HIMSS18 The leading health information and technology conference

WHERE THE WORLD CONNECTS FOR HEALTH

Conference & Exhibition | March 5–9, 2018

Las Vegas | Venetian – Palazzo – Sands Expo Center

How to Best Manage Cybersecurity Risks

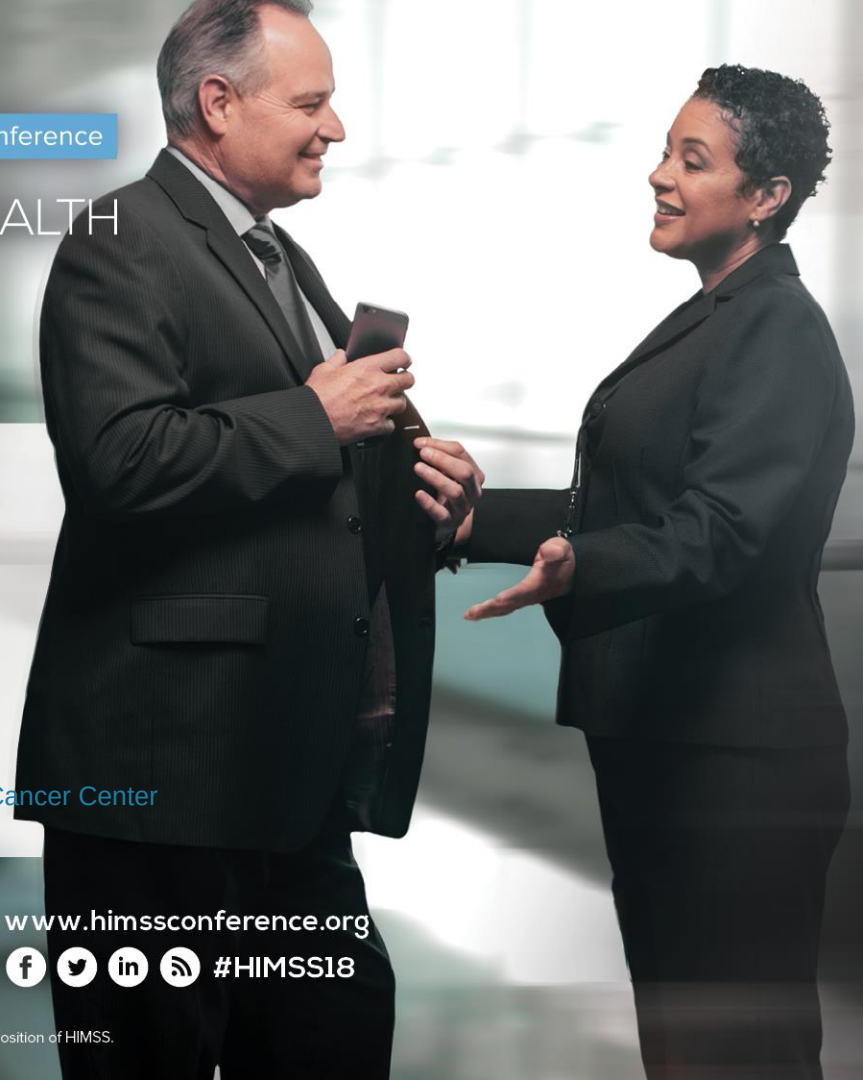
Session 5, March 5, 2018

Abhishek Agarwal, VP & CISO, Fresenius Medical North America

Kristen Ahearn, Associate GC, Director & Privacy Officer, Memorial Sloan Kettering Cancer Center

Peter McLaughlin, Partner, Burns & Levinson LLP

COMMITMENT



www.himssconference.org

#HIMSS18

Learning Objectives

- Identify the steps to take for security compliance and effectively training your workforce
- Describe what is involved in a risk assessment and the importance of penetration testing
- State how to expeditiously address identified risks
- Discuss how to prepare for government audits and maintain good documentation of compliance efforts
- Recognize the importance of reputational risk

Agenda

- Overview of Cybersecurity risks in Healthcare
- Standard Practices in Cybersecurity
- Overview of Cybersecurity Controls
- Identifying and Responding to Issues
- Demonstrating Good Compliance
- Reputational Risk

Cybersecurity Risks in Healthcare

- While healthcare industry integrates advance technologies to continue providing improved services and outcomes, the rising threat of Cybersecurity impedes the pace of technology adoption.
- Healthcare providers realize the socio-economic benefits of connecting to health information exchanges, adopting to electronic health record (EHR), using mobile solutions (telemedicine), and executing Connected Health strategies. However the risks of online threat continues to emerge.
- Both HIPAA physical safeguards and HIPAA technical safeguards have an important impact on a healthcare provider's technology infrastructure.

