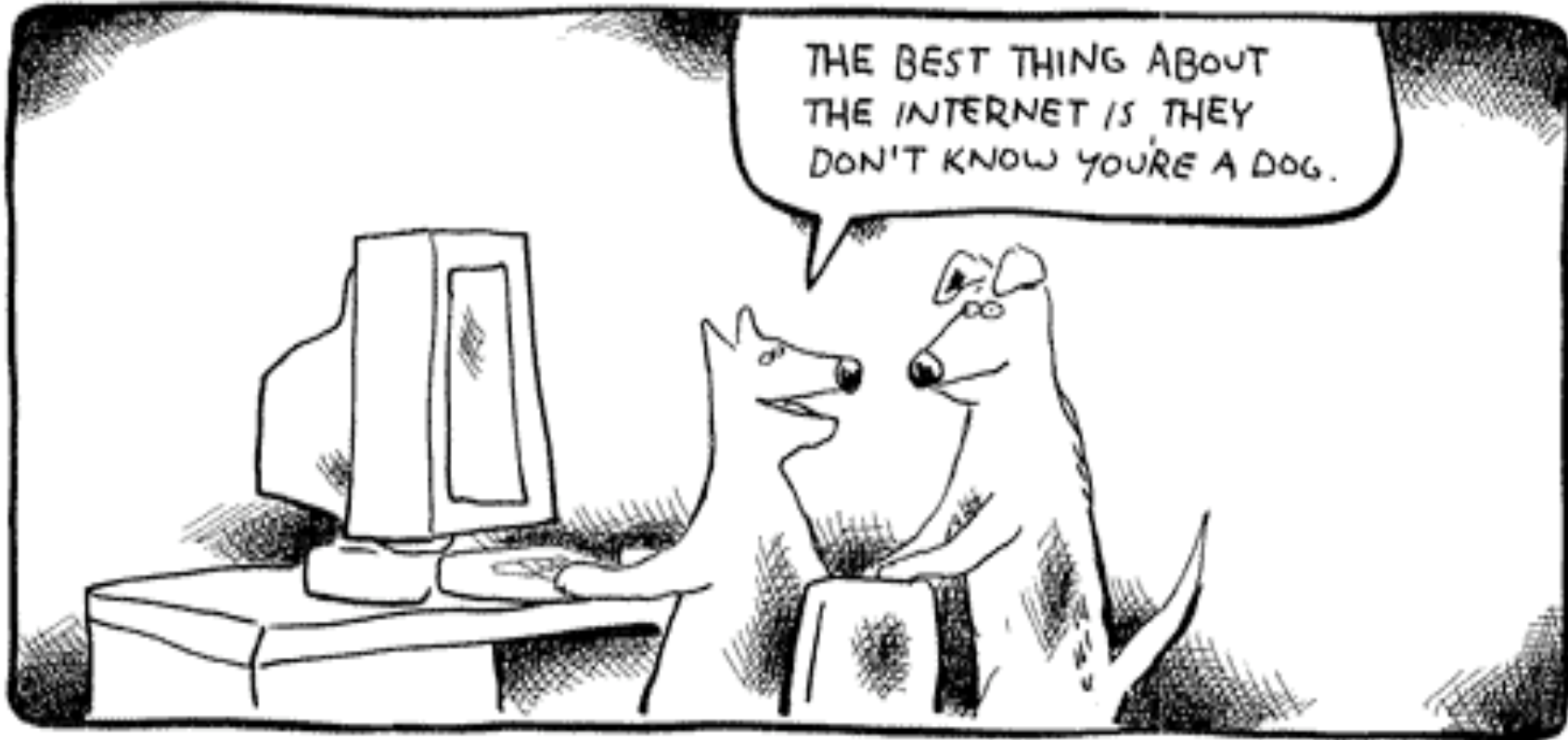
Role of Internal Audit In Protecting NPI

- ▶ Internal audit can be very helpful in the development of processes and procedures to help with compliance.
- ▶ Their insight has been critical to the idea of improving data management by centrally tracking in our IDMS compliance training, access rights, and verifying what machines are allowed to have NPI on them.
- ▶ In working to develop this system we are planning to use internal audit to help with compliance reviews within central IT and with departments on campus.



Broader Privacy Issues

- ▶ Increasingly through either state laws or as a result of the European Union privacy efforts we are going to have to manage varying rules for what is private information and how to manage that information based on the relevant jurisdiction of the individual.
- ▶ Additionally, as the EU rules take hold we will need to recognize what outside groups we can share information with and what attributes can be released on individuals to different entities.



"The best thing about the Internet is they don't know you're a dog."

Tom Toles. *Buffalo News*, April 4, 2000.



