Biomedical Device Security:
New Challenges and Opportunities

Florence D. Hudson
Senior Vice President and Chief Innovation Officer
Internet2

June 22, 2015

The evolution to today's reality in biomedical devices

- Number of connected devices is increasing with the goal to improve patient care and create efficiencies in the healthcare system
- Growing "Bring Your Own Device" paradigm for providers and patients
- Proprietary / closed devices and systems are "assumed" secure
- Inadequate teamwork between medical providers, device vendors, technology innovators, cybersecurity experts, insurance companies, regulators, patients, to assess & address vulnerabilities
- ROI not agreed for improved security needs across ecosystem
- Rate of innovation is slow, and will continue to be unless we work as a Collaborative Innovation Community

Biomedical devices have inadequate security controls

"There is no such thing as a threat-proof medical device"

Suzanne Schwartz, M.D., MBA, Director of emergency preparedness/ operations and medical countermeasures at the FDA Center for Devices and Radiological Health, October 2014

FDA areas of concern about cybersecurity vulnerabilities

- Malware infections on network-connected medical devices or computers
- Smartphones and tablets used to access patient data – "BYOD"
- Unsecured or uncontrolled distribution of passwords
- Failure to provide timely security software updates and updates to medical devices and networks

Source: http://www.informationweek.com/healthcare/security-and-privacy/fda-delivers-medical-device-security-guidelines/d/d-id/1316304

FDA recommendations for Management of Cybersecurity in Medical Devices

Cybersecurity - is the process of preventing unauthorized access, modification, misuse or denial of use, or the unauthorized use of information that is stored, accessed, or transferred from a medical device to an external recipient.

- Manufacturers should develop a set of cybersecurity controls to assure medical device cybersecurity and maintain medical device functionality and safety.
- Failure to maintain cybersecurity can result in compromised device functionality, loss of data (medical or personal) availability or integrity, or exposure of other connected devices or networks to security threats. This in turn may have the potential to result in patient illness, injury, or death.
- FDA recognizes that medical device security is a shared responsibility between stakeholders, including
  - Health care facilities
  - Patients
  - Providers
  - Manufacturers of medical devices.

Source: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices,
Guidance for Industry and Food and Drug Administration Staff, Document Issued on: October 2, 2014
http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

FDA recommendations for manufacturers to protect networked biomedical devices and patients

- Manufacturers should address cybersecurity during the design and development of the medical device
  - This can result in more robust and efficient mitigation of patient risks
  - Establish a cybersecurity vulnerability and management approach as part of the software and hardware validation and risk assessment

- Address the following elements
  - Identification of assets, threats, and vulnerabilities
  - Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients
  - Assessment of the likelihood of a threat or vulnerability being exploited
  - Determination of risk levels and suitable mitigation strategies

Source: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices,
Guidance for Industry and Food and Drug Administration Staff, Document Issued on: October 2, 2014
http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf ;
National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Available at:
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214- final.pdf

FDA provides considerations regarding Cybersecurity for biomedical devices

- Connected Medical devices are more vulnerable to cybersecurity threats than devices not connected (wireless or hard-wired) to networks, internet, other devices
- The extent to which security controls are needed depends on a number of factors
  - Device's intended use and environment of use
  - Presence and intent of electronic data interfaces
  - Type of cybersecurity vulnerabilities present
  - Likelihood the vulnerability will be exploited (intentionally or unintentionally)
  - Potential risk of patient harm due to a cybersecurity breach.
- Need to balance between cybersecurity safeguards and the usability of the device in its intended environment of use
  - Ensure that the security controls are appropriate for the intended use case
    - Home use vs. closely monitored health care facility use
    - Patient use vs. health care provider use
  - For example, security controls should not unreasonably hinder access to a device intended to be used during an emergency situation.

Source: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices,
Guidance for Industry and Food and Drug Administration Staff, Document Issued on: October 2, 2014
http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

FDA and NIST recommend 5 step Cybersecurity Framework: Identify, Protect, Detect, Respond, Recover

Identify and Protect

- **Limit Access to Identified, Trusted Users Only**
  - Multi-factor authentication (e.g., user ID and password, smartcard, biometric)
  - Layered authorization model by differentiating privileges based on the user role
  - Avoid “hardcoded” password or common words
  - Limit public access to passwords used for privileged device access
  - Automatic timed methods to terminate session and/or update password
  - Require user authentication before permitting software or firmware updates

- **Ensure Trusted Content**
  - Restrict software or firmware updates to only authenticated code
  - Use systematic procedures for authorized users to download version-identifiable software and firmware from the manufacturer
  - Ensure capability of secure data transfer to and from the device, when appropriate use encryption

FDA and NIST recommend 5 step Cybersecurity Framework: Identify, Protect, Detect, Respond, Recover

Detect, Respond, Recover

- Implement features that allow for security compromises to be detected, recognized, logged, timed, and acted upon during normal use
- Develop and provide information to the end user concerning appropriate actions to take upon detection of a cybersecurity event
- Implement device features that protect critical functionality, even when the device's cybersecurity has been compromised
- Provide methods for retention and recovery of device configuration by an authenticated privileged user

Source: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices,
Guidance for Industry and Food and Drug Administration Staff, Document Issued on: October 2, 2014
http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf ;
National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Available at:
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214- final.pdf

Start today to identify and address risks and challenges to overcome to provide improved connected healthcare

Considerations	Potential Actions
Security / Privacy	• Design in security and privacy from the beginning for devices and applications • Use federated identify and multi-factor authentication
Cultural transformation	• Engage patients & providers in development of the devices and solutions • Focus on user experience
Data quality	• Systematic data analysis and cleansing
Integrating data from various systems to get a complete picture	• Use connectors & translators to integrate multiple data formats and protocols
Ownership, collection, use and sharing of data	• Develop and deploy enterprise data policy, comply with regulatory policy
Incorporating new types of sensors / devices	• Develop an extensible architecture to incorporate future data / sensor types

