Organizational Resilience: The True Measure of Readiness
Sharing Our Perspective

- Vulnerability/Risk Assessment
- Program Development
- Program and Organizational Audit
- Resilience and Continuity
- 100% Healthcare Focus
Introductions

Keith Kenna

- *Vice President, Program Management*
- 10+ years’ Healthcare industry experience
- Member of HITRUST Assessor Council
- Experienced pre-hospital healthcare provider
- PMP, HCISPP, HITRUST Certified CSF Practitioner
Introductions

Mark Ferrari

- Executive Vice President
- 20+ years’ Healthcare industry experience
- Former U.S. Air Force Officer
- Member of HITRUST Assessor Council
- Experienced pre-hospital healthcare provider
- PMP, CISSP, HCISPP, HITRUST Certified CSF Practitioner
Current State

• Attacks continue to become more insidious
• Information Security in Healthcare is a “key public health concern”
• Patient safety demands the availability and integrity of data
• Need for Resilience...
Health Care Industry Cybersecurity (HCIC) Task Force

• Established March 2016 by Congress as a result of the Cybersecurity Act of 2015

• Goal – explore challenges healthcare industry faces relating to security/privacy

• Report on Improving Cybersecurity in the Healthcare Industry - June 2017
  – Based on current threats, vulnerabilities in implemented technologies, nature of patient care
  – Information security – **public health concern** – needs **immediate** and **aggressive** attention
Health Care Industry Cybersecurity (HCIC) Task Force

• Confidentiality, Integrity, and Availability of patient data is **VITAL** in the clinical environment
  – Quality care delivery relies on present and accurate information
  – Disruptions to data → disruptions in the clinical workflow
  – Disruptions in the clinical workflow → directly impact patient safety
Cyber Resilience

• “Healthcare must move from risk to resilience.”
  - Tom Ridge, Healthcare Security Forum, September 2017

• The increased emphasis on this concept marks an evolutionary point for Health Information Security

• What is Resilience?
Risk vs Resilience

• Progression of Attacks
  – Nuisance → Theft → Disruption

• Risk Management
  – Active identification and mitigation of risks
  – Implement safeguards to achieve Defense in Depth

• Organizational Resilience
  – Capability of the enterprise
  – A state not an action
  – Result of exercising
Organizational Resilience Fitness

• Fitness/Resilience
  – Build not buy
  – Achieved through regular exercising
  – “Train like you fight, fight like you train”
  – Cultural AND Procedural
The Importance of Resilience

• Attacks are becoming more insidious
• Modification of ransomware
• Goal of destruction versus profit or disruption
• Depth of disruption within organizations increasing
• Requires deeper probing, deeper degrees of preparedness – beyond the walls of IT or Information Security
What Happens in Healthcare?

• When...
  – Preventable risk identified that affects the patient population

• Then...
  – An organization wide program is developed to actively mitigate that risk
Campaign Approach

• “Fall Campaign”
  – EHR assessments to identify fall risk
  – Patient education
  – Socks with grip
  – Bed alarms
  – “Fall board” in each room identifying fall risk
  – Shift change huddles discuss at risk patients

• Falls
  – Impacts Care
  – Organizational Issue
  – Preventable Issue

• Information Security
  – Impacts Care
  – Organizational Issue
  – Preventable Issue
What Happens in IT?

• When...
  – Preventable risk identified that affects the patient population

• Can we say...
  – An organization wide program is developed to actively mitigate that risk?!?
“Awareness” is Failing

3 Levels of Proficiency:

1. Awareness
2. Operator
3. Technician

Train to Operator Level
Daily Safety Briefings

• The **purpose** is to:
  – promote a culture of safety
  – provide means of transparency/communication (Horizontal and Vertical)

• Why?
  – maintain quality patient care

• How?
  – Hospital leaders meet daily to quickly review identified and realized risks
  – Facility focused
  – Quality/Issue Reports
  – Escalated Ad Hoc Department/Employee Findings
### Daily Safety Briefings - Topics

#### Realized Issues
- Quality/Incident Reports (e.g., Midas, Veritas, etc.)
- Falls
- Equipment Issues
- Delays in Care
- Employee Injuries
- Rapid Responses

#### Identified Risks
- Construction Projects
- Planned Downtimes
- Facility Shutdowns

#### Daily Census
- Bed Capacity
- Surgery Metrics
- ED Throughput

#### Accountability
- Stand Up Style Report
- Open Issues
Plan Integration and Testing

- Business Impact Analysis
  - *Meaningful Analysis → Probe for SPOF*
- Business Continuity Plan
- Backup/Disaster Recovery Plan
- Incident Response Plan
- Emergency Management Plan
  - *Utilize and involve this discipline*
  - EOC Activation
- Cross-Discipline Tabletop Exercises
  - Information Security events graduating into full EOC activation
All Hazards Approach

• FEMA

  ▪ Integrated approach to emergency preparedness planning
  ▪ All-hazards planning does not specifically address every possible threat but ensures those hospitals and all other providers and suppliers will have the capacity to address a broad range of related emergencies
  ▪ Drives BIA, Risk Analysis, Emergency Planning
Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Content Spotlight