Addressing the Privacy & Security Risks of Medical Devices

Presented By:

Clyde Hewitt, Executive Advisor

CynergisTek won the 2017 Best in KLAS Award for Cyber Security Advisory Services

CynergisTek has been recognized by KLAS in the 2016 and 2018 Cybersecurity report as a top performing firm in healthcare cybersecurity.

1

Why CynergisTek?

Healthcare Focused

- Founded in 2004
- Over 1,000 hospitals
- Payers, Medical Device Manufacturers, Labs
- Vulnerability Assessments on 1.5M devices/year

Trusted Advisor

- Unbiased assessments & development
- Vendor agnostic
- Executive level sponsors
- Community-based problem solving

Award Winning

- **2018 KLAS** Top Comprehensive Firm for Cybersecurity Services
- **Best in KLAS** 2017 Cybersecurity Advisory Services
- 10 Best Cybersecurity Companies in 2018-CIOBulletin.com
- Top 10 Health Compliance Solution Provider-2017, Healthcare Tech Outlook
- Frost & Sullivan “Best Practices Award, 10/10”

Experts & Thought Leaders

- Unique OCR expertise
- Over 600 articles & interviews per year
- CHIME & AEHIS Foundation Firm
- ISACA, ISSA, NH-ISAC, InfraGuard
- HIMSS platinum member
- Served on board of AEHIS, CHIME, ACHE, HIMSS, etc.

2

Today's Presenter

- MS, CISSP, CHS, ISO 27001 Lead Auditor, Level III Program Manager, former PCI-QSA
- Subject matter expert on health information security management, security operations, & compliance
- Board of Directors (Past President), North Carolina Healthcare Information & Communications Alliance (NCHICA)
- 30-years executive experience in developing, implementing, and operating complex information technology and security programs
- Served in CSO roles for an Academic Medical Center, two hospital organizations, a payer, and an EHR vendor

Clyde Hewitt
Executive Advisor
CynergisTek, Inc.

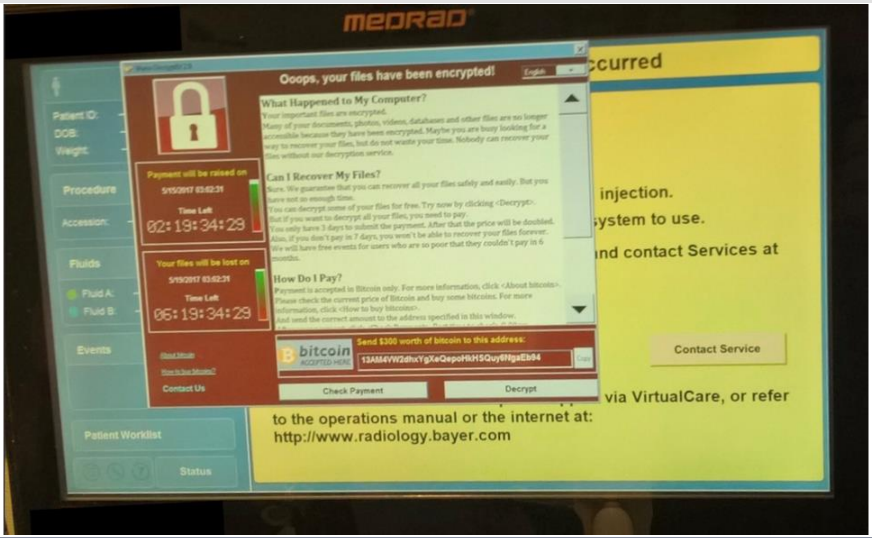
Desired Learning Objectives

Desired Learning Objectives

- Define the current security and patient safety risks posed by medical devices
- Analyze the operational challenges of managing medical device risks
- Identify best practices to incorporate medical devices into risk assessments and to implement a functional medical device governance structure

Security and Patient Safety Risks with Medical Devices

This Is Real, This Is Now



Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.

Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

ccurred

injection.

system to use.

nd contact Services at

via VirtualCare, or refer to the operations manual or the internet at:
http://www.radiology.bayer.com

https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#74

CYNERGISTEK

This Is Real, This Is Now

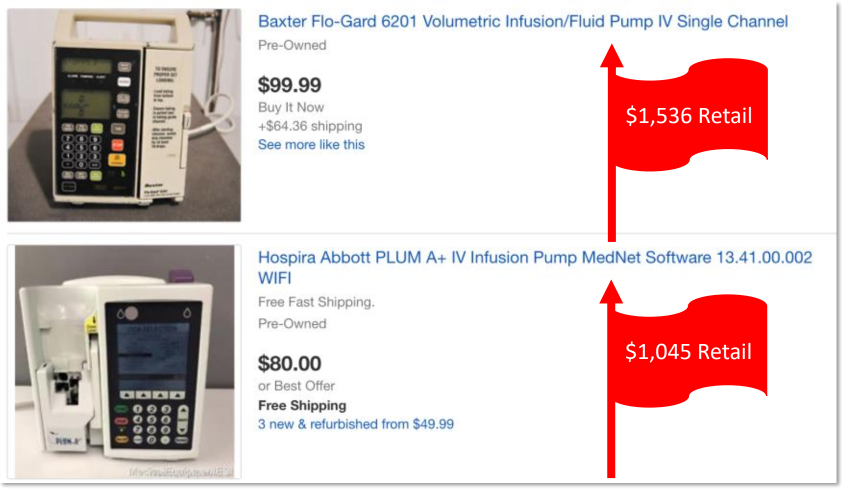
WakeMed technician accused of stealing supplies to sell on Ebay

- ....charged Tuesday with stealing $20,000 worth of supplies **and medical devices** from the hospital since early November...
- ... a magistrate noted that police said he had $20,000 worth of “equipment” in his home...
- ... worked as a clinical services technician in the Pathology Department...

https://www.newsobserver.com/news/local/news-columns-blogs/barry-saunders/article197575019.html

CYNERGISTEK

This Is Real, This Is Now



Baxter Flo-Gard 6201 Volumetric Infusion/Fluid Pump IV Single Channel

Pre-Owned

$99.99

Buy It Now

+$64.36 shipping

See more like this

$1,536 Retail

Hospira Abbott PLUM A+ IV Infusion Pump MedNet Software 13.41.00.002 WIFI

Free Fast Shipping.

Pre-Owned

$80.00

or Best Offer

Free Shipping

3 new & refurbished from $49.99

$1,045 Retail

https://www.ebay.com/sch/i.html?infusion+pump

CYNERGISTEK

9

This Is Real, This Is Now

"Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication"

The FDA has reviewed information concerning potential cybersecurity vulnerabilities associated with St. Jude Medical's RF-enabled implantable cardiac pacemakers and has confirmed that these vulnerabilities, if exploited, could allow an unauthorized user (i.e. someone other than the patient's physician) to access a patient's device using commercially available equipment. This access could be used to modify programming commands to the implanted pacemaker, which could result in patient harm from rapid battery depletion or administration of inappropriate pacing.

https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm

CYNERGISTEK

10

Ripped from the Headlines

- About 18% of provider organizations surveyed by KLAS experienced malware attacks on medical devices in the past 18 months. https://www.modernhealthcare.com/article/20181005/NEWS/181009942
- August 31, 2018 - Nine cybersecurity vulnerabilities have been found in the Philips e-Alert Unit, a tool that monitors MRI system performance, according to an Aug. 30 ICS-CERT advisory. https://healthitsecurity.com/news/9-cybersecurity-vulnerabilities-found-in-philips-e-alert-tool
- October 15, 2018 - The FDA issued a medical device safety alert about cybersecurity vulnerabilities in Medtronic's CareLink programmers that could enable an attacker to change the functionality of the programmer or the implanted pacemaker it controls. https://healthitsecurity.com/news/fda-warns-of-cybersecurity-vulnerabilities-in-carelink-programmers
- November 7, 2018 - ICS-CERT is warning about cybersecurity vulnerabilities in Roche point-of-care handheld medical devices. https://healthitsecurity.com/tag/medical-device-security
- January 30, 2019 - DHS Alerts to Vulnerabilities in Stryker and BD Medical Devices – Smart medical beds subject to wireless attacks that can lead to compromise of administrator accounts.https://healthitsecurity.com/news/dhs-alerts-to-vulnerabilities-in-stryker-and-bd-medical-devices

CYNERGISTEK

11

But Why All the Attention Now. . .

