HIMSS18 The leading health information and technology conference

WHERE THE WORLD CONNECTS FOR HEALTH

Conference & Exhibition | March 5–9, 2018

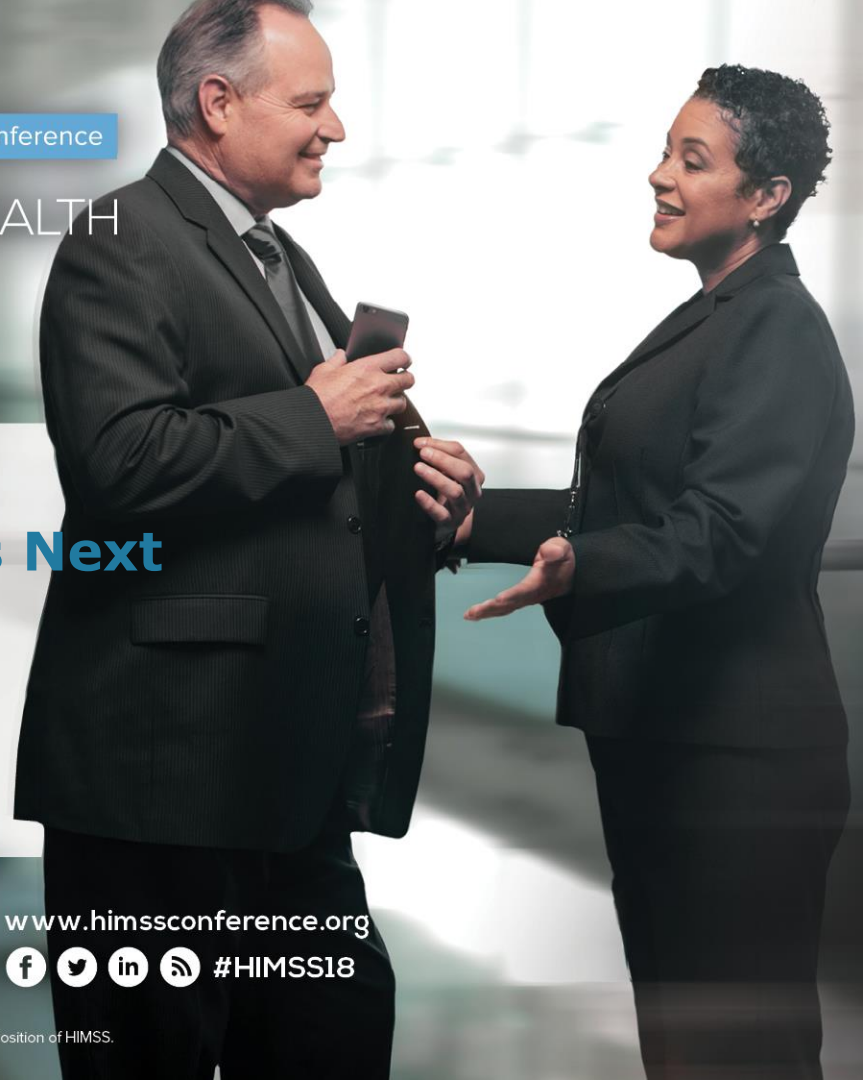
Las Vegas | Venetian – Palazzo – Sands Expo Center

Healthcare Cybersecurity: What's Next

CYB6, March 5, 2018

Kevin Stine, Chief, Applied Cybersecurity Division

National Institute of Standards and Technology



COMMITMENT

www.himssconference.org

#HIMSS18

Conflict of Interest

Kevin Stine has no real or apparent conflicts of interest to report.

Agenda

- Cybersecurity in Healthcare
- NIST's Cybersecurity Purpose
- Key Cybersecurity Activities and a Look to the Future
- Discussion and Questions

Learning Objectives

- Discuss how the interdependencies of the healthcare sector with other sectors introduce complexity into cybersecurity defense
- Describe advancements in technology for cybersecurity defense and how such technology may help your organization in the future
- Explore potential scenarios for the future and what to expect and plan for in the future in the realm of cybersecurity

Cybersecurity in Healthcare

"The growing convergence, interconnectedness, interdependence, and global nature of cyber and physical systems means that cybersecurity must be better managed in all contexts—international, national, organizational, and individual."

"While the threats are real, we must keep a balanced perspective. We should be able to reconcile security with innovation and ease of use. … We need to preserve those qualities while hardening it and making it more resilient against attack and misuse."