Progress Through Sharing

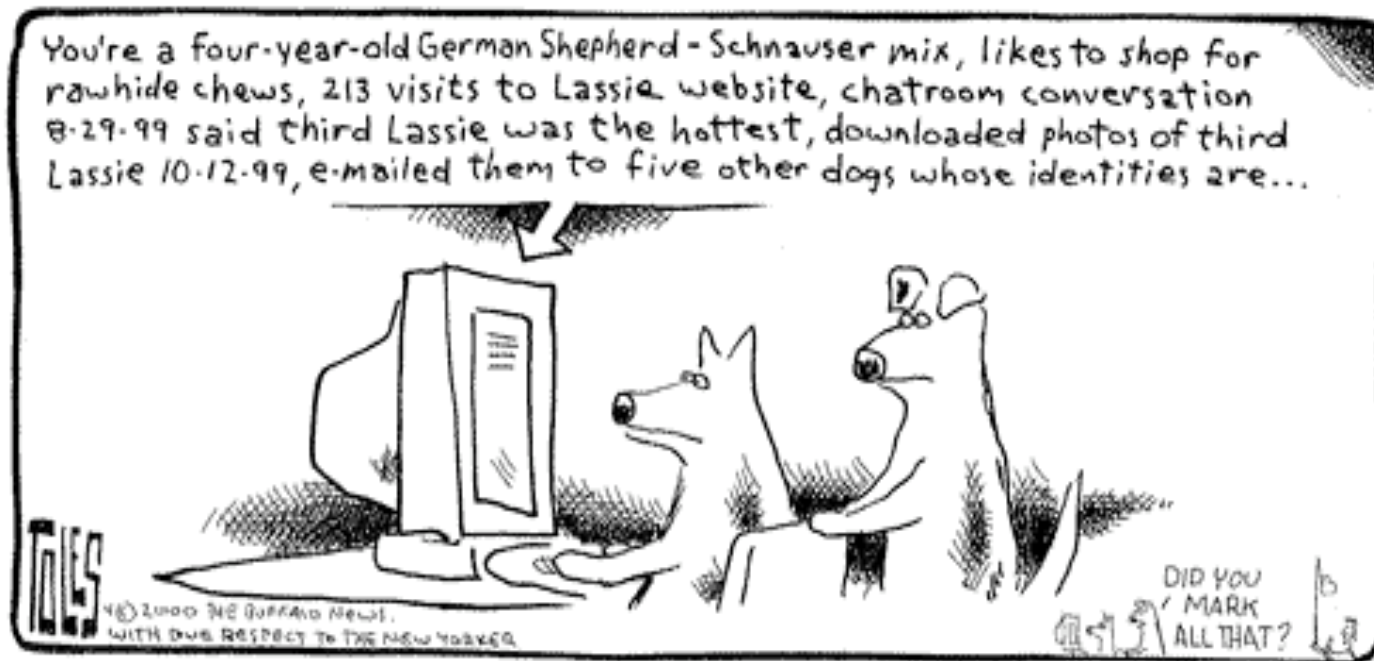
ATC - 3 October
2004

2008 INTERNATIONAL CONFERENCE

July 6-9 / San Francisco, CA, USA

54

YOUR GOLDEN GATE TO EXCELLENCE



“You’re a four-year-old German Shephard-Schnauser mix, likes to shop for rawhide chews, 213 visits to Lassie website, chatroom conversation 8-29-99 said third Lassie was the hottest, downloaded photos of third Lassie 10-12-99, e-mailed them to five other dogs whose identities are...”

Kim Cameron's Identity Blog

Kim Cameron is Microsoft's Chief Architect of Identity.

His blog is a very good place to get thoughtful discussion on identity.

<http://www.identityblog.com/>



Kim Cameron's Laws of Identity Whitepaper

Seven Laws of Identity

1. User control and consent
2. Minimal disclosure for a constrained use
3. Limit relationships to justifiable parties
4. Control over who can see my identifier, directed identity
5. Pluralism of operators and technologies
6. Human integration
7. Consistent experience across contexts



Dick Hardt's Identity 2.0 Presentation at OSCON

- ▶ One of the best presentations on identity management is by Dick Hardt at OSCON 2005.
- ▶ This is a good overview of looking at how identity management may evolve. In 15 minutes he gives a great presentation.
- ▶ <http://www.identity20.com/media/OSCON2005/>

