Building an Information Security Organization

Jason Taule, Chief Security and Privacy Officer, FEi Systems
Joy Poletti, Director IT Security Compliance, Catholic Health Initiatives
Michael Pinch, Chief Information Security Officer, University of Rochester Medical Center
Dave Summitt, Chief Information Security Officer, University of Alabama at Birmingham Health System
BUILDING A SECURITY PROGRAM
The Basics
Joy Poletti
April 2014
About Catholic Health Initiatives

- **Nonprofit, Faith-Based Health System Formed in 1996**
- **Nation's Third Largest Catholic Health System**
- **91,000 Employees**
- **2013 Operating Revenues - $10.7 Billion**
- **2013 Charity Care/Community Benefit - $762 Million**

Includes 30 market-based organizations operating in 17 states and comprising of 87 acute care hospitals, including four academic medical centers, four teaching hospital affiliations, and 23 critical access facilities.

Services span the inpatient and outpatient continuum of care – hospitals, long term care facilities, community health services organizations, accredited nursing colleges, home health agencies, and physician provider clinics.
Building an Effective Security Program
Simple, Economical Approaches

**Size and Funding Neutral Approaches**

- **Senior Leadership Awareness**
  - Various Ways
  - Appropriate Level of Involvement

- **Integrate Security with Business Requirements**

- **Formalize a Security Strategy**
Establish a Cross-Functional Senior Level Security Steering Committee

Bring Risk-Relevant Information into Decision Making Process

Key Responsibilities May Include:

- **Authority** to approve, or to recommend Security decisions
- **Accountability** for ensuring security strategic plans and roadmaps are in alignment with organizational strategic objectives
- **Provide** oversight, guidance, direction and support to all security functions
- ** Ensure** ongoing support for security within the organization
- **Liaison** with larger risk management committees, if applicable.

Ensure Risk Decisions are Made and Owned by Senior Leadership
Establish a Strong Foundation

Provides the Ability to Act Rather than React

- Policies, Standards and Processes – Create, Communicate, and Enforce
- Define your Risk Management Approach
- Perform and Act on Risk Assessments
- Employee Security Education and Awareness
Security Posture

Can Vary in Formality

Baseline your Current Security Level

Collaborate with Other Departments for Support

Build your Security Plan

Risk Reduction Benefit to Organization

Maturity Level
Risk Assessment Process

1. Establish a Process that Makes Sense for your Organization
2. Identify, Estimate, and Prioritize Risks
3. Create a Risk Register
   - Keep It Simple
   - Track and Measure Risks
   - Establish an Exception Process
4. Continuous Management and Updates
   - Threats and Vulnerabilities
**People, Process & Technology**

- **People**: Brightest well-trained people may not deliver.
- **Process**: Develop processes regardless of technology capabilities.
- **Technology**: Technology cannot address all potential process failures alone.

**We often say it in this order for good reason**
Recap

Management Involvement in Risk Decisions
Determine Security Posture
Formalize a Security Plan
Develop a Security Risk Assessment Process
Assess Mix of People, Process & Technology
Building an Information Security Program

Dave Summitt, CISO

UAB HEALTH SYSTEM
Knowledge that will change your world
UABHS Security Organization

- Senior InfoSec Architect
- Senior InfoSec Engineer
- 2 InfoSec Engineers
- Project Manager
- Computer Technician

- In addition, we use approximately 50 individuals known as Entity Security Coordinators.
Responsibilities

- Writing/Reviewing/Revising all InfoSec Plans & Policies
- Owns BCP/Disaster Recovery plan
- Owns Configuration Change program
- Owns Risk Assessment & Analysis process and provides mitigation recommendations
- Incident Response & Reporting
- Vulnerability scans, Pen tests, and system audits
- Investigations & Forensics
- SEIM, network, systems & firewall log monitoring
- Review BAAs and new systems/application security
- Media Destruction
- Security Awareness & HIPAA training
Security Team Philosophy

- Try to be enablers – not disablers
- Offer alternative solutions if something doesn’t work with our way of business
- Stay informed of the business strategy
- Improve customer relations by keeping them informed throughout a problem/solution
- Work with high ethics and accountability – we don’t work outside our policies & rules
- Don’t suffer from burn-out
- Encourage “out-of-the-box” thinking
Recommendations

- Continuing education
- Benchmark yourself and your team
  - What are you doing well?
  - Where are your weak spots?
- Encourage creativity – don’t micro-manage
- Leave your ego at home, and when you go home, leave your work.
- CISO, Director, or Manager should be regularly attending meetings throughout the organization
Questions?