We must work together across the healthcare & technology ecosystem to improve biomedical device security

Assess and understand the risks

- Threat vectors
- Malicious and inadvertent security/safety issues
- Singular and extended risks

Work as Collaborative Innovation Community (CIC) to improve security

- Collaborative Innovation Community to include medical providers, device vendors, technology innovators, insurance companies, regulators, patients
- Start with assessment of device security, privacy, safety risks
- Agree ROI for improved security needs based on device / use case

Classify & enable medical devices for appropriate levels of Trust, Identity, Privacy and Security (TIPS)

- FDA has provided guidance on medical device categories
  - Class I (low-risk) - not relied on in decision to take immediate clinical action
  - Class III (high-risk) - sustain human life, prevent impairment, risk of illness/injury
- TIPS requirements can be determined by device Class / connected use case
  - Low TIPS requirements – e.g., FitBit, wearable IOT clothing
  - High TIPS requirements – e.g., insulin pump, heart device
- Collaborative Innovation Community of technology & device vendors, providers, payers can develop optimized security based on use case & cost to reduce risk
- Security can be addressed at various levels in a biomedical device
  - Based on the low or high TIPS requirements
  - "Defense in Depth" – multiple levels of security & privacy can be developed.
  - Enable any/all of Service level, Software level, Firmware level, Hardware level
- Service level security is fastest to deploy, followed by software
- Firmware and hardware level security take more time to bake into the device

Source: Mobile Medical Applications, Guidance for Industry and Food and Drug Administration Staff, Feb. 9, 2015 ;
Medical Device Data Systems, Medical Image Storage Devices, and Medical Image Communications Devices Feb. 9, 2015

MAYO
CLINIC

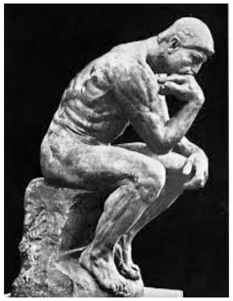
Medical Device Security in a Connected World

Debra Bruemmer
Manager of Clinical Information Security

Mayo Clinic Overview

- Mayo Clinic decided to dramatically increase it’s security posture
  - Over 1 million patients per year
  - Paperless patient care
  - ~230,000 active IP addresses
  - High profile patients, significant intellectual property, and classified research
- Hired an external CISO & formed Information Security Department
- Reviewed “surface area” of environment
  - ~10,000 Windows servers
  - ~2,000 Linux servers
  - ~80,000 workstations
  - ~20,000 +++ networked medical devices
  - ?????
- Found a significant number of networked devices not IT “managed”
- Formed team focused on medical device security – **Clinical Information Security**

Mayo Clinic Philosophy



- Incorporate security into the procurement process
  - RFP questions and standard security contract language
  - Practice drives purchase decision, security enables secure execution
- Test medical devices, do not wait for the vendors to identify and address issues
- Document/Share test findings with the vendor
  - Outline actions and timeline to address findings
  - Prefer collaboration vs. public disclosure
  - Goal: Partner with our vendors to have a safe outcome for our patients; this includes assisting vendors in providing us with a secure product

- Benefit society by using Mayo Clinic's influence
  - Require changes made put into standard product
  - Drive changes for long term vendor process improvements

What You Learn from 2 Years of Medical Device Security Research and Management …

Vendor Situations

- Most are engaged and trying to catch up
  - Struggling to change internal culture and build security awareness
  - Think of themselves as device manufactures, not software developers
  - No one has a full understanding of how everything works together
- Engineers & product designers really "love" their software
- Executives understand the company/brand impacts (thanks to Target)
- Poor processes for development, testing, and support
  - Lack coding standards with security tollgates
  - Lack hardened configuration standards
  - Lack testing process & tools (vulnerability scanning, fuzz & penetration testing)
  - Lack mature processes to apply updates & patches across install base

- Vendor Responses
  - Initial reaction is guarded, follow up meetings have been more productive
  - Remediation timelines are prolonged **(~ 88% of issues are vendor owned)**
- Significant support process implications

MAYO CLINIC

Incorporate Security Language Into Procurement Contracts

- Medical device questions to include in RFPs
  - Modeled from ICS-CERT materials
- Security contract – Mayo Minimum Requirements:
  - Security standards
  - Development standards
  - Requirements for meeting FDA guidelines
  - Breach response program
  - Vulnerability notification
  - Testing and scanning requirements
    - SANS CWE Top 25
    - OWASP Top 10
  - Installation standards
  - Testing rights
  - Penalties for failure to fix issues
  - Indemnification for cyber-security incidents caused by device
- NDA for testing and IP sharing

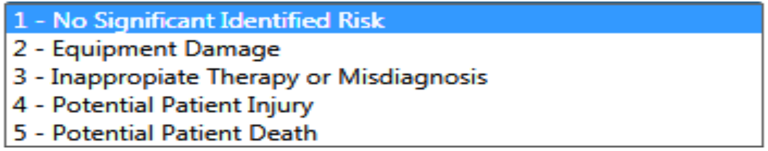
Focus Security Testing on Risks

- Current production devices and systems
- Upgrades and new versions
- Pre-purchases
- Remediated devices
- Medical Devices AND Clinical Support Systems (applications)
  - Infant Protection System
  - Nurse Call
  - Temperature Monitoring
  - Etc.