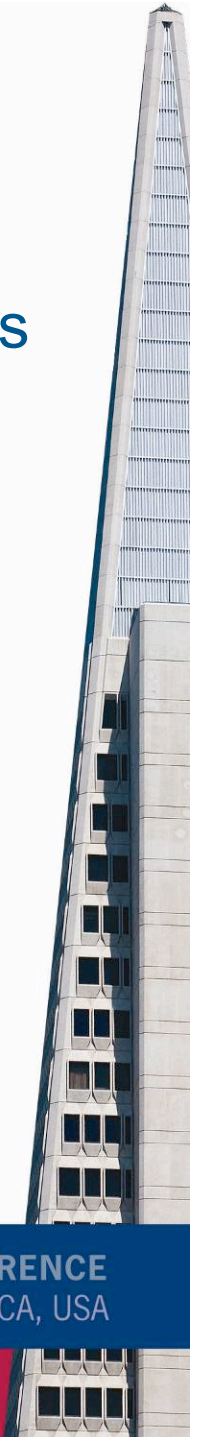


Progress Through Sharing

2008 INTERNATIONAL CONFERENCE

July 6–9 / San Francisco, CA, USA

YOUR GOLDEN GATE TO EXCELLENCE





Identity 2.0

The next generation of Identity

OSCON 2005 Keynote - Identity 2.0 [RSS 2.0](#)

Dick Hardt | Founder & CEO, Sxip Identity

Watch Dick deliver a compelling and dynamic introduction on Identity 2.0 and how the concept of digital identity is evolving.

“Dick Hardt is brilliant. Watch (and copy) the style. Learn tons from the substance.” - [Lawrence Lessig](#)

“Really captures the complexities of participating in an online world and how identity is at the center of the Web experience.” - [Dan Farber](#)

“A barn-burner of a presentation. I loved this.” - [Cory Doctorow](#)

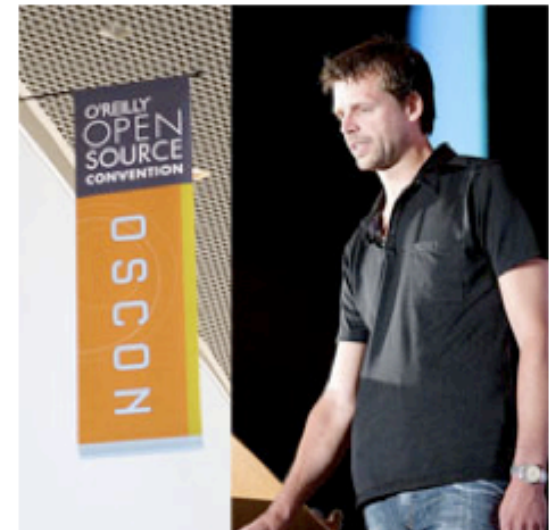


Photo by James Duncan Davidson/O'Reilly Media, Inc.



Progress Through Sharing

2008 INTERNATIONAL CONFERENCE

July 6–9 / San Francisco, CA, USA

YOUR GOLDEN GATE TO EXCELLENCE

Dick Hardt's 2005 OSCON Video on Identity 2.0

O'REILLY
OPEN SOURCE
CONVENTION

Keynote
Identity 2.0

Dick Hardt
Founder and CEO | Sxip Identity



Progress Through Sharing

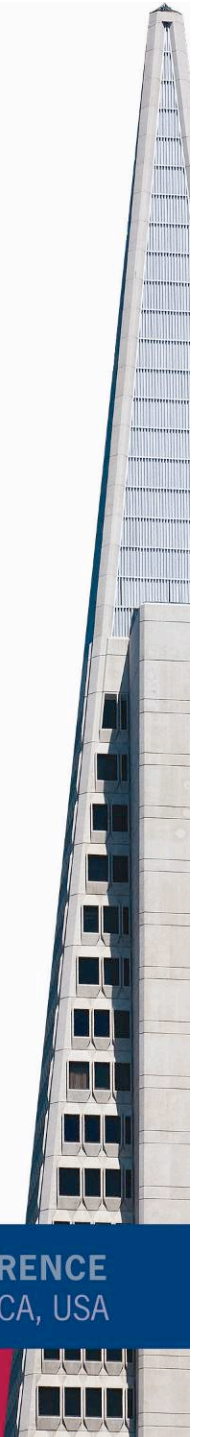
2008 INTERNATIONAL CONFERENCE

July 6-9 / San Francisco, CA, USA

YOUR GOLDEN GATE TO EXCELLENCE

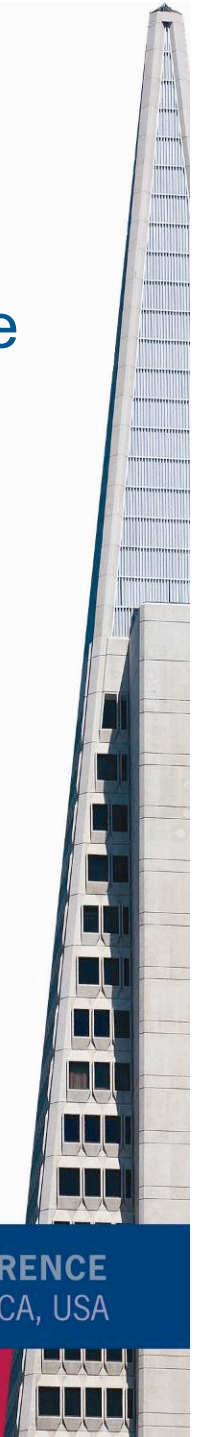
Implications for IDMS

- ▶ We are in the beginning stages of managing identity.
- ▶ There won't be a single identity provider solution.
- ▶ The human integration component is critical and we need to create something flexible that people can consistently use.
- ▶ We will see a lot of products and technologies over the next 5 years because this is a critical component in making the Internet usable.



