THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Defending the Fortress:
New Threats Meet New Defenses

Identity Management Process Design

Steve Jensen

VP/Chief Information Security Officer

Carlson Wagonlit Travel

Agenda

- How to determine if IAM is driven by business processes
- How to align to the business
- 10 step program for successful IAM
- Q&A

IAM Business Requirements

Company Identities

- Provisioning – Give them ALL access NOW!
  - I have no idea what they need (or don't need).
  - Don't you know what they need?
  - I really didn't need it immediately, but rather sooner than later.
- Attestation - Review access to make sure it is appropriate
- De-Provisioning – Remove access after termination or transfer

Customer Identities

- B2B – let client manage identities
- B2C – let customer manager their own identity

Quick Alignment Quiz

What is <u>THE</u> primary reason you are implementing your IAM project?

- ❑ For compliance reasons – because HIPAA, PCI, SOX, (name your compliance program) requires it
- ❑ To enhance the security of our systems by ensuring access is on a need to know basis
- ❑ To make the security operations team more efficient; save costs in IT through automation
- ❑ To make security easier to do business with, thereby helping the business get involved in identities and access

Primary driver needs to be the business processes

- ❑ For compliance reasons – because HIPAA, PCI, SOX, (name your compliance program) requires it
- ❑ To enhance the security of our systems by ensuring access is on a need to know basis
- ❑ To make the security operations team more efficient; save costs in IT through automation
- ✔ To make security easier to do business with thereby helping the business get involved in identities and access

Traditional Identity Technologies

What everyone seems to purchase

- Identity Manager/Warehouse
- Automated Provisioning
- Password Self Service
- Web Access Management

What often is overlooked

- Request system
- Role management
- Federation/Single Sign-on

My opinion…Why do many IAM projects fail?

Primarily IT/Security focused

- Significant time and energy in tool selection based on IT needs
- Primarily focused on automation and efficiency for IT operations
- Driven by IT requirements (e.g. small number of roles)

Primarily treated as an IT infrastructure project, not like a development project

- Program team should be funded based on gathering business requirements first
- Business Analysts need to be key members of project team
- Program might contain various business pilots

Complexity to Simplicity

Directories	Systems and Servers	Applications and Tools	Databases	Cloud
Active Directory	Mainframe – RACF	SAP	DB2	Google Apps
E-Directory	z/Linux	Lotus Notes	IMS	Salesforce.com
Lotus Notes Directory	Unix	STAR	Oracle	Gmail
SAP Employee Directory	Microsoft	Focus	SQL	Ebay
⋮	⋮	⋮	⋮	⋮

Step 1 – Identity warehouse

- Leverage purchase by quick-win – password self-service functionality
- Platform coverage should be a key purchasing decision
- You will still need to build custom feeds
  - Legacy systems
  - Externally hosted systems
  - Proprietary security systems
- Move to directory services whenever possible

Step 2 – Enterprise role management

- Either design/build or purchase a role management product
- Ensure product can meet business requirements
- Include role management, role mining, and role attestation as bare-bones minimum requirements
- Plenty of choices now on the market

Step 3 – Define entitlements

- Create entitlements based on business terms
  - Don't attempt enterprise roles on day one
- Map one or more access groups into application entitlements by leveraging documentation, comments, and description fields
- Combine like groups that have been applied on multiple platforms.

Step 4 – Entitlement attestation

- Validate the assignments of application functionality to users
- Must be in business terms
  - No acronyms
  - No technical terms
  - No security specific terms
- Provide timely adjustments

Step 5 – Adjust request system

- Change your request system to request via application entitlements instead of “IT group lingo”
- Immediate business value
- Generate processes to keep in synch
- Can show what access is in place, and they can add checks, or remove checks
- My advice – stay focused and run automated provisioning as a later project

Step 6 – Create enterprise roles

- Only do this with application entitlements in hand.
- Leverage the “set me up like…John Doe” mentality
- Go to each line of business with a plan
- Assign role ownership – usually the manager
- Allow for multiple enterprise roles per person
- Advice – don’t try to align with HR job codes
- Don’t focus on keeping roles to a minimum – you have role management software to deal with the complexity

Step 7 – Role attestation

- Validate the assignments of enterprise roles to users
- Must be in business terms
  - No acronyms
  - No technical terms
  - No security specific terms
- Provide drill-down capabilities to entitlements

Step 8 - Adjust request system (again)

- Change your request system to request a enterprise roles instead or in addition to application entitlements
- New request type – grant access of an enterprise role to an application entitlement
- Generate processes to keep role management in synch
- Again, show what access is in place, and they can add checks, or remove checks

Step 9 – Segregation of Duties

- Solicit from internal audit
- Solicit from risk management
- Provide mutually exclusive entitlements and roles and do not allow a person to have both

Step 10 – Leverage and Measure

- Apply role management from internal employees to address customers, suppliers, business partners, etc.
- Automate the process

The transformation of access

After STEP 1 (Obscure IT Technical Terms)

- SA_ACCTRECCLK
- SAS_CML_GROUP_6
- CARSVIEW
- …

After STEP 3 (Application Entitlements)

- SelectAccount (SAM) Accounts Receivable Clerk Access
- Compliance Audit Review & Reporting System (CARS) - View Access
- …

After STEP 6 (Enterprise Roles)

- Select Account Receivable Clerk

Questions?

Steve Jensen
Carlson Wagonlit Travel
sgjensen@carlsonwagonlit.com
Linkedin   Twitter:sgjense