-- *Report on Securing and Growing the Digital Economy*, Commission on Enhancing National Cybersecurity, 12/1/2016

The health care system cannot deliver effective and safe care without deeper digital connectivity. If the health care system is connected, but insecure, this connectivity could betray patient safety, subjecting them to unnecessary risk and forcing them to pay unaffordable personal costs.

-- *Report on Improving Cybersecurity in the Health Care Sector*, Health Care Industry Cybersecurity Task Force, 12/1/2016

Cultivate trust in information and technology…

… By conducting foundational & applied research to produce and advance standards, best practices, measurements, and reference resources

Risk Management

Cryptography

Vulnerability Management

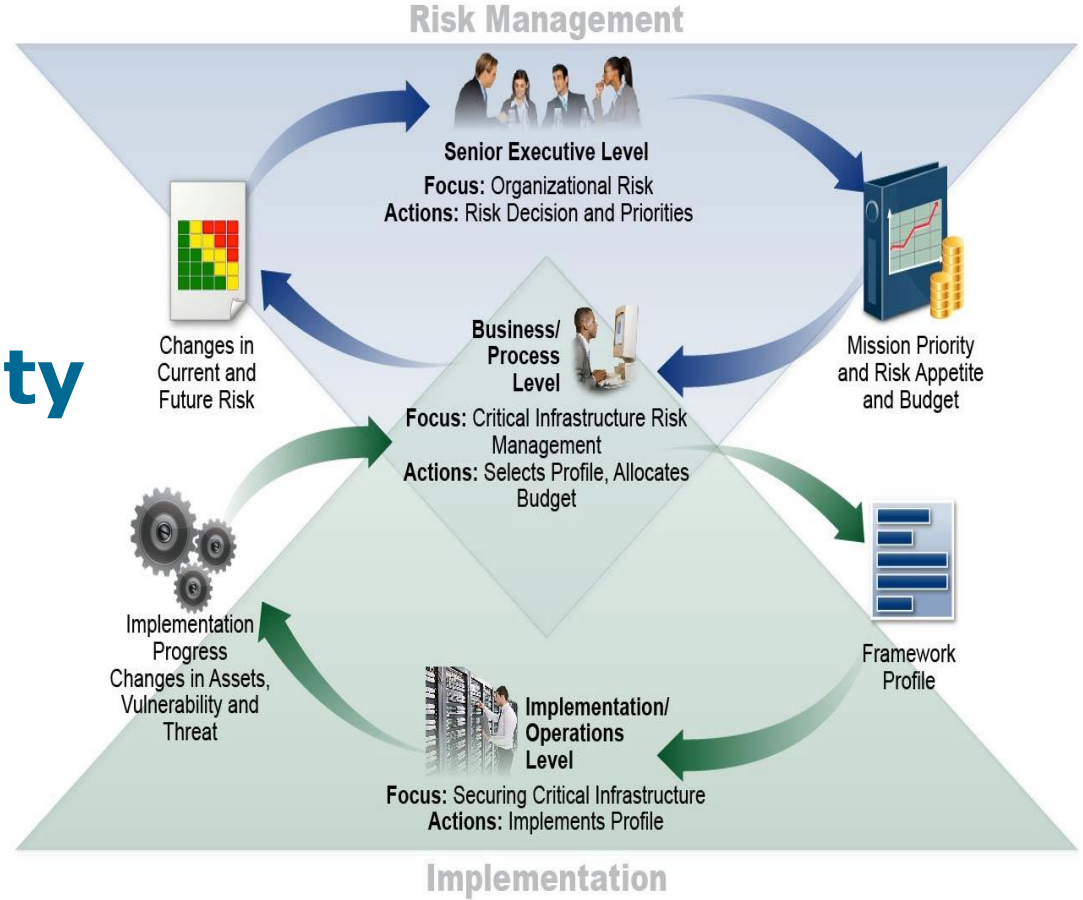
Identity and Access Management

Education and Workforce Development

Internet and Communications Infrastructure

Transition to Practice

Managing Cybersecurity Risk in the Enterprise

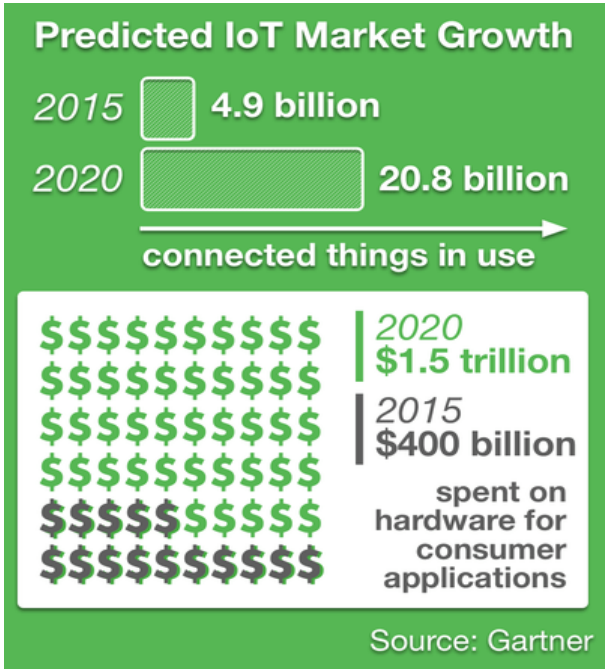


Understanding, Managing, and Communicating Cybersecurity Risk

- What processes and assets need protection?
- What safeguards are available?
- What techniques can identify incidents?
- What techniques can contain impacts of incidents?
- What techniques can restore capabilities?

https://www.nist.gov/cyberframework

IoT Adoption on the Rise



The Challenge

Fostering security for devices and data in the internet of things (IoT) ecosystem, across industry sectors and at scale

Program Mission

Cultivate trust in IoT and foster an environment that enables innovation on a global scale.

Cybersecurity for IoT

Develop & apply standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed.

https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

NIST Mobility Guidance

