Cybersecurity: An Emerging Emergency Management Challenge in the Healthcare and Public Health Sector

October 5, 2016

AHEPP Conference

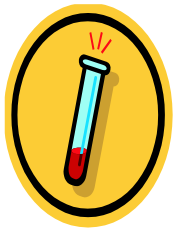
The Critical Infrastructure Protection Partnership

- The Critical Infrastructure Protection (CIP) Program is located in ASPR's Office of Emergency Management.
- CIP coordinates a partnership among federal, state, local, tribal, territorial, and private sector partners within the Healthcare and Public Health Sector to prepare for and respond to all hazards.
- The CIP program is organized around two primary functions:
  - Risk Management
  - Information Sharing

Healthcare and Public Health Sector Breakdown

- Direct Healthcare
- Health Plans and Payers
- Pharmaceuticals, Laboratories, and Blood
- Medical Materials
- Health Information Systems
- Mortuary Care
- Public Health





Cybersecurity In Healthcare: "Traditional" Risks

Attack Targets

- Personal identifiable information
- Payment systems

Impacts of Attacks

- Identity theft
- Healthcare fraud
- Breaches of privacy

Mitigation Measures

- Regulation (HIPAA / HITECH)
- Insurance
- Basic "cyber hygiene"

Recent Escalation of Size and Scope of Protected Health Information Breaches

- Prior to 2014 no hacking incident had ever been reported impacting 1 million patient records or more
- Since that time there have been 10 such incidents, impacting more than **120 million** patient records total.
  - July 2014, State Health Agency, **1.1 million**
  - August 2014, Hospital System, **4.5 million**
  - March 2015, Health Insurer, **79 million**
  - March 2015, Health Insurer, **11 million**
  - May 2015, Health Insurer, **1.1 million**
  - July 2015, Healthcare Software Vendor, **3.9 million**
  - September 2015, Health Insurer, **10 million**
  - March 2016, Specialty Care System, **2.2 million**
  - August 2016, Insurance I.D. Card Provider, **3.5 million**
  - August 2016, Hospital System, **3.6 million**

Growing Threat of Ransomware Attacks

- Ransomware attacks are showing the potential to disrupt healthcare operations.
- February 2016 hospital ransomware attack (CA)
  - Interrupted communications for more than one week.
  - Caused the hospital to revert to manual record-keeping.
  - Caused patient transfers and service cancellations.
  - Caused hospital to declare an internal emergency.
- April 2016 hospital system ransomware attack (MD/DC)
  - Caused systems to be shut down at 10 hospitals.
  - Led to loss of access to patient records and other IT functions.
- And an unknown number more...

Ransomware (continued)

- In a recent survey, half of respondents were aware of having been hit with at least one ransomware attack in the past year.

Source: April 2016 Healthcare IT News and Healthcare Information and Management Systems Society (HIMSS) Analytics Quick Hit Survey: Ransomware

- In another recent survey, respondents identified the most significant future threats.
  - Ransomware **(69%)**
  - Advanced persistent threat (APT) attacks **(61%)**

Source: Healthcare Information Management Systems Society (HIMSS) 2016 Cybersecurity Survey

A Growing List of Threats

- "Traditional" Threats
  - Financial Crimes
  - Identity Theft
  - Healthcare Fraud
- Emerging Threats
  - Large Scale PII Theft
  - Intellectual Property
  - Hacktivism
  - Ransoming

- Potential Future Threats
  - Malicious Attacks
  - Medical Devices
  - SCADA Systems

Why Public Health Emergency Management?

- Incidents are increasingly showing the potential to impact lives and health.
- Some incidents may not be detected until information aggregated across multiple patients/facilities
- Incidents often exceed the organization's capacity to respond and require bringing in outside resources.
- Cyber response encounters similar issues to "traditional" response
  - Coordination with law enforcement
  - Coordination across levels of government
  - Importance of risk communication and public affairs

Federal Cybersecurity Structures: Response

- FBI
  - Cyber Watch (CyWatch)
  - Internet Crime Complaint Center (IC3)
- DHS
  - National Cybersecurity and Communications Integration Center (NCCIC)
- HHS
  - Office for Civil Rights (OCR)
  - Food and Drug Administration (FDA)
  - Office of the Assistant Secretary for Preparedness and Response (ASPR)

Federal Cybersecurity Structures: Preparedness

- National Institute of Standards and Technology
- DHS
  - Office of Infrastructure Protection (IP)
  - Office of Cybersecurity and Communications (CS&C)
  - Office of Cyber and Infrastructure Analysis (OCIA)
- HHS
  - FDA
  - Office of the National Coordinator for Health IT (ONC)
  - ASPR Healthcare and Public Health Sector Critical Infrastructure Protection Partnership

National Policies

- Executive Order 13636, Improving Critical Infrastructure Cybersecurity
- Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing
- Cybersecurity Information Sharing Act of 2015
- Cybersecurity National Action Plan
- Presidential Policy Directive 41

HPH Sector Activities

- Policy Development
  - Healthcare Industry Cybersecurity Task Force
  - NIST Framework Implementation
- Information Sharing Activities
  - Homeland Security Information Network
  - Threat briefings
  - Teleconferences, webinars, and presentations
  - Information sharing study
- Preparedness and Response Activities
  - Development of cyber incident response plans
  - Participation in exercises

What Else Can We Do?

- Implement of NIST Cybersecurity Framework and related standards at all levels of the healthcare system.
- Encourage collaboration between IT and Emergency Management staff.
- Incorporate cyber incidents into response plans.
- Incorporate cyber threats in risk assessments.
- Engage in cybersecurity exercises.
- Recognize that future “outbreaks” could potentially have a cyber nexus
- Be aware of cyber attacks conducted while other incident responses are underway.

Questions?

Steve Curren

U.S. Dept of Health & Human Services

Stephen.Curren@hhs.gov

cip@hhs.gov

www.phe.gov/cip