- Medical device security was thrust into the spotlight in 2018, as the Food and Drug Administration continued to bolster its cybersecurity program.
- August 2018 MedCrypt report found that since the FDA released its cybersecurity guidance in 2016, medical device vendors reported 400 percent more vulnerabilities per quarter.

CYNERGISTEK

12

12

And Why Is This a Compliance Problem?

- There are several medical device risks that can adversely impact healthcare organizations, including:
  - **Compliance risks:** medical devices contain electronic protected health information, so devices that are lost, stolen, or accessed by unauthorized individuals result in privacy incidents which must be investigated, and potentially reported as breaches

Operational Challenges of Securing Medical Devices

Historical Perspective – Starting with Culture

Skipping through history...

- 35 years ago Clinical Engineering was maintenance focused
  - Management/consulting services & support for discrete equipment

While on the other side...

- IT historically was focused on the business side of healthcare
  - Accounting, billing, A/P and P/R, Supply Chain

Many providers still have not closed the chasm between the two cultures

- Clinical Engineering departments typically do not report to IT departments
  - Clinical Engineering reports to Operations, Procurement, Facilities, or sometimes to vendors
- Compliance and Security teams are often left outside the door

Securing Medical Devices Is Hard, Technically...

- Unlike IT-managed laptops & servers, medical devices...
  - Are sometimes purchased new with obsolete/EOL operating systems
  - May not have the ability to integrate endpoint protection software
  - Are generally not designed to be remotely managed
  - Are installed with default user ID and passwords
  - May not have the ability to be encrypted
  - AND..., security is just not considered a priority

Are the Manufacturers On-Board?

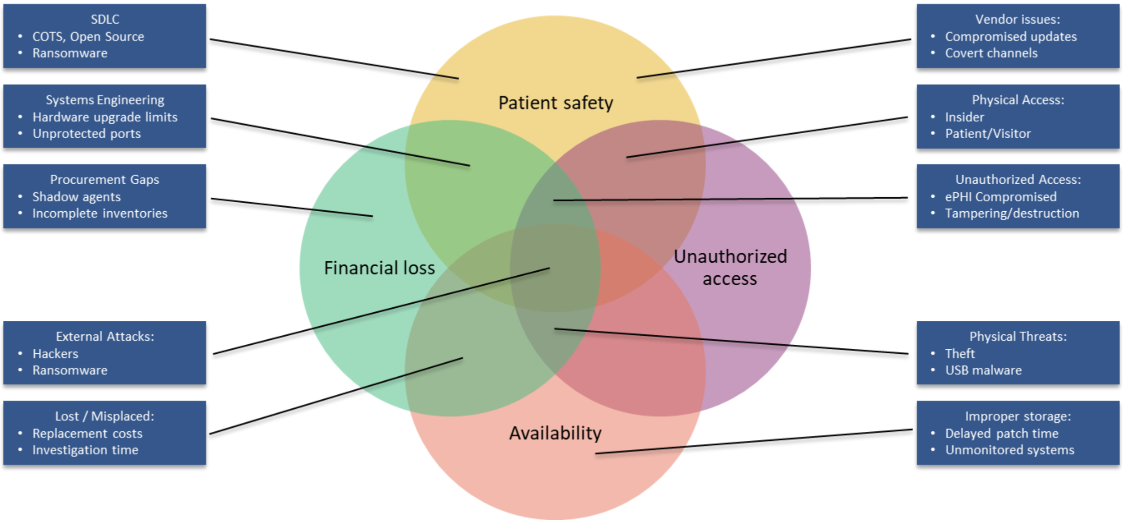
- 67% of medical device makers
  - Believe their devices are likely to be attacked in next 12 mo.[1]
- 17% of device makers
  - Are taking significant steps to prevent attacks[2]
- 10 to 15 connected devices
  - Per bed in U.S. hospitals[3]

