Outline of Identity and Access Management (IAM)

- IAM Introduction
  - Drivers
  - Approaches

- IAM Ecosystem
  - directories / meta-directories
  - identity management and governance
  - access management
  - federation

- IAM Program Considerations
Compliance: the pain chain

1. Are we properly managing user access? Will our security controls pass the next audit?
2. Could you prove that John Smith has “appropriate” permissions for his job?
3. Can you confirm that John Smith has the proper access?
4. I can tell you what access John has – I can’t tell if it’s appropriate
5. Can you confirm that John Smith has the proper entitlements?
6. I could… If I was technical enough to understand all these IT details…

CFO, CEO, CRO

Application Managers

IT Security

Auditors

Business Manager
Typical Identity Management Inefficiencies - Gaps

Need to automate complex, administrator intensive Identity management business processes

<table>
<thead>
<tr>
<th>Provisioning New Users</th>
<th>Elapsed turn-on time for users is up to 12 days</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing Users</td>
<td>Help Desk costs $20 per call for pw resets</td>
</tr>
<tr>
<td>De-provisioning Users</td>
<td>30-60% of existing accounts are invalid</td>
</tr>
<tr>
<td>Deploying New Initiatives</td>
<td>Up to 30% of application development time is for access control</td>
</tr>
</tbody>
</table>
The Threat from Within

**Improper Use of Corp Data**

- 59% of workers who left their positions took confidential information with them
- 67% used their former company's confidential information to leverage a new job

**Time to terminate access**

- 24% still had access to corp systems

Source: “Data Loss Risks During Downsizing”, Ponemon Institute LLC, Feb 23, 2009
4 Core A’s of IAM

- Administration
- Authentication
- Authorization
- Audit

5th A

- Analytics
Integrated Decentralized Identity Management

Bottom Up

Enterprise Directory

Data Integration Processes

APP

APP

APP
Centralized Identity Management

Access Management Service

Enterprise Directory

Account Provisioning Service

Top Down
Identity and Access Mgmt
Directory Mythology

- **Myth:** An enterprise directory provides SSO
  - **Truth:** an enterprise directory could be the basis for SSO

- **Myth:** An enterprise directory provides centralized access control
  - **Truth:** only if all apps are enabled

- **Myth:** An enterprise directory solves all my acct provisioning issues
  - **Truth:** not all apps/OSs/dbs/etc. are enabled
  - **Truth:** still lacks workflow processing, end user interface, reconciliation

- **Myth:** An enterprise directory can replace all other directories
  - **Truth:** z/OS→RACF, Windows→AD, etc.
Identity and Access Mgmt

Identity Infrastructure

Meta(beyond)-directory

Directory

Sync

Store
Meta-Directory Fashion

Hierarchical

Distributed

Virtual
Identity and Access Mgmt

- Identity Mgmt
  - Admin
- Identity Applications
- Identity Infrastructure
  - Meta-directory
  - Directory
  - Store
  - Sync
Automating the Identity Lifecycle

- Identity change (add/del/mod)
- Access policy evaluated
- Approvals gathered
- Accounts updated

Automatically detect and correct local privilege settings

Accounts on different types of systems managed -- plus, in-house systems & portals

Integrated Web Console

HR Systems/Identity Stores

Operating Systems
Databases
Applications
Identity Management Flexibility: Request-based and Automated

The user provisioning approach a company uses is an evolving process

Operational Labor Required

Hybrid Approach

Initial Policy
Design Investment

Identity Mgmt System

Admin GUI
or custom front-end

Lifecycle Changes

Role Management

Rule or role based
Identity and Access Mgmt

Identity Applications
- Identity Mgmt
- Role Mgmt
- Admin

Identity Infrastructure
- Meta-directory
- Directory
- Sync
- Store

Identity and Access Management Diagram
Without Roles: Typical Practice

- **User:**
  - the entity requesting access to a resource
  - Ex: John Smith, AppXYZ

- **Resource:**
  - Ex: app, data base, table, etc.

- **Entitlement:**
  - a permission to access a particular resource
  - Ex: open table, read record, write record
With Roles: Best Practice

- **User:**
  - the entity requesting access to a resource
  - Ex: John Smith, AppXYZ

- **Resource:**
  - Ex: app, data base, table, etc.

