CHALLENGES & OPPORTUNITIES IN MANAGING CYBER RISKS

MAY 03, 2018

Ram Ramadoss, MBA, CISA, CISM, CISSP, CRISC, CIPP
Vice President – CRP Privacy and Information Security and EHR Oversight
Corporate Responsibility Program
Catholic Health Initiatives
Colorado, USA

AGENDA

- CHI Overview
- Small and Medium Sized Providers – an easy target
  - Challenges
  - Opportunities
- Board Members Engagement
- Highlights – Key recommendations from the Taskforce
- Q&A

CATHOLIC HEALTH INITIATIVES OVERVIEW

- An integrated Healthcare provider in the USA
- We operate in 17 states through 100 hospitals and 700 plus clinics, including three academic health centers and major teaching hospitals as well as 30 critical-access facilities, community health-service organizations, and nursing colleges.
- Operating revenue - $15.5 Billion
- 90,000 plus employees
- Merger discussion in progress with Dignity Health (a major faith-based healthcare provider in California, Nevada and Arizona)

Small and Medium Sized Healthcare Providers – an easy target for cyber threats

CHALLENGES

- Ignorance is bliss
- Dwindling operating margins - low or no security budget
- Lack of IT resources and support
- No policies/training and lack of cyber hygiene practices
- Lack of awareness and education – employees/physicians
- Risk assessment – even large companies struggle in this area
- No sense of urgency from this sector
- Ransomware attacks | No incident management program
- Majority of providers moving towards cloud based Electronic Health Record (EHR) solutions

CHALLENGES

- A major challenge for large healthcare systems – access to EMRs from third party physician practices
- Challenges with EHR vendors – configuration best practices
- No leverage when these entities deal with third party companies and partners
- No ability and resources to process security alerts from Information Sharing and Analysis Centers (ISACs)
- No cost effective Managed Security Service Providers (MSSPs) to support this sector

CHALLENGES

- Legacy applications and legacy medical devices
- Business Resilience (non-existent) – major confusion regarding the ownership even for large providers
- Lack of knowledge of organization's storage of data location for cloud based solutions
- Lack of accountability in addressing remediation
- No robust logging capabilities
- Monitoring of activities is minimal | a significant challenge when faced with security incidents

CHALLENGES

- No network segmentation
- No threat and vulnerability management program
- A small percentage of organizations with cyber insurance coverage

A coordinated attack on multiple small entities could pose a significant risk to national security

OPPORTUNITIES- SOLUTION PROVIDERS

- Cybersecurity solutions - patient treatment & ease of use
- Build more efficient and meaningful platforms (AI and Machine Learning)

  risk assessment | prioritization of risks

  options to manage risks
- Build cyber care platforms to manage

  asset management | policies & standards

  training | phishing campaigns

  incident management capabilities
- Build cost-effective ongoing monitoring solutions

OPPORTUNITIES- SOLUTION PROVIDERS

- Develop more intuitive security awareness training
- Encourage low-cost MSSPs to support these segments
  - who can enable automation, efficiency and effectiveness
- Witnessing a major shift in Third Party Risk Assessments and Monitoring
- Develop robust development and support strategies
  - EHR vendors and medical device manufacturers

OPPORTUNITIES – HEALTHCARE PROVIDERS

- Address baseline security controls for critical systems
- Apply 80-20 rule; maintenance is relatively easier
- Conduct independent risk assessments to identify key risks
- Focus on business resilience efforts
- Implement of advanced endpoint protection solutions
- Adopt a conservative approach – firewalls; web filtering; USB monitoring; basic Data Leakage Prevention (DLP)
- Security patching and cyber hygiene practices
- Reduce less defensible legacy systems and technologies

BOARD MEMBERS ENGAGEMENT

- Recent incidents have created solid awareness among board members and senior leadership teams
- Hire board members who are security savvy and champions of privacy
- Quarterly update to the board members
  - State of security – risks and emerging threats
  - Integration of security reviews – due diligence and new products/business lines
  - Identify areas where support is required
- Engagement is the key

Highlights – Key recommendations from the Health and Human Services National Cybersecurity Taskforce

RECOMMENDATIONS FOR SMALL AND MEDIUM SIZED PROVIDERS

- Tax incentives, grants to encourage low-cost MSSPs
- Crediting providers who have engaged MSSPs
- Explore opportunities for individuals to engage in ongoing internship programs
- Evaluate incentive options to encourage health care providers migrate to more secure environments

OTHER KEY RECOMMENDATIONS

- Establish a consistent, consensus based health care specific Cybersecurity Framework
- Explore potential impacts to the Physician Self-Referral Law, the Anti-Kickback Statute, and other fraud and abuse laws to allow large health care organizations to share cybersecurity resources and information with their partners.
- Improve manufacturing and development transparency among developers and users.
- Establish a model for adequately resourcing the cybersecurity workforce with qualified individuals.

OTHER KEY RECOMMENDATIONS

- Establish a cybersecurity hygiene posture within the health care industry to ensure existing and new products/systems risks are managed in a secure and sustainable fashion.
- Provide patients with information on how to manage their health care data, including a cybersecurity and privacy grading system for consumers to make educated decisions when selecting services or products around non-regulated health care services and products.
- Improve information sharing of industry threats, risks, and mitigations.

Q & A

RamRamadoss@catholichealth.net