Standard Security Testing Process

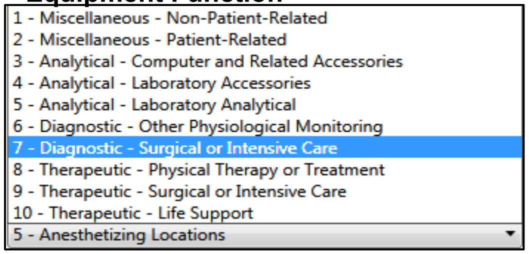
- Focus on high priority devices
  - Greatest potential to cause patient harm
  - Greatest potential to widely disrupt patient care processes
- Engage all stakeholders
  - Mayo (Clinical Users, Biomed, IT, Facilities)
  - Vendor
- Assess the whole "device family"
  - Follow the data flow to include points of testing
  - Workstations, servers, & endpoint
  - Document demographic information, establish rules of engagement
- Testing outcomes drive remediation efforts
  - Network mitigations
  - Endpoint & system mitigations
  - Partnering with the vendor

Clinical Application

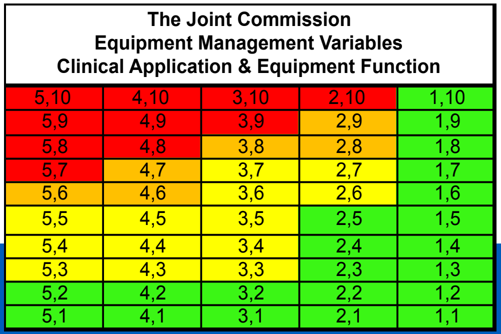


1 - No Significant Identified Risk
2 - Equipment Damage
3 - Inappropiate Therapy or Misdiagnosis
4 - Potential Patient Injury
5 - Potential Patient Death

Equipment Function



1 - Miscellaneous - Non-Patient-Related
2 - Miscellaneous - Patient-Related
3 - Analytical - Computer and Related Accessories
4 - Analytical - Laboratory Accessories
5 - Analytical - Laboratory Analytical
6 - Diagnostic - Other Physiological Monitoring
7 - Diagnostic - Surgical or Intensive Care
8 - Therapeutic - Physical Therapy or Treatment
9 - Therapeutic - Surgical or Intensive Care
10 - Therapeutic - Life Support
5 - Anesthetizing Locations



The Joint Commission
Equipment Management Variables
Clinical Application & Equipment Function

5,10	4,10	3,10	2,10	1,10
5,9	4,9	3,9	2,9	1,9
5,8	4,8	3,8	2,8	1,8
5,7	4,7	3,7	2,7	1,7
5,6	4,6	3,6	2,6	1,6
5,5	4,5	3,5	2,5	1,5
5,4	4,4	3,4	2,4	1,4
5,3	4,3	3,3	2,3	1,3
5,2	4,2	3,2	2,2	1,2
5,1	4,1	3,1	2,1	1,1

Standard Security Testing Process

- Testing includes:
  - Operational security review
  - Vulnerability scanning using commercial and public scanners
  - Fuzz testing
  - Penetration testing simulating multiple attack scenarios
  - Assessing a subset of application code
- Testers are provided network access to the system, the name of the product, and IP address
- Testing Outcomes
  - Generate detailed vulnerability assessment report
  - Review report with internal proponents
  - Review report with vendor
  - Outline and document actions (vendor and Mayo)
  - Track actions for closure

Standard Security Testing Process

- Comprehensive test report
  - Rate vulnerabilities as high / medium / low severity
  - Complete details enable vendor to reproduce the vulnerability
  - Include screen prints, video, scripts, etc.
- Initial week of testing good to have a vendor rep on-site to provide feedback on severity and to understand the process & vulnerabilities found

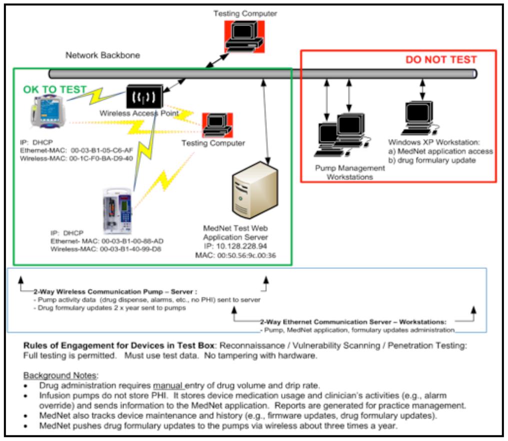
Testing Axiom

"Visibility, Transparency, Moral High Ground"

Security Testing – System Thinking

- No device lives in isolation
- Need to review the ecosystem a device lives in
- Many devices have control software that is vulnerable
- External access methods and process require testing
- Map communication patterns to determine all possible threat vectors, test the whole chain
- End user processes can thwart security measures

Device Family Concept is Important



2-Way Wireless Communication Pump – Server :
- Pump activity data (drug dispense, alarms, etc., no PHI) sent to server
- Drug formulary updates 2 x year sent to pumps

2-Way Ethernet Communication Server – Workstations:
- Pump, MedNet application, formulary updates administration

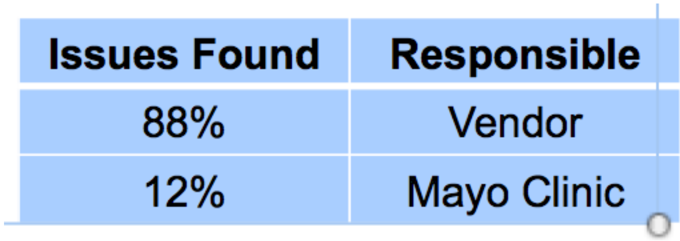
Rules of Engagement for Devices in Test Box: Reconnaissance / Vulnerability Scanning / Penetration Testing: Full testing is permitted. Must use test data. No tampering with hardware.

Background Notes:

- Drug administration requires manual entry of drug volume and drip rate.
- Infusion pumps do not store PHI. It stores device medication usage and clinician's activities (e.g., alarm override) and sends information to the MedNet application. Reports are generated for practice management.
- MedNet also tracks device maintenance and history (e.g., firmware updates, drug formulary updates).
- MedNet pushes drug formulary updates to the pumps via wireless about three times a year.

