February 6th, 2014

Out of Sight, Not Out of Mind: The Growing Risks of Medical Devices

The 22nd National HIPAA Summit

Mac McMillan
FHIMSS, CISM
CEO, CynergisTek

CYNERGISTEK

www.cynergistek.com

Securing The Mission of Care

Today's Presenter

- Co-founder & CEO CynergisTek, Inc.
- Chair, HIMSS P&S Policy Task Force
- Chair, HIMSS P&S Steering Committee
- HIT Exchange Editorial Advisory Board
- HCPro Editorial Advisory Board
- HealthInfoSecurity.com Editorial Advisory Board
- Health Tech Industry Advisory Board
- Director of Security, DoD
- Excellence in Government Fellow
- US Marine Intelligence Officer, Retired

Mac McMillan
FHIMSS/CISM
CEO CynergisTek, Inc.

CYNERGISTEK

Medical Devices

Discussion Items

- The Threat Is Real
- “Catch 22”
- The Government’s Response
- The Question

“Broken Hearts”

- The series plot shows how dangerous a dedicated terrorist can be with the right information.
- Vice President Walden is assassinated by hacking his pacemaker and inducing a heart attack.

CYNERGISTEK

The Washington Post

October 21, 2013

The headline read:

"Yes, Terrorists could have hacked Dick Cheney's heart."

A real life example, in 2007 doctors disable the communication capability of Vice President Cheney's defibrillator to prevent hacking.

CYNERGISTEK

A History

1957 - 1993

- Pacemaker, Implants, Drug Pump, ICD and other medical devices are introduced

2002 - 2006

- Remote monitors and wireless devices are introduced

2007 - 2012

- Researchers such as Jay Radcliffe, Nathaniel Paul and Barnaby Jack warn of risks with connected devices

2012

- Barnaby Jack demonstrates successfully hacking an insulin pump remotely

2013

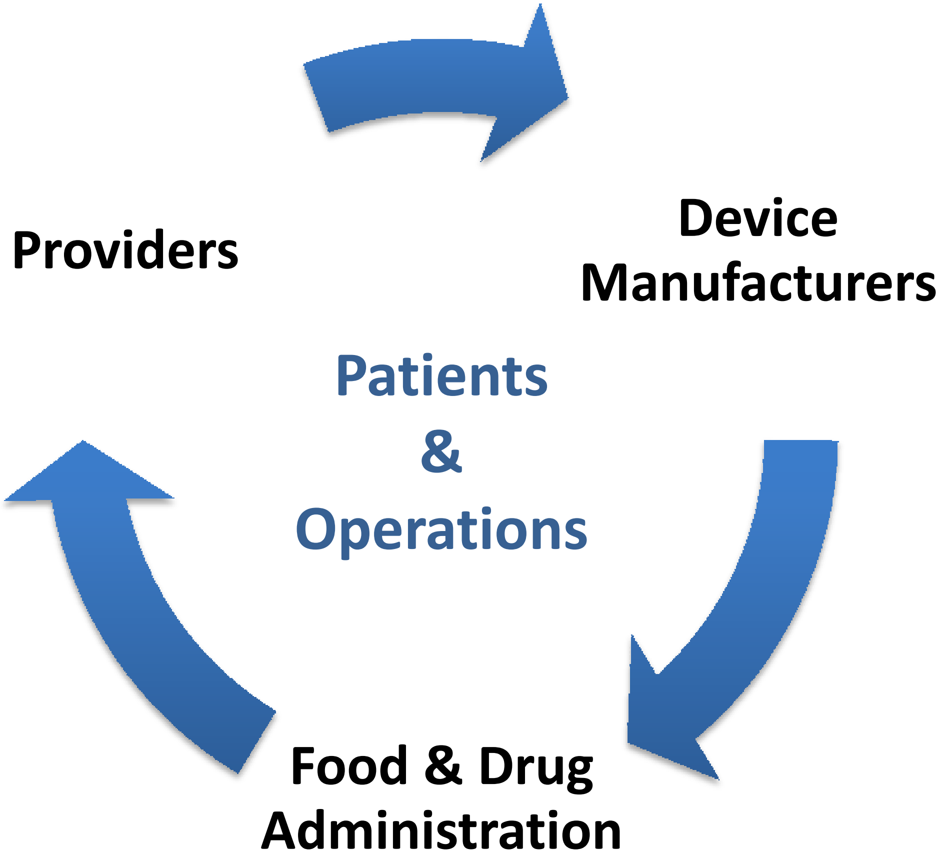
- Barnaby Jack successfully hacks pacemaker, the Homeland Episode airs, DHS issues advisory after ¾ of 300 devices found insecure and FDA issues guidance for device makers and consumers

Networks & Devices At Risk

- If you did not think Malware was a threat, think again…
- 3.4 million BotNets identified
- Slightly less than half of all malware hosted in the United States
- 26% of Malware delivered via HTML, one in less than 300 emails infected
- Malware analyzed last year was undetectable in 40% of all anti-virus engines tested
- Starting in April 2014 Microsoft will no longer provide patches for WN XP and 2003. WN 2000, NT, etc. are already EOL

Various: Symantec, IBM, Solutionary Annual Threat Reports

“Catch 22”



CYNERGISTEK

Government Response

- Alert (ICS-ALERT-13-164-01). Medical Devices Hard-Coded Passwords, *June 13, 2013*
- Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, *June 14, 2013*
- Radio Frequency Wireless Technology in Medical Devices, *August 14, 2013*
- Unique Device Identification System, Final Rule, *September 24, 2013*