[1] Synopsys, “Medical Device Security: An Industry Under Attack and Unprepared to Defend,” https://www.synopsys.com/software-integrity/resources/analyst-reports/medical-device-security-report.html
[2] Ibid.
[3] Newman, L.H.; “Medical Devices Are the Next Security Nightmare,” Wired, 2 March 2017, https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

Compliance Challenges

- Asset management gaps
  - Visibility issues
  - Cultural issues
  - Accountability
- Access management gaps
  - Always on
  - Generic logins, if used at all
- Physical management
  - 10+ devices per hospital bed
- Technical vulnerabilities
  - Lax regulatory security focus
  - Delays between alerts/action
  - Legacy operating systems
  - Vulnerability scanning risks
- Resource gaps
  - Staff focused on physical assets
- Risk management lethargy
  - Risk assessment scope

Identifying All Risk Vectors



SDLC
- COTS, Open Source
- Ransomware

Systems Engineering
- Hardware upgrade limits
- Unprotected ports

Procurement Gaps
- Shadow agents
- Incomplete inventories

External Attacks:
- Hackers
- Ransomware

Lost / Misplaced:
- Replacement costs
- Investigation time

Vendor issues:
- Compromised updates
- Covert channels

Physical Access:
- Insider
- Patient/Visitor

Unauthorized Access:
- ePHI Compromised
- Tampering/destruction

Physical Threats:
- Theft
- USB malware

Improper storage:
- Delayed patch time
- Unmonitored systems

Medical Device Management Best Practices

(or Five Easy Pieces)

1: Recognizing the Future, For it Is Already Upon Us

- Integrated medical systems whose function includes:
  - Store & permit retrieval of physiological data & images
  - Permit remote viewing of stored data/images by physicians & clinicians
  - Chart information to the EMR
  - Ingest personal data from personal wearables and remote monitor
- Examples of these integrated medical systems:
  - DB servers (physiologic monitoring)
  - Cardiac Cath lab and Diagnostic Cardia ultrasound
  - Endoscopy
  - Pacs/Lab/RX
  - Alarms
  - Fitbit

2: Identify the Drivers to CE-IT Convergence

- Integrating the Healthcare Enterprise (IHE)
- Patient Safety and Quality Outcomes Management
- Telemedicine
- Increasing application of:
  - RFID, DICOM, Bluetooth, WiFi
- Increased Government/Industry Focus
  - FDA, MDS2, other initiatives
- Information Security – integrity, availability, confidentiality
  - Cybersecurity, Privacy, Disruption (ransomware, DDoS)

3: Develop Management Solutions

- Biomedical devices are not just hardware
  - Treat them as computing endpoints
  - Treat them as if they contain patient data – many do!
  - Protect them from unauthorized physical and network access
  - You must presume a breach if lost, stolen, or even out of your control
- Addressing biomedical risks is a management problem
  - Accountability stops w/CEO, but departments share responsibility
  - The CISO and compliance must act as a team to assess these risks
- Look at newer tools that can passively scan
  - These also interface with the common CMMS applications
  - Consider outsourcing the security management to address talent gaps

4: Demonstrate That You Have A Problem

Conduct a litmus test to identify the extent of the problem

1. Ask for a copy of the Could Not Locate (CNL) list for previous 12 months
2. Determine if any devices on the list can create and store ePHI
3. For devices ID'ed in #2 above, ask if you have reported (or will report) a breach or have a documented "low probability of compromise" in your files
4. For all remaining devices, ask how any technical vulnerabilities have been remediated

5: Adopt a Framework

- Good security hygiene and awareness are key…
- But, there is *<u>no</u>* one-size-fits-all answer, this is unique to each org.
  - Key factors that make the difference:
    - Leadership style
    - Leaderships risk tolerance
    - Corporate/practice culture
  - The message needs to be delivered in a way the recipient can understand, in their terms
  - Training materials you find or get from outside *<u>need</u>* to be customized

Thank You!

We look forward to working together!

Questions?

Clyde Hewitt
Executive Advisor
clyde.hewitt@cynergistek.com
512-402-8550 x7016