Building a Security Program on a Limited Budget
HIMSS Cybersecurity Community Sponsor
Faith Regional Health Services
CIO/CISO

- Brian Sterud, MBA, CHCIO, FACHE
MISSION
The MISSION of Faith Regional Health Services is to serve Christ by providing all people with exemplary medical services in an environment of love and care.

VISION
The VISION of Faith Regional Health Services is to be recognized as a regional referral center by providing comprehensive, high-quality services to the residents of Northeast Nebraska.
Keys to Success

• Executive Governance (aka buy-in)
  • Board of Directors
  • Organizational Leadership
  • Explain the why
• Education and awareness
• Continuous monitoring and improvement
Healthcare is Complex

**Laboratories, Blood & Pharmaceuticals**
- Pharmaceutical Manufacturers
- Drug Store Chains
- Pharmacists’ Associations
- Public and Private Laboratory Associations
- Blood Banks

**Medical Materials**
- Medical Equipment & Supply
- Manufacturing & Distribution
- Medical Device Manufacturers

**Health Information Technology**
- Medical Research Institutions
- Information Standards Bodies
- Electronic Medical Record Systems Vendors

**Federal Response & Program Offices**
- Coordinated Response Activities Under
- Emergency Support Function 8
- Government Coordinating Council
- Federal Partners (e.g., HHS, DoD, other sector partners)

**Direct Patient Care**
- Healthcare Systems
- Professional Associations
- Medical Facilities
- Emergency Medical Services

**Mass Fatality Management Services**
- Cemetery, Cremation, Morgue, and Funeral Homes
- Mass Fatality Support Services (e.g., coroners, medical examiners, forensic examiners, & psychological support personnel)

**Health Plans and Payers**
- Health Insurance Companies & Plans
- Local and State Health Departments
- State Emergency Health Organizations

**Public Health**
- Governmental Public Health Services
- Public Health Networks
Security: Where to Begin?
Building the Right Team
Security Governance

• Generally speaking, the obvious choice may not be the only option
• Organizing correctly may help limit future liability and exposure
• Building a governance structure with both accountability and authority over the enterprise takes careful planning and solid policies
Governance Structure

- Security Committee
  - Human Resources
  - Health Information Management
  - Biomedical Engineering
  - Facilities Management
  - Compliance
  - Information Technology
What Boards and Executives Should Know?

• Understand:
  • Cyber security is an enterprise wide management issue, not an IT issue
  • Legal and financial implications of a security breach
  • Impact to reputation if security is compromised

• Boards should:
  • Be included in cyber risk discussions
  • Ensure adequate resources are spent on security
Monitor Gateways into Organization

• Establish vetting process for the following:
  • All Capital projects
  • Operational projects
  • Network Connected Devices
Enterprise Risk Management

• Traditionally, risk has been addressed in a siloed, segmented fashion

• Information security incidents can impact the organization beyond the IT department
  • Decreased revenue due to canceled elective services
  • Increase risk of medical errors due to use of paper
  • Increased stress on staff
A New Balance Between Compliance and Security

Healthcare has undergone a paradigm shift

Traditionally, HIPAA-driven priorities: confidentiality, integrity, availability

Over the past 2-3 years, availability has become a growing concern

Ransomware impacted information access and therefore clinical workflows
WannaCry shut down hospitals (UK, NHS)
Medical device incidents have impacted care delivery

And we are starting to understand the integrity problem

Again, medical devices (hacks that could kill – research only so far)
Risk to critical systems and data ... and patient trust
Changing Risk Priorities

From “Business Critical” to “Mission Critical” to “Life Critical”

Confidentiality
- PHI (HIPAA)
- But also PII & PCI
- Account Information
- Billing & Payment Data
- Intellectual Property
  - Clinical Trials
  - Research
  - Design & Formularies
- Legal & HR Documents
- Identities & Credentials

Availability
- Clinical Systems
  - EHR & Specialty
  - Ancillary (PACS, Lab, Pharma)
  - ePrescription / EPCS
- Medical Devices
  - Availability of clinical services and results
- Business Systems
  - Email
  - Billing, Scheduling

Integrity
- Critical Patient Data
- Prescriptions, Medications
- Dosages
- Allergies
- History
- Diagnosis
- Alarms
- Critical Technical Data
  - Calibration
  - Safety Limits

Patient Experience: “Patient Trust Zone”

