Identity Management: Challenges and Opportunities

Session #213, February 22, 2017

Brian Decker, MBA, CISSP, PMP
Muna Khan, MBA, MPH, CSSBB, CPHIMS
Speaker Introduction

Brian Decker, MBA, CISSP, PMP
Senior Manager, Identity and Access Management
Office of Information Security
Mayo Clinic

Muna Khan, MBA, MPH, CSSBB, CPHIMS
Sr. Principal Health System Engineer
Management Engineering and Internal Consulting
Mayo Clinic
Conflict of Interest

Brian Decker, MBA, CISSP, PMP
Muna Khan, MBA, MPH, CSSBB, CPHIMS

Has no real or apparent conflicts of interest to report.
Agenda

• Learning Objectives
• Key Takeaways
• Definitions
• STEPS
• Problem Statement
• Identity Management Program
• Organizational Change Management/Communications
Learning Objectives

• Explain the importance of identity management as a central tenant of an organization’s security strategy
• Discuss the opportunities and challenges in creating an identity management program
• Describe the process of establishing an identity management program with effective governance
• Demonstrate the challenges encountered for implementing an identity management system
• Identify organizational change management and communications challenges with new identity management operational infrastructure
Realizing the Value of Health IT Through Identity Management

• Satisfaction
  • Providing the right access to the right users at the right time allows users to be functional and effective in their work (as quickly as possible)
  • Providing managers with the appropriate tools to manage access

• Savings
  • The wrong user or a compromised credential getting access to critical data (patient/financial) poses a significant risk to organizations
Key Takeaways

• Identity and access management is central to reducing organizational risk, both internal and external.

• Long-term success comes from identity and access management being a business initiative, not a technology project.

• Understanding identity relationships is an important first step in planning an effective program

• Governance must align with business initiatives and identified risks.

• Work hard to know how the organization works to create a long-term sustainable program (think: lifestyle change)
Identity Management System

• An Identity Management System is any system that creates, issues, uses, and terminates electronic identities. In other words, an Identity Management System provides lifecycle management for the digital credential sets that represent electronic identities.

- NIST
Identity and Access Management

• An identity and access management (IAM) system is a framework for business processes that facilitates the management of electronic identities.

  - TechTarget
  • http://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system

• Definition simplified:

  Ensuring the right “subjects” have the right access to the right “objects” at the right time and nothing else.
Healthcare is being targeted
Today’s Hostile Environment

• Threat actors have multiple levels of skills
  • Insiders (Current & Ex)
  • Script Kiddies
  • Hacktivists
  • Organized Crime
  • Nation State

• Active adversary must be assumed
  • Unlimited time and resources

• Skill level to cause harm is going down

• Tools to compromise and harm systems are readily available and cheap (free)

• **Harm or disruption could be deliberate or collateral**

• We are way past relying upon firewalls
Attack Motivations

• Revenge
• Personal Gains
• Bragging Rights / Status
• Expression of Political or Social Views
• Intellectual Property Theft
• $$$$$$ (ransomware, theft, etc.)
• Identity Theft – Financial / Medical

- Health records sell for $50
- Can be used for billing fraud by fake clinics
- Used for prescription fraud to get and then sell narcotics
Threats to Identity and Access

- Nation State
- Organized Crime
- Hacktivists
- Individuals
- Insiders
- Snoopers

- Phishing (to get credentials)
- Lateral movement (using credentials to move around and find data)
- Malware (use credentials to get foothold)
- Ransomware (use credentials to access and then encrypt data)
- Viewing sensitive data (use access inappropriately)
- Drug diversion (inappropriate access)
- Etc.

IAM
Simplified Problem Statements

• Who *actually* are our users?
• Are they *appropriate* users?
• Who has *access* to what and *why*?
• Who is *accountable* for user’s access?
Imagine these scenarios...
Real World Scenarios

• Identities have different relationships to Mayo Clinic depending upon their immediate needs. The different relationships require appropriate and specific levels of security.