Security Testing - Statistics

- Tested or Reviewed
  - ~ 30 Device / System "Families"
  - Infusion pumps and formulary systems (multiple brands)
  - CT
  - MRI
  - Infant Abduction Protection
  - Building Automation
  - Etc.



Issues Found	Responsible
88%	Vendor
12%	Mayo Clinic

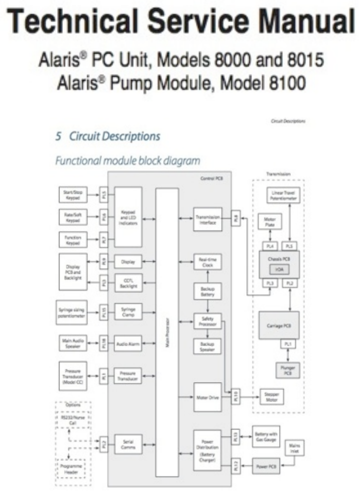
- Engaged 9 vendors in addressing findings
- Tested $100 million dollars of pre-purchased equipment
- Finalized contracts with 3 vendors to include security language (Mayo Minimum Security Requirements)

Medical Device Issues

- Operational Security Issues
  - Customer support web sites
  - Internal technical documentation
  - Publicly available information
  - Devices publically available for purchase
  - Customer service social engineering

- Application Vulnerabilities
  - Generally fragile software
  - Poor or no authentication
  - Elevated privilege requirements
  - No anti-virus
  - Many known exploits

- Configuration Vulnerabilities
  - Unneeded functionality left operational
  - Unneeded files / users / applications / ports
  - Default settings and passwords
  - Old communication and file transfer protocols



Technical Service Manual

Alaris® PC Unit, Models 8000 and 8015
Alaris® Pump Module, Model 8100

Circuit Descriptions

5 Circuit Descriptions

Functional module block diagram

Control PCB
Transmission
Start/Stop Keypad
Rate/Soft Keypad
Function Keypad
Keypad and LED Indicators
Display PCB and Backlight
Display
CCFL Backlight
Syringe sizing potentiometer
Syringe Clamp
Main Audio Speaker
Audio Alarm
Pressure Transducer (Model CC)
Pressure Transducer
Options
RS232/Nurse Call
Programme Header
Serial Comms
Main Processor
Transmission Interface
Real-time Clock
Backup Battery
Safety Processor
Backup Speaker
Motor Drive
Power Distribution (Battery Charger)
Linear Travel Potentiometer
Motor Plate
Chassis PCB
IrDA
Carriage PCB
Plunger PCB
Stepper Motor
Battery with Gas Gauge
Mains Inlet
Power PCB
PL1
PL2
PL3
PL4
PL5
PL6
PL7
PL8
PL9
PL10
PL12
PL13
PL15
PL18

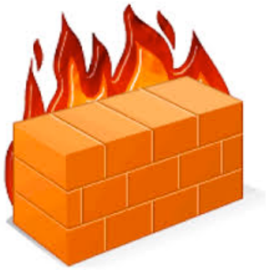
Adobe

Medical Device Issues

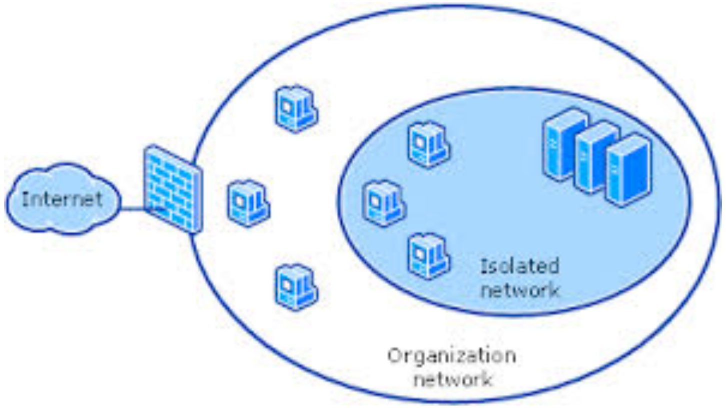
```
Starting MS-DOS...

C:\>_
```

- Unpatched Software
  - Old and un-supported operating systems
  - Unpatched COTS with published exploits
  - No updates schedules or processes
  - Time and labor intensive or patient care impact update process
- Lack of Encryption
  - PHI and PII not encrypted or weak encryption
  - Un-encrypted communication
  - Weak wireless encryption - WEP

Network Mitigation Strategies



- Remove from the network
- Attach to the network only when updates needed
- Network segmentation and isolation
  - Access Control Lists
  - Firewalls / IPS / IDS
  - Air gap



Many times have to be "hand crafted"

Endpoint & System Mitigation Strategies

- Remove un-needed applications (IE, MS Office, etc.)
- Change default passwords
- Patch & update if possible

Many times have to be “hand crafted”

- Remove un-needed or generic accounts
- Limit administrative accounts
- Review configurations of databases and third party software
- Super glue all open ports
- Install advanced end point protection
  - AV
  - Virtual patching
  - Host IPS

Targeted Monitoring Strategies

- Determine high risk / high impact devices
- Send system logs to a SIEM or a log manager
- Install agents (as able) to monitor for activity and file integrity
- Monitor netflows for unusual traffic
- Custom rules
  - High priority
  - Immediate alerts
- Develop analytic capabilities

First have to determine "normal"

MAYO CLINIC

Fixing the Medical Device System

- Vendors
  - Design in security for living in a dangerous environment
  - Make devices easily and efficiently upgradable
  - Include security in testing
  - Follow security best practices
  - Review operational security
  - "Think" like they are out to get you!

