Achieving Cyber-Readiness through Information Sharing Analysis Organizations (ISAOs)

Florida Hospital Association
Friday, March 23, 2018

Welcome!

John Wilgis
Director, Emergency Management Services
Florida Hospital Association
Objectives

- Understand what an Information Sharing and Analysis Organization (ISAO) is as defined by Presidential Executive Order 13691.
- Learn why all health organizations should participate in an ISAO.
- Learn how to practice better "cyber-hygiene" by participating in an ISAO.
Objectives

• Understand what an Information Sharing and Analysis Organization (ISAO) is as defined by Presidential Executive Order 13691.
• Learn why all health organizations should participate in an ISAO.
• Learn how to practice better "cyber-hygiene" by participating in an ISAO.

What’s the Issue?

CYBERSECURITY
The Risk

- Cybersecurity vulnerabilities and intrusions pose risks for every hospital.
  - Expanded use of networked technology
  - Internet-enabled medical devices
  - Electronic databases for clinical, financial and administrative operations

*Increased exposure to possible cybersecurity threats!*

Managing the Risk

- Evaluate and manage risks
  - Federal privacy rules and related polices.
  - Part of the hospital’s governance, risk management and business continuity framework.
- Approach must be flexible and resilient to address threats that are likely to be constantly evolving and multi-pronged.
Achieving Cyber-Readiness through Information Sharing Analysis Organizations (ISAOs)

Friday, March 23, 2018

Lots of Resources…

- FBI
- DHS
- AHA
- HIMMS
- Vendors
- Consultants
- ISAO…

Today’s Speakers

Kendra Siler, PhD
Executive Director, Population Health ISAO and Secure Together Program Contact

Sanjay Patel
CEO
Smart Hive
The Population Health ISAO is a cyber intelligence community for healthcare providers working together to meet regulatory requirements, reduce cyber risk, and identify cyber threats in the healthcare environment.

Introduction to the Population Health ISAO
2018

WHAT IS THE 405(d) EFFORT?
An industry-led process to develop consensus-based guidelines, best practices, & methodologies to strengthen the HPH-sector’s cybersecurity posture

WHO IS PARTICIPATING?
The 405(d) Task Group is convened by HHS and comprised of information security officers, medical professionals, privacy experts, and association leaders

HOW WILL 405(d) ADDRESS HPH CYBERSECURITY NEEDS?
With a targeted set of applicable & voluntary guidance that seeks to cost-effectively reduce the cybersecurity risks of the healthcare industry

WHY IS HHS CONVENING THIS EFFORT?
To strengthen the cybersecurity posture of the HPH Sector, Congress mandated the effort in the Cybersecurity Information Sharing Act of 2015 (CISA), Section 405(d)
Achieving Cyber-Readiness through Information Sharing Analysis Organizations (ISAOs)

Friday, March 23, 2018

What’s Next: Pre-Testing and Medical Community Baselining

Pre-Testing of 405(d) Guidance:
- Assessments with Medical Professionals, HPH CIOs/CISOs, and other HPH Staff.
- Assessing practicality, usability, and actionability.

Medical Community Baselining Phase II (Building for Version 2.0):
- Qualitative Research with Medical Professionals, HPH CIOs/CISOs, and other HPH Staff.
- Assessing levels of awareness and prioritization of cybersecurity.

Growing prevalence & magnitude of cyber attacks
- Q1 2017: Phishing and ransomware attacks more prevalent worldwide with ransomware increasing 250%.
- Q2 2017: More publicly disclosed security incidents in the life sciences and healthcare industry than in any other sector.

Organizational Risks
- Reputation and integrity
- Confidentiality and compliance
- Availability of needed information and communication systems

Federal Requirements
- HIPAA Security Rule
- Meaningful Use

Why should small- to mid-sized healthcare organizations care about cyber-readiness?

Florida Hospital Association
Achieving Cyber-Readiness through Information Sharing Analysis Organizations (ISAOs)

Friday, March 23, 2018

Florida Hospital Association

According to the Health Care Industry Cybersecurity Task Force, challenges include:
- lack of infrastructure to identify and track threats
- technical capacity to analyze the threat data in order to quickly translate it into actionable information.

What are the challenges to small to mid-sized health organizations becoming cyber-prepared?

- Healthcare organizations
  - FQHCs and other CHCs
  - Behavioral health centers
  - Rural and community health systems
  - RHCs
  - Long-term care
- Their vendors
- Their partners

Who does the Population Health ISAO help?
Secure Together Program

- **Vulnerability Management:** Provides a technological platform that maintains standard techniques for identification of cyber exploits and introduces cyber risk management.
- **Brings two very critical elements together:** Compliance and Vigilance
- **Peer comparison and Business Intelligence:** Organizations can use REAL threat intelligence data from Secure Together to understand where they stack up against their peers.

Cyber threats and vulnerabilities of critical components of the healthcare ecosystem put the reputations and businesses of health organizations and patient lives at risk. Secure Together minimizes that risk.

**Executive Order (EO) 13691** protects ISAO participants (individuals and transportation organizations) against being penalized as they share information regarding cyber-related breaches, interference, compromise or incapacitation. Through EO 13691, the Population Health ISAO is to:

- Protect individuals’ privacy & civil liberties
- Preserve business confidentiality
- Safeguard the information being shared

*If my organization shares information with an ISAO will it be penalized?*
How does my organization join the standard Secure Together program?

Step 1
Target stops attack from hacker

Step 2
Within seconds Smart Hive learns what Target did to stop the attack.

Step 3
Within minutes Smart Hive will tell all Retail Members in the HIVE what defense to put up. The Hacker cannot attack anyone in the HIVE.

Threat intelligence shared in real time with all Smart Hive customers, preventing additional attacks of the same kind.

How does Smart Hive work?
How does my organization’s firewalls connect to the Secure Together platform?

1) All security devices send event logs to a central SEM or syslog server
2) SEM forwards event to Echo Station (virtual server)
3) Echo station removes all sensitive information normalizes data. Normalized data is sent to the HIVE for analysis.

Cloud Ready: Hive is agnostic to data source.

What does my organization’s information look like to others in the HIVE?

Cloud Ready: Hive is agnostic to data source.
What information does the Secure Together platform collect and analyze?

What does the Secure Together program dashboard look like?
Achieving Cyber-Readiness through Information Sharing Analysis Organizations (ISAOs)

- Highly scalable - up to 2 million events per second
- Hosted in the cloud – AWS
- Cisco firewall, Palo Alto edge protection
- Air Gap security (isolates our network from unsecured networks and LANs)
- Lateral network techniques (prevents “sideways” attacks)
- AWS Lambda/ Serverless architecture - no surface to attack
- SSL data transfer – session authentication, no credentials are hard coded or persistent

Is Secure Together secure?

Kendra Siler, PhD
Kendra.Siler@ISAONetwork.org
904.318.5803

Population Health ISAO and Secure Together program contact:
Kendra Siler, PhD
Kendra.Siler@ISAONetwork.org
904.318.5803
NASA/Kennedy Space Center
AMF Center for Space Education
Kennedy Space Center, FL 32899

Healthcare... Secure Together,
Join Us!
Questions?

Upcoming Webinars

• Risk Assessment: Recognizing Today’s Threats and Your Vulnerabilities
• Protection Strategies for Your Network
• Protection Strategies for the Workforce and Your Devices
• Cloud Strategies and Continuity Coming Soon!
Thank you!

John Wilgis
407-841-6230
john@fha.org