DHS Alert

- Alert discusses a hard-coded password vulnerability affecting roughly 300 medical devices across 40 vendors
- “If exploited could be used to change critical settings or modify device firmware”
- Affected devices include: surgical and anesthesia devices, ventilators, drug infusion pumps, external defibrillators, patient monitors & laboratory analysis equipment

Premarket Submissions for Management of Cybersecurity in Medical Devices

Draft – Contains Non-Binding Recommendations

- Provides recommendations for effective cybersecurity management
- Stresses a careful consideration of the balance between cybersecurity and usability
- Security considerations include:
  - Limited access to trusted users only
  - Ensuring trusted content
  - Use of fail safe and recovery features
  - Hazards analysis, mitigations and design considerations
  - Traceability matrix linking controls to risks
  - Plan for providing validated updates and patches
  - Certification that device is provided free of malware
  - Instructions for antivirus/firewall use when appropriate

Radio Frequency Wireless Technology in Medical Devices

Contains Non- Binding Recommendations

- Provides guidance for addressing considerations related to incorporating radio frequency wireless technology in medical devices, to include:
  - Considerations for selecting RF bands
  - Wireless quality of service issues
  - Wireless Coexistance issues
  - Security of wireless signals & data
  - Electromagnetic compatibility issues
  - Proper set up and operation
  - Considerations for maintenance
  - Labeling considerations for users

CYNERGISTEK

Unique Device Identification System
Final Rule

Federal Food, Drug and Cosmetic Act

- Requires medical device manufacturers to provide a unique identifier as part of the label on medical devices
- This is a post market surveillance effort designed to:
  - Reduce medical errors
  - Simplify integration of device use information
  - Provide for more rapid identification of deices with adverse events
  - Provide for more rapid resolution of problems
  - Facilitate effective safety communications with the FDA

CYNERGISTEK

The Problem

- Most of the FDA’s guidance on medical devices does not establish legally enforceable responsibilities. Instead, it describes the Agency’s current thinking on a topic and provides recommendations, unless specific regulatory or statutory requirements are cited.

FDA Guidance Documents

The “Late” Barnaby Jack

Bloomberg

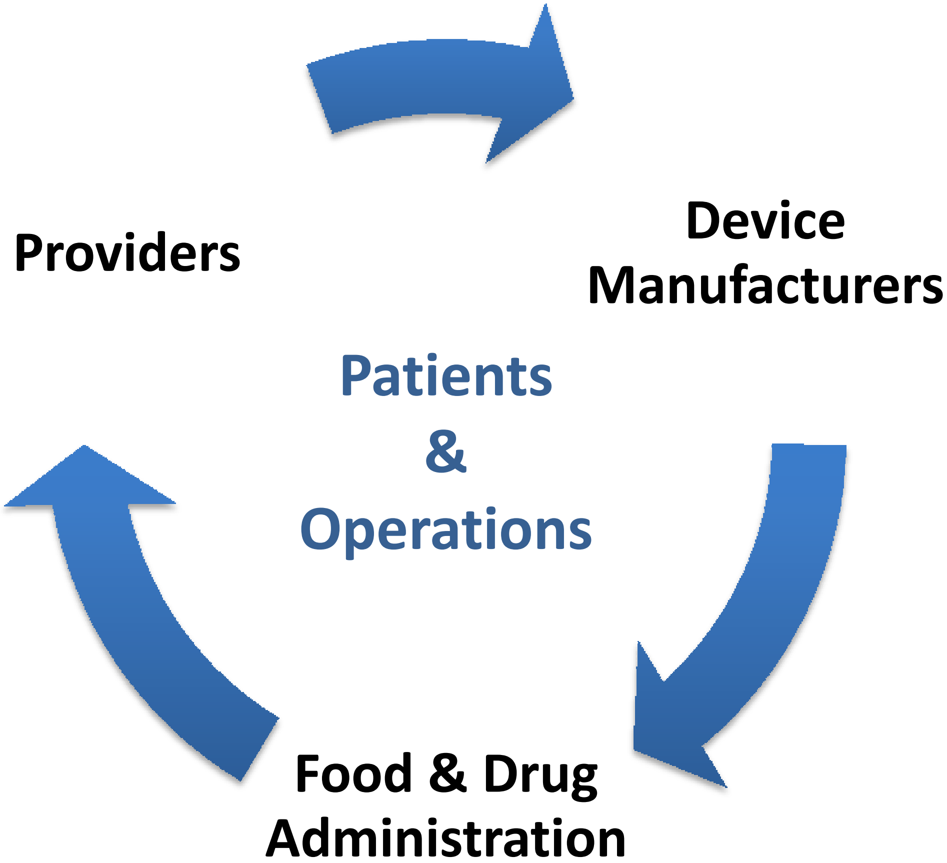
A laptop, a directional antenna and a poorly engineered solution…

Common Shortfalls Cited Across Industry

- Lack of communication between Biomedical/Clinical Engineering and Information Technology
- Poor policies and procedures for medical device management
- Lack of segregation of devices on the network
- Lack of comprehensive/accurate inventory of medical devices
- Lack of policy/standards defining minimal requirements for deployment on network
- Non-existant or poorly defined patch management practices
- Devices running on EOL operating systems
- Medical devices not included in risk assessments
- Incomplete or missing MDS2 forms for devices deployed
- Medical devices not included in Entities HIPAA security program

The Question

What is it going to take?



Providers

Device Manufacturers

Food & Drug Administration

Patients & Operations

“Just because we haven’t heard of it yet doesn’t mean its not a risk.” *Bruce Schnierer*

CYNERGISTEK

Thank You

Mac McMillan
Mac.McMillan@cynergistek.com
(512) 402-8555
www.cynergistek.com

CYNERGISTEK