Everyone Has a Role

- Providers
  - Implement "defense in depth"
  - Monitor for issues and compromises
  - Develop business continuity and incident response plans
  - Perform timely upgrades
  - Test equipment before patient care
  - Include contract language that requires security, testing and liability
  - "Think" like they are out to get you!

MAYO CLINIC

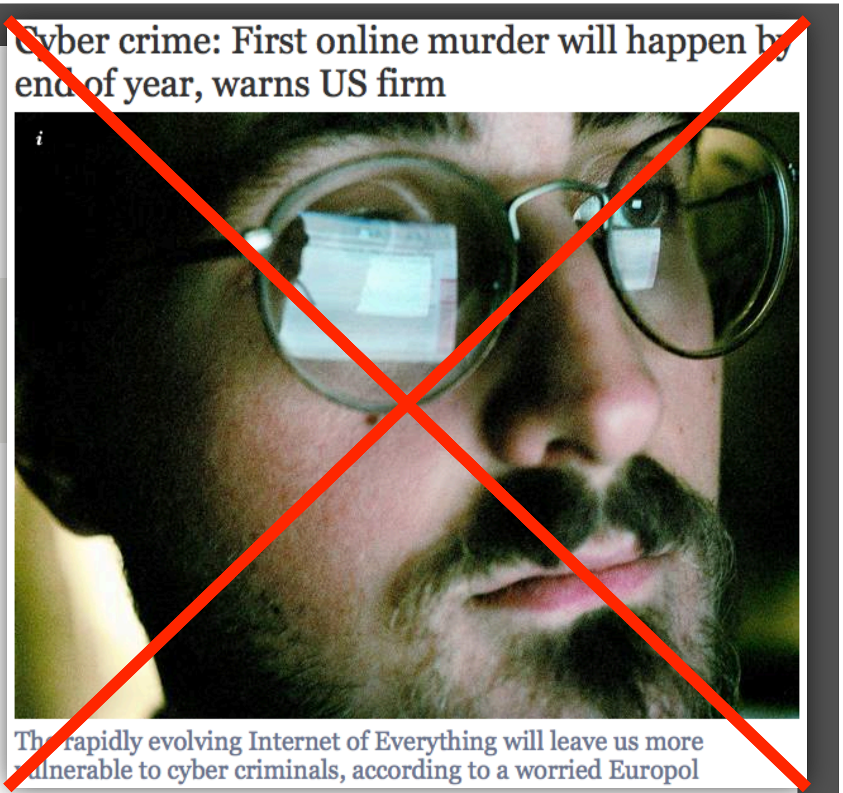
Fixing the Medical Device System

- Regulators
  - Have a prescriptive baseline for security
  - Provide a framework for best practice
  - Make cyber-security issues a mandatory reportable event
  - Revise issue submission and reporting to facilitate the entry and reporting of security issues
  - Regulatory actions for cyber-security issues
  - Exclusions in Digital Millennium Copyright Act (DMCA) for cyber-security testing
- Government Security Agencies
  - Implement a database of reported vulnerabilities
  - Provide intelligence for medical device issues and attacks
  - Investigations of issues and events
  - Security research

Final Thoughts

- The full medical device eco-system is currently broken
- We will be living with this problem for at least a decade
- While vendors have a responsibility to fix equipment, healthcare providers have a responsibility to protect patients
- The technology and knowledge exist to fix the problem, but it's not always a technology problem
- All healthcare organizations can and must take action, start small and mature your efforts
  - Educate yourself
  - Inventory and prioritize devices (engage Clinical, Biomed, and IT staff)
  - Talk with vendors
  - Incorporate contract language into procurement processes
  - Engage in industry efforts
  - Etc.
- Be prepared, it's only a matter of time…

Ok, this did not happen in 2014 …
somebody got ahead of themselves



Cyber crime: First online murder will happen by end of year, warns US firm

The rapidly evolving Internet of Everything will leave us more vulnerable to cyber criminals, according to a worried Europol

Medical Device Security

From Cybersecurity to Cybersafety

Axel Wirth, CPHIMS, CISSP, HCISPP
National Healthcare Architect
Distinguished Systems Engineer

June 22, 2015

Medical Device Security – a unique problem set

Regulated

- FDA Quality System Reg's: manufacturer to test & approve config.
- Lengthy and complex release process (product, updates, patches)
- Results in impact on: patching, cyber security (AV), security updates
- Providers need to comply with: HIPAA, HITECH, FDA MDDS