• Example 1:
  1. Physician – outpatient clinic in the AM & PM
  2. Physician – surgery late AM
  3. Physician – administrative leader at noon
  4. Physician – researcher late afternoon
  5. Physician – professor in the evening

• Example 2:
  1. RN – Hospital nursing primary job function (with floating)
  2. RN – Nurse Anesthetist in School of Health Sciences
Identity & Access as a Central Tenet of Information Security

• Business enabler – the right access to the right information
• Can’t manage what you don’t know or can’t see – what identities actually have access to
• Enables visibility and transparency
• Drives accountability
• Requires organizational behavior change
Identity Management Program

Mayo Clinic began creating our Identity Management Platform to support all population types across all sectors (B2E, B2B, B2C)

Primary objectives:
1. Security
2. Experience
3. Scalability and Sustainability

Core elements:
1. Identity and Account Management
2. Authorization and Access Management
3. Authentication Centralized
4. Accountability - Access Certification / Validation
Common Challenges

- Identity and Population Management
  - Knowledge and appropriate management of user populations
  - Appropriate Roles

- Accountability / Audit
  - Holding Managers, role owners, data owners accountable for access and access decisions

- Account and Credential Management
  - Privileged accounts (IT and other users)
  - Appropriate authentication

- Access Management Appropriateness
  - Authorization
  - Identity Lifecycle (joiner, movers and leavers)

- Lack of access visibility into platforms and applications
Identity Relationships
Identity and Population Management

Diverse Challenges:
- Populations
- What people do
- Where people do it
- Multiple personas
- Multiple types of accounts
- Multiple managers
- Thousands of applications
Non-Employee Populations

***100+ non-employee populations

Identity Hub

- Non-Employees – All Sites
- IT Contractors
- Vendors
- Contract Physicians
- Convent Residents
- Site Specific Nursing Homes
- Site Specific Nursing Students
- Some Interns
- Visiting Scientists & Appointments
- Health Club

- Volunteers
- Visiting Clergy
- External Access to Medical Record
- Public Committee Member
- Emeritus Staff

---

HIMSS17
Growth of Subspecialties at Mayo Clinic

- **1900**: Drs. Will & Charlie
- **1925**: Clinical
- **2010**: Cardiovascular Radiology
- **Internatinal Medicine Divisions**
  - Cardiovascular Health
  - Chest Pain & Coronary Physiology
  - Congenital Heart Clinic
  - Pericardial Disease Clinic
  - Thrombophilia Center
  - Pulmonary Hypertension
  - Heart Rhythm Center
  - Cardiomyopathy
  - Electrophysiology
  - Pediatric Cardiology
  - Heart Failure
  - Counterpulsation
  - Transplant
  - Marfan Clinic
  - Valvular Heart Clinic
  - Vascular Medicine
  - Women’s Heart Clinic
  - Nuclear Cardiology
  - Cardiovascular Radiology
  - Ulcer & Wound Care Clinic
  - Cardiovascular Epidemiology
  - Coronary Physiology & Imaging
  - Cardiovascular Surgery

- **Cardiovascular Subspecialties**
  - + 13 Specialty Labs
Traditionally, IAM systems naturally model identities and roles, but not persona, a 2-tier model.

How do we map 3-tiers to 2-tiers?

Additionally, how do we bound approvals, certifications and reporting to the appropriate tier?
Role Based Access Control Model

IAM tool manages business and functional roles

IAM tool is aware of application roles (as entitlements) via business logic and performs user assignment through provisioning
Gaining Electronic Access

3-Tier Access Control Model

1. Birthright Roles & Attributes

2. Business Roles

3. On-Demand “Shopping Cart”
The Role of Identity and Access Governance

- Understand and prioritize IAM related risks and business drivers
- Own identity-related policies
- Ensure risks and drivers are staged and addressed
- Drive the platform and IAM security services into the business and technical environment
- Stakeholder management and communication
How do we make change happen?

- Organizational Change Management
  - Stakeholder Analysis
  - ADKAR
- Communications, Communications, Communications
- Sr. Leadership support, engagement and visibility
Organizational Change Management

• Establishing new norms
  – Creating a culture of accountability and audit
    • Functional role owners
  – Behavioral changes
    • Supervisors/managers
    • Users
    • Applications teams (IT/Security Administrators)
New Roles & Responsibilities

• Information Technology & Information Security
  – Provide the necessary tools and policies to maximize security within the organization
  – Compliance with new application access protocols
  – Participating in roles and application access rights definition

• Business Leaders
  – Take full ownership in definition and refining functional roles within organization
  – Hold managers/supervisors accountable for access provisions

• Institutional Leaders
  – Support an environment for IAM to take hold as a central tenet of security
Realizing the Value of Health IT Through Identity Management

• Satisfaction
  • Providing the right access to the right users at the right time allows users to be functional and effective in their work (as quickly as possible)
  • Providing managers with the appropriate tools to manage access

• Savings
  • The wrong user getting access to critical data (patient/financial) poses a significant risk to organizations
Questions

Thank you!
(Please complete online evaluations)

Decker.brian@mayo.edu

Khan.Munawwar@mayo.edu