 NIST SP 800-124 Managing Enterprise Mobile Devices	Provides recommendations for selecting, implementing, and using mobile management technology.
 NIST SP 800-163 Vetting the Security of Mobile Applications	Helps organizations understand, plan, and implement a mobile app security review process.
 NIST SP 800-157 Guidelines for PIV Derived Credentials	Technical guidelines for a standards-based, secure, reliable, interoperable PKI-based PIV infrastructure.
 NIST SP 800-187 Guide to LTE Security	Provides a security analysis of the 4G LTE architecture.

Other Mobility Projects

Mobile Device Security for Enterprises	Using 2 separate management technologies to demonstrate a standards-based mobile deployment.
Handset & Wearable Security	Identify security objectives, determine best practices, and analyze the security of devices on the marketplace.
Over the Air SIM Updates	Analyze current OTA methods to determine the security posture for OTA and possible recommended enhancements.
Mobile Single Sign On	Demonstrate a Public Safety SSO architecture incorporating existing multiple authentication platforms.

NIST's National Cybersecurity Center of Excellence

Core Tenets

Standards-based

Apply relevant industry standards to each security implementation; demonstrate example solutions for new standards

Modular

Develop components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable

Provide a detailed practice guide including a reference design, list of components, configuration files, relevant code, diagrams, tutorials, and instructions to enable system admins to recreate the example solution and achieve the same results

Commercially available

Work with the technology community to identify commercially available products that can be brought together in example solutions to address challenges identified by industry