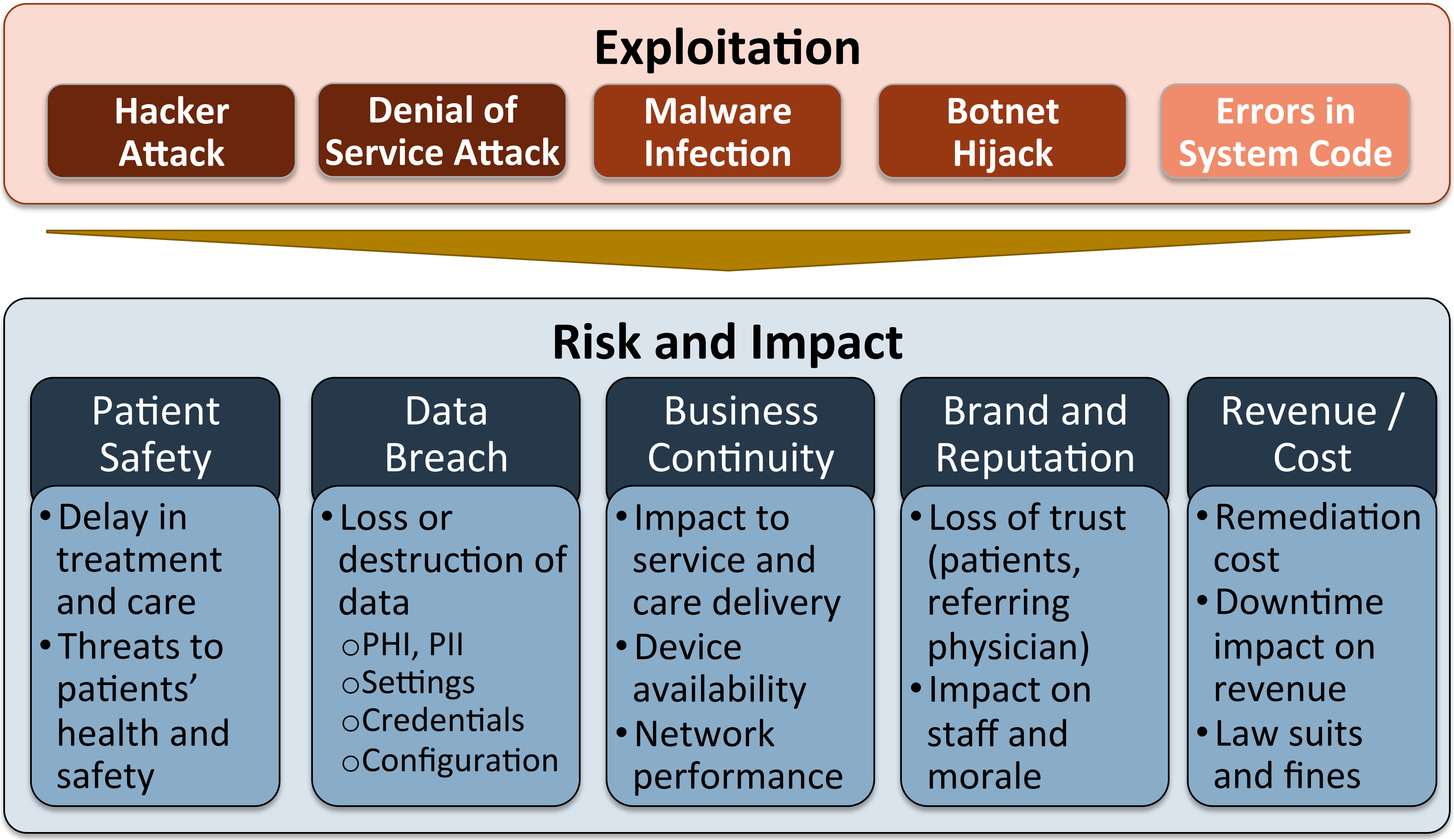
Complex

- "System of Systems", "Industry of Industries" Problem
- 10.000's of devices, 1.000's of types, 100's of manufacturers
- 5-10x of regular IT systems, 20-40% already networked
- Ownership & responsibility: IT vs. BioMed vs. Manufacturer

Vulnerable

- Multiple threat vectors: network, ports, USB, user
- Device breach/infection impact: operational to patient care & safety
- Device may hinder recovery & remediation
- "Weakest link" – can become entry point

Medical Device Threat Scenarios



Exploitation

- Hacker Attack
- Denial of Service Attack
- Malware Infection
- Botnet Hijack
- Errors in System Code

Risk and Impact

Patient Safety

- Delay in treatment and care
- Threats to patients’ health and safety

Data Breach

- Loss or destruction of data
  - PHI, PII
  - Settings
  - Credentials
  - Configuration

Business Continuity

- Impact to service and care delivery
- Device availability
- Network performance