Patient Harm Risk: “Patient Safety Zone”
# Changing Risk Priorities

Regulatory Controls Need to Be Balanced with Nimble Security

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Availability</th>
<th>Integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Past</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lost or stolen devices</td>
<td>Technical failure</td>
<td>Accidental alteration of data</td>
</tr>
<tr>
<td><strong>Now</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financially motivated</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Criminal intent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Political attacks (nations, hacktivists)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Care delivery</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ransomware</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Medical devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Targeted attacks, intent to harm</td>
<td>Create doubt in data (and healthcare system)</td>
</tr>
</tbody>
</table>
Evolution

Crawl  Walk  Run
Crawl

• Governance
  • Policy and Procedure development
  • BYOD Policy and MDM
  • Select a CyberSecurity framework to serve as guideposts for program
  • Disaster Recovery Plan and Business Continuity Plan
  • Asset Inventory including Recovery Point Objectives and Recovery Time Objectives

• Technical
  • Redundant Internet connections
  • Encryption of mobile assets
  • Role based security
  • Patch Management
Crawl

• Governance
  • Policy and Procedure development
  • BYOD Policy and MDM
  • Select a CyberSecurity framework to serve as guideposts for program
  • Disaster Recovery Plan and Business Continuity Plan
  • Asset Inventory including Recovery Point Objectives and Recovery Time Objectives

• Technical
  • Redundant Internet connections
  • Encryption of mobile assets
  • Role based security
  • Patch Management
Walk

- Governance
  - Established security metrics
  - CISO role solidified
  - Onboarding/offboarding
  - Security Awareness program established for all staff
  - Standardization of Security roles and assignments
  - Processes for Data Destruction and Decommissioning
  - Development of Incident Response Plan

- Technical
  - Encryption of ALL assets within the organization
  - Email encryption, with HIPAA algorithm enabled
  - Multi-Factor authentication
  - Hardening of workstation and server builds
  - H-ISAC
  - Penetration Testing
Walk

• Governance
  • Established security metrics
  • **CISO role solidified**
  • Onboarding/offboarding
  • **Security Awareness program established for all staff**
  • Standardization of Security roles and assignments
  • Processes for Data Destruction and Decommissioning
  • **Development of Incident Response Plan**

• Technical
  • **Encryption of ALL assets within the organization**
  • Email encryption, with HIPAA algorithm enabled
  • Multi-Factor authentication
  • Hardening of workstation and server builds
  • H-ISAC
  • **Penetration Testing**
Run

• Governance
  • Security Metrics shared with organization, including Board of Directors
  • Internal Phishing Campaigns with robust policy on demonstrating improvements
  • Targeted Security Awareness training
  • Tabletop Exercises (Cyber and Disaster)
  • Documented change of custody
  • Formalized Change Control process

• Technical
  • Data Loss Prevention
  • Advanced Threat Protection
  • SIEMaaS
  • Vulnerability Scanning
  • IoT Profiling
  • Microsegmentation
  • Application whitelisting/blacklisting
Run

• Governance
  • Security Metrics shared with organization, including Board of Directors
  • Internal Phishing Campaigns with robust policy on demonstrating improvements
  • Targeted Security Awareness training
  • Tabletop Exercises (Cyber and Disaster)
  • Documented change of custody
  • Formalized Change Control process

• Technical
  • Data Loss Prevention
  • Advanced Threat Protection
  • SIEMaaS
  • Vulnerability Scanning
  • IoT Profiling
  • Micro segmentation
  • Application whitelisting/blacklisting
Building without $$$$$

• Incident Response Plan
• Periodic review of Firewall configuration
• Cross functional Security Committee
• Tabletop exercises
• ePHI Inventory
• Removal of generic accounts
• Periodic reviews of Physical access via badge system
• BAA process redesign with security requirements of third parties
• Processes for onboarding/offboarding

• Policy and Procedure development
• USB Restrictions
• Change Management processes
• Separate Admin accounts from personal accounts
• Processes for documenting security exceptions
  • Generic logons, remote access, USB Access
Building without $$

- Incident Response Plan
- Periodic review of Firewall configuration
- Cross functional Security Committee
- Tabletop exercises
- ePHI Inventory
- Removal of generic accounts
- Periodic reviews of Physical access via badge system
- BAA process redesign with security requirements of third parties
- Processes for onboarding/offboarding

- Policy and Procedure development
- USB Restrictions
- Change Management processes
- Separate Admin accounts from personal accounts
- Processes for documenting security exceptions
  - Generic logons, remote access, USB Access
Workforce Shortages

• Internships
• Advisory Committees
  • 2 year and 4 year schools
CULTURE!!!

• Organization-wide
  • Establish a culture of security and awareness.
  • Focus on critical thinking, rather than specific Q and A
    • Staff need to understand concepts and adapt to situations

• Security team
  • Quick response
  • Teamwork across IT staff as well as non-IT departments
  • Focus on the situation, not the blame game
Questions?