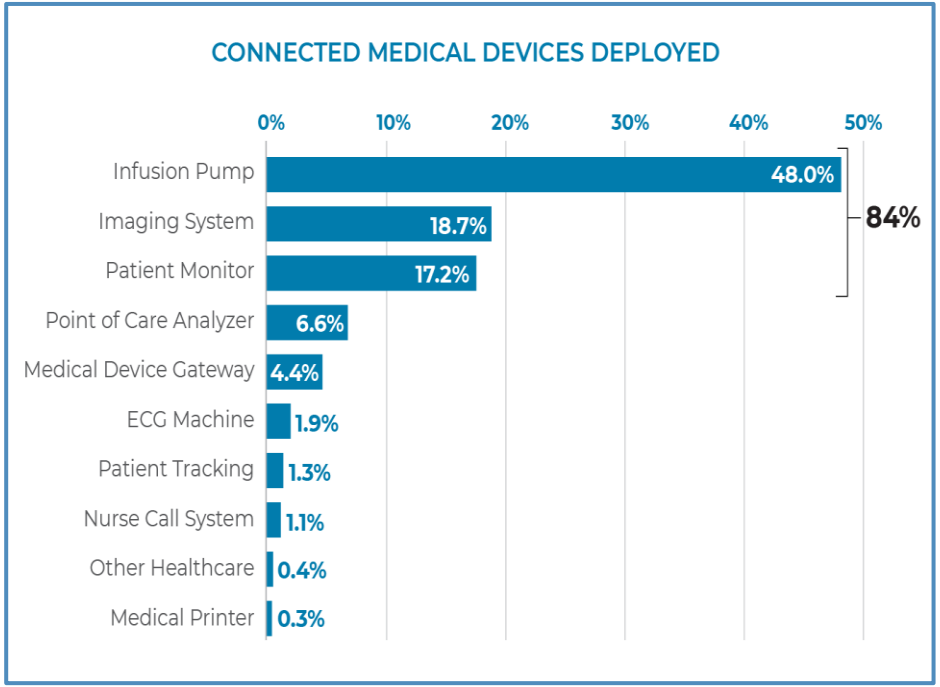
Usable

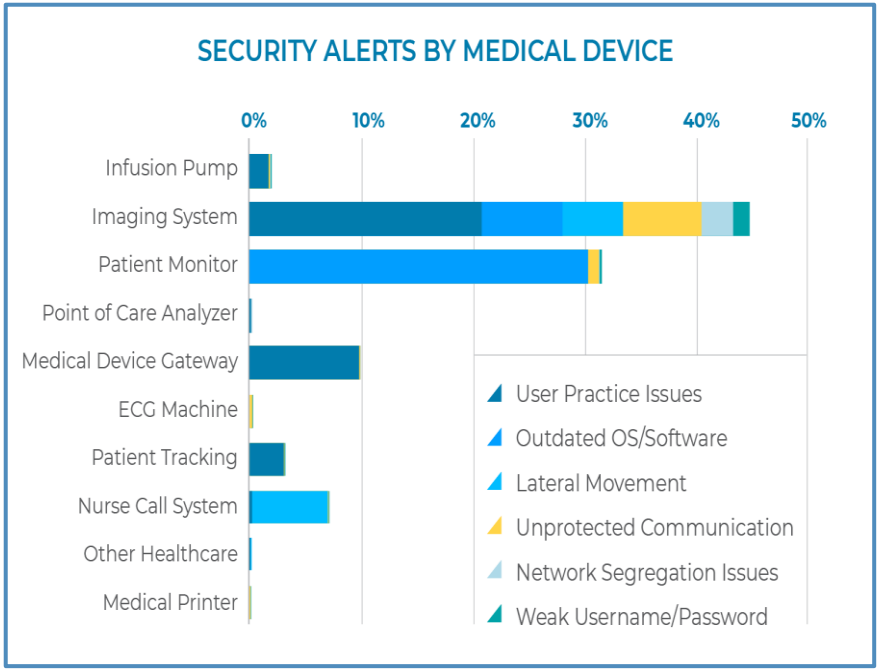
Design blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent

Use open and transparent processes to complete work; seek and incorporate public comments on NCCoE publications

Imaging Systems rank #2 in Number of Connected Medical Devices





Imaging Systems Lead in Security Alerts

Source: ZingBox, "*Threat Report on IOT Medical Devices*," 1/25/18

#HIMSS18

Securing Wireless Infusion Pumps in Healthcare Delivery Organizations

- Today's wireless infusion pumps connect to a variety of healthcare systems, networks, and other devices.
- While this can improve delivery of care, this can also increase cybersecurity risk.
- Apply security controls to the pump's ecosystem to protect infusion pumps and their surrounding systems against various risk factors.
- Guidelines demonstrate how to securely configure and deploy wireless infusion pumps to reduce cybersecurity risk.

https://nccoe.nist.gov/projects/use-cases/medical-devices

Securing Picture Archiving and Communication Systems

- PACS are nearly ubiquitous throughout healthcare delivery organizations, allowing remote image review by users.
- They interact with various healthcare systems and functions, and are central to doctor-patient workflow management.
- This project intends to provide a practical solution for securing the PACS ecosystem, including a reference design and example solution.

https://nccoe.nist.gov/projects/use-cases/health-it/pacs

Cybersecurity: What's Next

- Cloud
- Mobile
- IoT
- Data Integrity
- Cryptography
- Blockchain
- AI/ML

Some Closing Thoughts…

Questions

Kevin Stine
kevin.stine@nist.gov