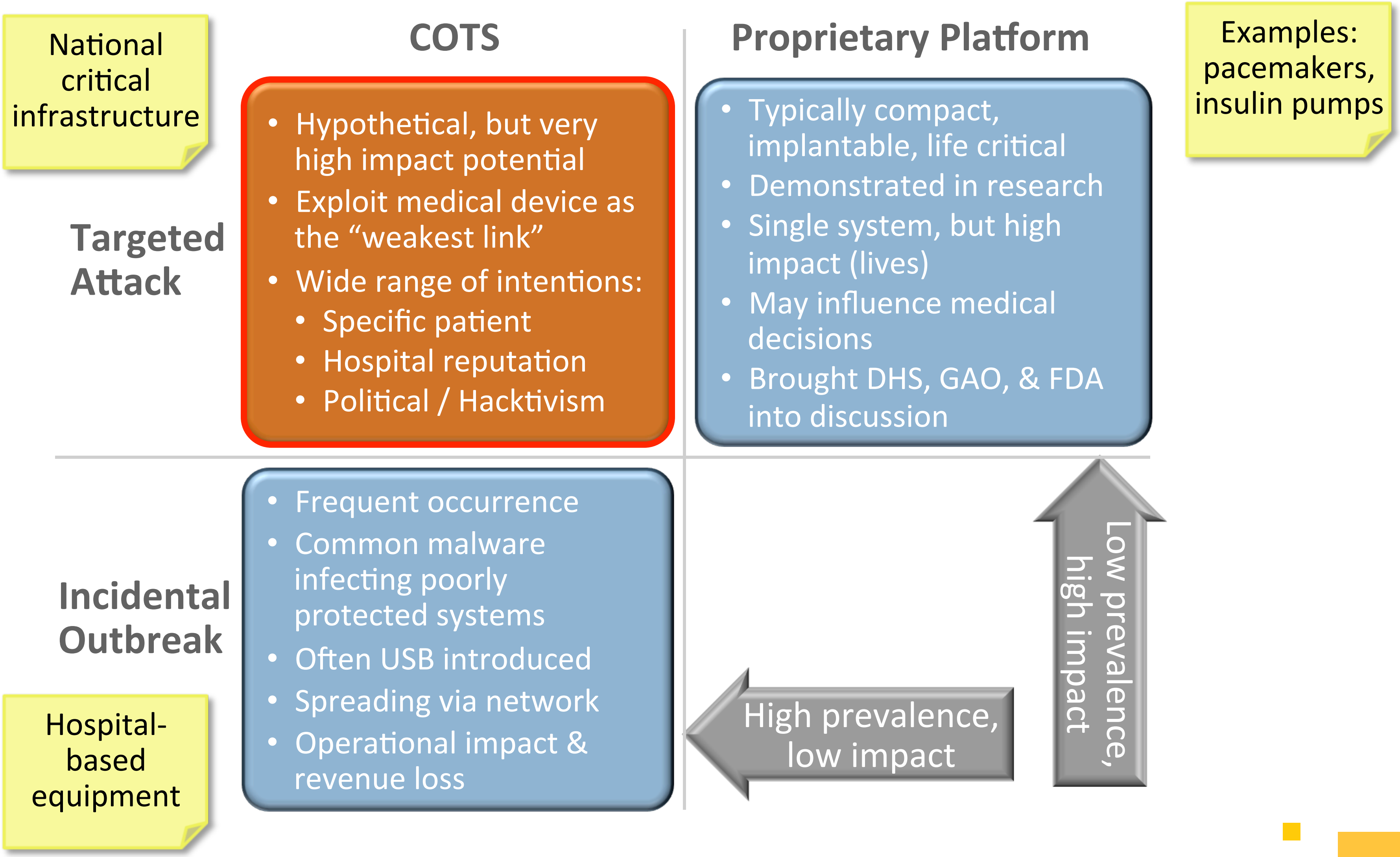
Brand and Reputation

- Loss of trust (patients, referring physician)
- Impact on staff and morale

Revenue / Cost

- Remediation cost
- Downtime impact on revenue
- Law suits and fines

Infection Scenarios: Intentional vs. Unintentional



National critical infrastructure

COTS

Proprietary Platform

Examples: pacemakers, insulin pumps

Targeted Attack

COTS:

- Hypothetical, but very high impact potential
- Exploit medical device as the "weakest link"
- Wide range of intentions:
  - Specific patient
  - Hospital reputation
  - Political / Hacktivism

Proprietary Platform:

- Typically compact, implantable, life critical
- Demonstrated in research
- Single system, but high impact (lives)
- May influence medical decisions
- Brought DHS, GAO, & FDA into discussion

Incidental Outbreak

COTS:

- Frequent occurrence
- Common malware infecting poorly protected systems
- Often USB introduced
- Spreading via network
- Operational impact & revenue loss

Hospital-based equipment

COTS = Commercial off-the-shelf Software

Malware Example – Conficker (computer worm)

Characteristics:

- Surfaced Nov. 2008 through 2009 (Conficker A-E); affected 200+ countries
- Microsoft patch available since Dec. 2008
- Today, largely eliminated in IT - but still a problem for Medical Devices

Capabilities:

- Spreads via <u>removable media</u>, mapped drives, shared folders, <u>LAN</u>
- Blocks AV sites, disables autoupdate, hides files
- Registers as system service, injects malware into good processes
- Upgrades itself, <u>downloads other malware</u>

Medical Device Risks:

- Medical Device Characteristics: Long useful life, poorly patched, lack of antimalware, easy to guess passwords (dictionary attack)
- Air-gap (USB) risk, spreads across network to devices with like vulnerabilities
- Medical Device exploited as the "weakest link"

Exploit / Impact Examples

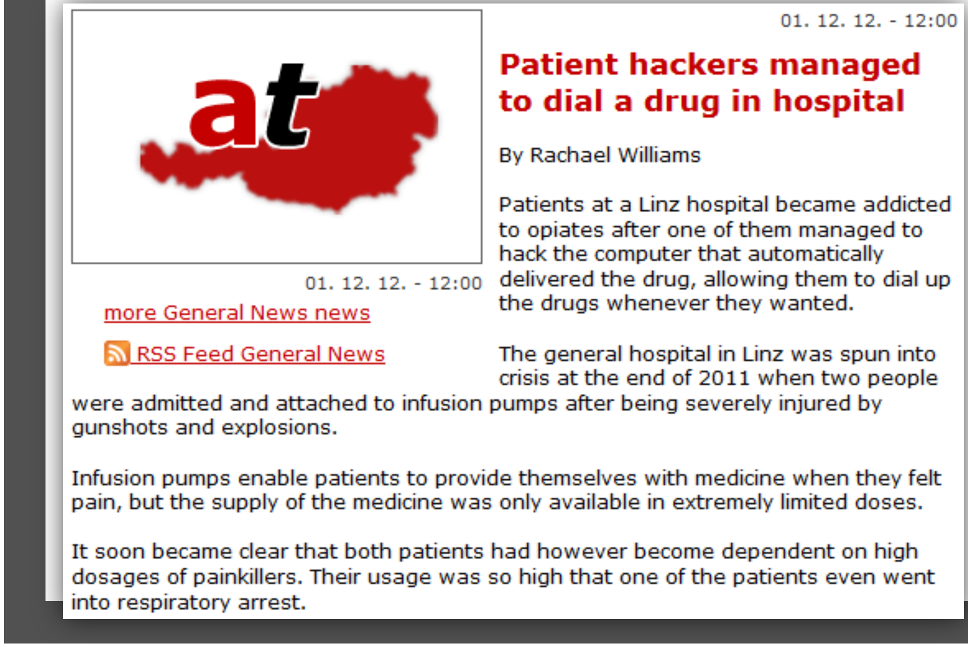
Conficker introduced by Service Tech and USB;
Infected Medication Cabinets across multiple sites
-> 24 hr manual medication management

Conficker introduced by Service Tech and USB;
Infected all equipment across 6 Cathlabs
-> Re-routing of all cardiac emergencies