Standard Practices in Cybersecurity

- A healthcare company must consider baseline cybersecurity controls embedded within it's IT infrastructure.
- Adopting a standard framework such as NIST Cybersecurity Framework (CSF) brings effective and efficient practices.
- Identity and access controls, including multifactor authentication, secure transmission protocols, data protection and monitoring solutions are essential components of day to day security operations.
- Conducting regular security risk assessments, which are also required under HIPAA rules, helps maintain HIPAA compliance with physical, technical, and administrative safeguards.

NIST Cybersecurity Framework(CSF)

- Facilitate organization-wide identification of common controls and the development of organization-wide tailored security and privacy control baselines, to reduce the workload on individual system owners and the cost of system development and protection.
- Reduce the complexity of the IT infrastructure by consolidating, standardizing, and optimizing systems, applications, and services through the application of enterprise architecture concepts and models.
- Identify, prioritize, and focus resources on high-value assets and high-impact systems that require increased levels of protection—taking steps commensurate with risk such as moving lower-impact systems to cloud or shared services, systems, and applications.

Standard Cybersecurity Controls

First 5 CIS Controls
Eliminate the vast majority of your organization's vulnerabilities

1: **Inventory of Authorized and Unauthorized Devices**
2: **Inventory of Authorized and Unauthorized Software**
3: **Secure Configurations for Hardware and Software**
4: **Continuous Vulnerability Assessment and Remediation**
5: **Controlled Use of Administrative Privileges**

All 20 CIS Controls
Secure your entire organization against today's most pervasive threats

6: **Maintenance, Monitoring, and Analysis of Audit Logs**
7: **Email and Web Browser Protections**
8: **Malware Defenses**
9: **Limitation and Control of Network Ports**
10: **Data Recovery Capability**
11: **Secure Configurations for Network Devices**
12: **Boundary Defense**
13: **Data Protection**
14: **Controlled Access Based on the Need to Know**
15: **Wireless Access Control**
16: **Account Monitoring and Control**
17: **Security Skills Assessment and Appropriate Training to Fill Gaps**
18: **Application Software Security**
19: **Incident Response and Management**
20: **Penetration Tests and Red Team Exercises**

Source: https://www.cisecurity.org/controls/

Risk Management

- Identify, Protect, Detect, Respond, Recover (NIST CSF)
- Identifying Risks
  - Data and system inventory
  - Data flows
  - Wants vs Needs
  - What if… Sharknado
- Internal vs External resources

Risk Management (2)

- Mitigating Identified Risks
  - Prioritization of risks
  - Resource planning
  - Accountability
  - Insurance
- Effective & Legally Defensible

Organizational Approach

- Chief Information Security Officer leads efforts
- Close collaboration with Information Systems, Internal Audit and Compliance to ensure cyber risk has appropriate oversight
    - Risk assessment factors
    - Work plan coordination
- Legal Counsel
    - Preparing for an incident, governance, actual incident
    - Named on panel for institution's cyber insurance
- Coordination with Communications team
- Quarterly Reports to the Board

Staff Awareness

Policy as Foundation
- ✓Authorized Individuals
- ✓Access Controls
- ✓Password Security
- ✓Minimum Necessary

Periodic Communications
- ✓Information Security Weekly Blog
- ✓Annual Compliance Week
- ✓"Protect. Enable."

Training
- ✓New Employee Orientation
- ✓Mandatory Online Training
- ✓Adhoc In Person Presentations

Incident Response
- ✓Identify potential for cyber risk
- ✓Re-educate staff with actual example

Assessment, Monitoring and Detection

- Information Security Initial Assessment
  - Legacy Vendors
  - Tiered approach dependent on data sensitivity
- Phishing Tests
- Use of Data Loss Prevention
- Access to Medical Records
- Review and approval of Access/Data Requests for institutional resources

Questions???

Friendly Reminder:
Please complete online session evaluation.