Technical Frameworks to Build On

- ▶ I have been following the work of the Burton group since 2000 and feel they are among the thought leaders in this space.
 - ▶ 2002 – their whitepaper on Virtual Enterprise Networks
 - ▶ 2003 – updated to consider SOX
 - ▶ 2004 – worked with Network Applications Consortium to develop a white paper titled *Enterprise Security Architecture*.
 - ▶ 2007 -The Open Group Architecture Forum
<http://www.opengroup.org/togaf>



Policy frameworks to Build Upon

- ▶ The evolution of security processes and procedures from ISO 17799 to ISO 27003 provides a strong foundation for risk management and developing strong internal controls as these pertain to security.
- ▶ While much of the ISO 27003 program is helpful to building a strong identity management function it was not necessarily written for this function. As the IDMS becomes a key business driver we will see the frameworks evolve.
- ▶ We are looking at internal audit to help us bridge some of these gaps while the policy approaches are resolved.



A Few Key IDMS Issues for Audit

- ▶ Define the level of assurance required for different applications supported by IDMS.
 - ▶ IDMS activity logging – how much should be kept and who has access.
 - ▶ IDMS activity reporting – what reports should be produced and when.
 - ▶ Rules for identity proofing and credentials
 - ▶ Compliance with federation requirements
- ▶ IDMS user self-service – how do we integrate user privacy and company compliance into the interface.



More Information

Jack Suess, VP of IT, UMBC (www.umbc.edu)

Phone – 410.455.3208

Email – jack@umbc.edu

URL – <http://userpages.umbc.edu/~jack>

This presentation –

<http://userpages.umbc.edu/~jack/talks/iia-talk.pdf>

Questions

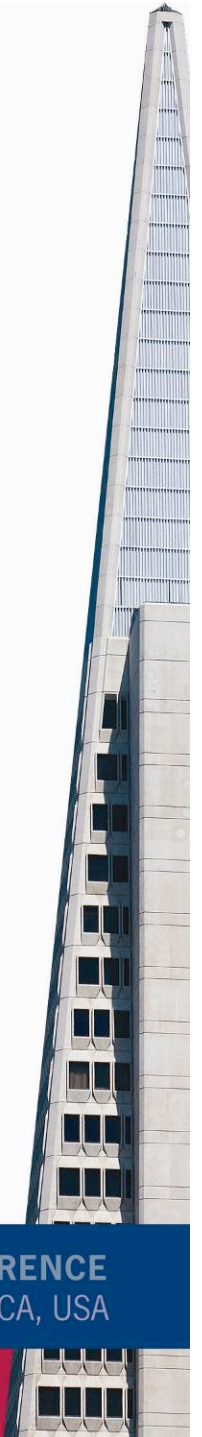


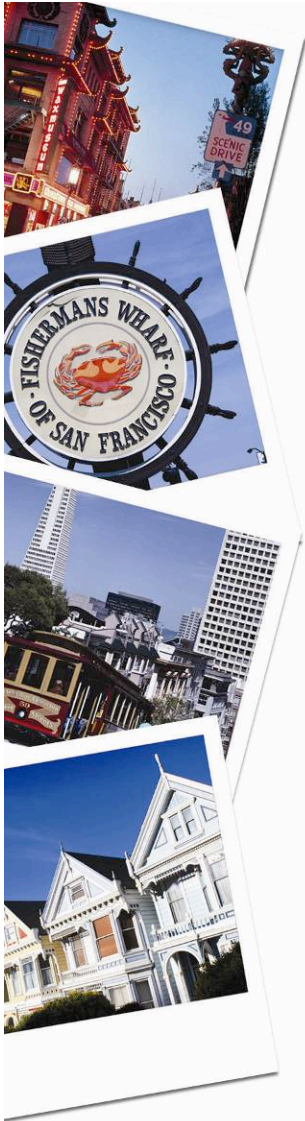
Progress Through Sharing

2008 INTERNATIONAL CONFERENCE

July 6–9 / San Francisco, CA, USA

YOUR GOLDEN GATE TO EXCELLENCE





YOUR GOLDEN GATE TO EXCELLENCE



Progress Through Sharing

2008 INTERNATIONAL CONFERENCE
July 6-9 / San Francisco, CA, USA

San Francisco