- **Entitlement:**
  - a permission to access a particular resource
  - Ex: open table, read record, write record

- **Business role:**
  - a logical collection of users performing a similar business function
  - Ex: Doctor, Nurse, Lab Tech

- **Application role:**
  - a logical collection of entitlements needed to perform a particular task
  - Ex: create patient record, discharge patient, view X-rays, etc.)
Identity and Access Mgmt

Identity Mgmt

Access Mgmt

Meta-directory

Directory

Sync

Store

Identity Infrastructure

Identity Applications

Admin

Role Mgmt

Enforce
End User Authentication – Typical

- User authenticates to each application separately
- User must remember passwords
- User calls helpdesk for password reset
- User changes passwords manually
End User Authentication – Best Practice

- User authenticates to SSO manager
- All other logins automated
- Password reset by user at desktop
- Password change automated

Enterprise Single Sign-On

Windows
Intranet Portal
BP Portal
Lotus Notes
VPN Client
3270 Emulator
Citrix
Java Application
Make risk-based authentication decisions – what, who, when -> how

**Resource / Action:**
- The resource being requested and what is being done.
- E.g. Login to view a file vs. submit payment order to existing payee vs. adding a new-payee

**Identity/Entity:**
- Groups, roles, organization, type (person, Thing, application, bot)
- Identity assurance level (employee vs. un-verified customer vs. verified customer using state-ID)

**Device:**
- Device fingerprint, malware infected, Jailbroken/Rooted, device elements spoofed, RAT controlled
- Screen depth/resolution, Fonts, OS, Browser, Browser plug-in, device model & UUID

**Environment:**
- Geographic location, IP address / IP reputation of source, local timezone
- Location spoofing - Proxy/VPN

**Behavior:**
- Analytics of user historical and current resource usage.
- User activity monitoring, specific business activity monitoring (e.g. transactions monitoring)

Risk Mitigation (Authentication) methods to use given certain “who”s and “when”s
Making the case for SSO

- 400+ healthcare respondents on SSO savings:
  - saves clinicians an average of 9.51 minutes a day (122 hours per year)
  - estimated $2,675/clinician/year
  - total annual savings of more than $2.6 million

- 51 apps using SSO on average

- 80% of SSO users would recommend the technology to others

Identity and Access Mgmt
Typical Audit findings – Case for Governance

✗ Poor visibility on why access has been delivered
  • Who requested and who approved it?
  • Is that access still required?

✗ Lack of violation detection
  • Sensitive access assigned to ordinary employees
  • Conflicting permissions creating SoD violations

✗ Manual efforts to retrieve data
  • Time consuming
  • 3rd party consulting fees
Seek a business-driven approach to Identity Governance

Identity and Governance Evolution

1. Administration
   - Cost savings
   - Automation
   - User lifecycle
   - Self-care / Sponsored Care

2. Governance
   - Role management
   - Access certification
   - Business-centric
   - Decision Support
   - Risk-based controls

3. Analytics
   - Intelligence-based control
   - Deep application analysis
   - Application usage
   - Structured and unstructured data

Identity Intelligence: Collect and Analyze Identity Data

- How to gain visibility into user access?
- How to prioritize compliance actions?
- How to make better business decisions?
Identity and Access Mgmt

Identity Integration

Identity Applications

Identity Infrastructure

Federated Identity Mgmt

Identity Mgmt

Audit/Decide

Access Mgmt

Govern

Role Mgmt

Enforce

Admin

Meta-directory

Sync

Directory

Store
IAM Program Recommendations

- **Identify and measure pain points**
- **Describe in terms of business problem**
  - Ex: helps build ROI/compliance business case
- **Develop IAM architecture**
  - Identify authoritative data sources/owners
  - Identify new and legacy components
  - Etc.
- **Develop phased implementation plan**
  - Goal: early success to gain subsequent buy-in
    - don’t try to “boil the ocean”
    - but don’t set long term sights too low
  - try to avoid political / control wars by choosing phase 1 systems judiciously – partner with pilot group
- **Ensure results are measurable**
Thank You