Slow Ultrasound performance was
eventually contributed to Botnet activity

Impact – Further Examples

- Device hack (research only, so far)
- Device loss/theft (PHI breach)
- Drug abuse
- Patch deployment failure
- Multiple reports on device testing – with disastrous results
- ICS-CERT and FDA warnings
- FDA, DHS, FBI regulatory action



01. 12. 12. - 12:00

Patient hackers managed to dial a drug in hospital

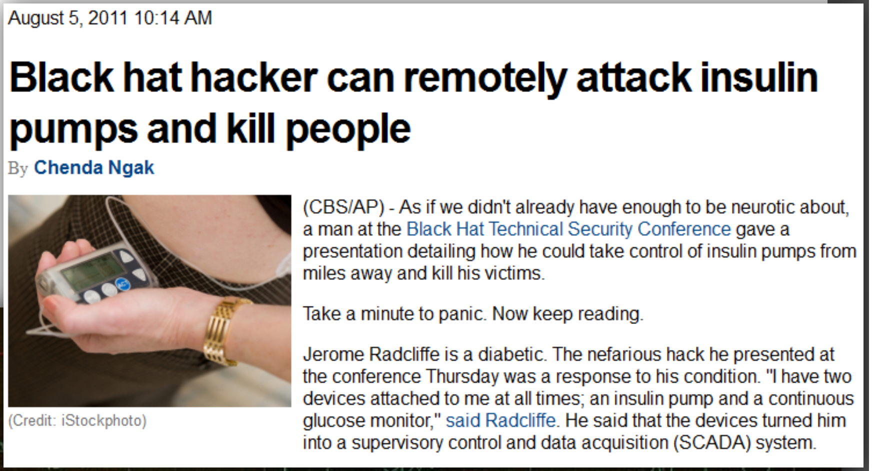
By Rachael Williams

Patients at a Linz hospital became addicted to opiates after one of them managed to hack the computer that automatically delivered the drug, allowing them to dial up the drugs whenever they wanted.

The general hospital in Linz was spun into crisis at the end of 2011 when two people were admitted and attached to infusion pumps after being severely injured by gunshots and explosions.

Infusion pumps enable patients to provide themselves with medicine when they felt pain, but the supply of the medicine was only available in extremely limited doses.

It soon became clear that both patients had however become dependent on high dosages of painkillers. Their usage was so high that one of the patients even went into respiratory arrest.



August 5, 2011 10:14 AM

Black hat hacker can remotely attack insulin pumps and kill people

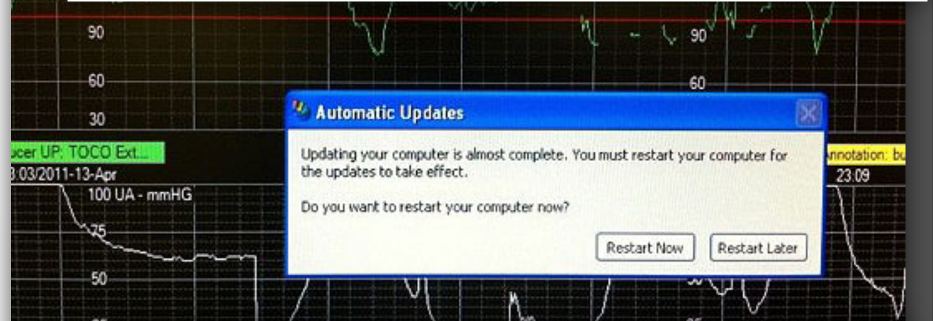
By Chenda Ngak

(Credit: iStockphoto)

(CBS/AP) - As if we didn't already have enough to be neurotic about, a man at the Black Hat Technical Security Conference gave a presentation detailing how he could take control of insulin pumps from miles away and kill his victims.

Take a minute to panic. Now keep reading.

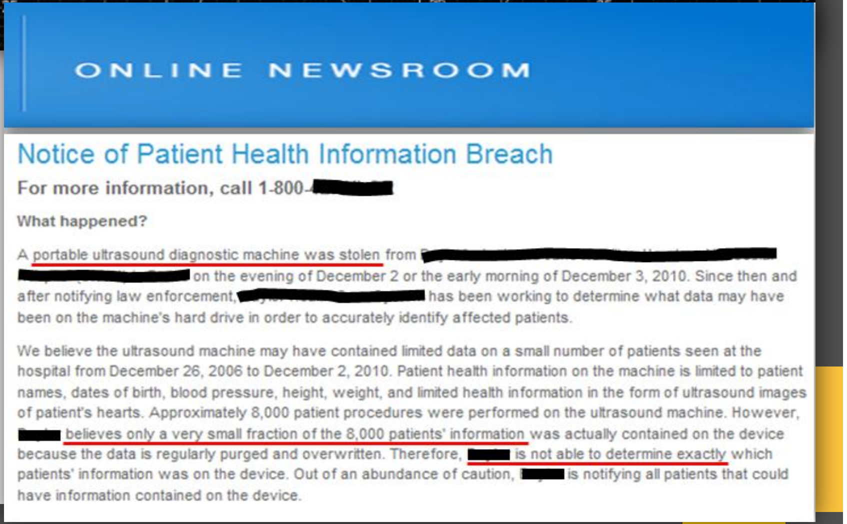
Jerome Radcliffe is a diabetic. The nefarious hack he presented at the conference Thursday was a response to his condition. "I have two devices attached to me at all times; an insulin pump and a continuous glucose monitor," said Radcliffe. He said that the devices turned him into a supervisory control and data acquisition (SCADA) system.



Automatic Updates

Updating your computer is almost complete. You must restart your computer for the updates to take effect.

Do you want to restart your computer now?



ONLINE NEWSROOM

Notice of Patient Health Information Breach

For more information, call 1-800-[redacted]

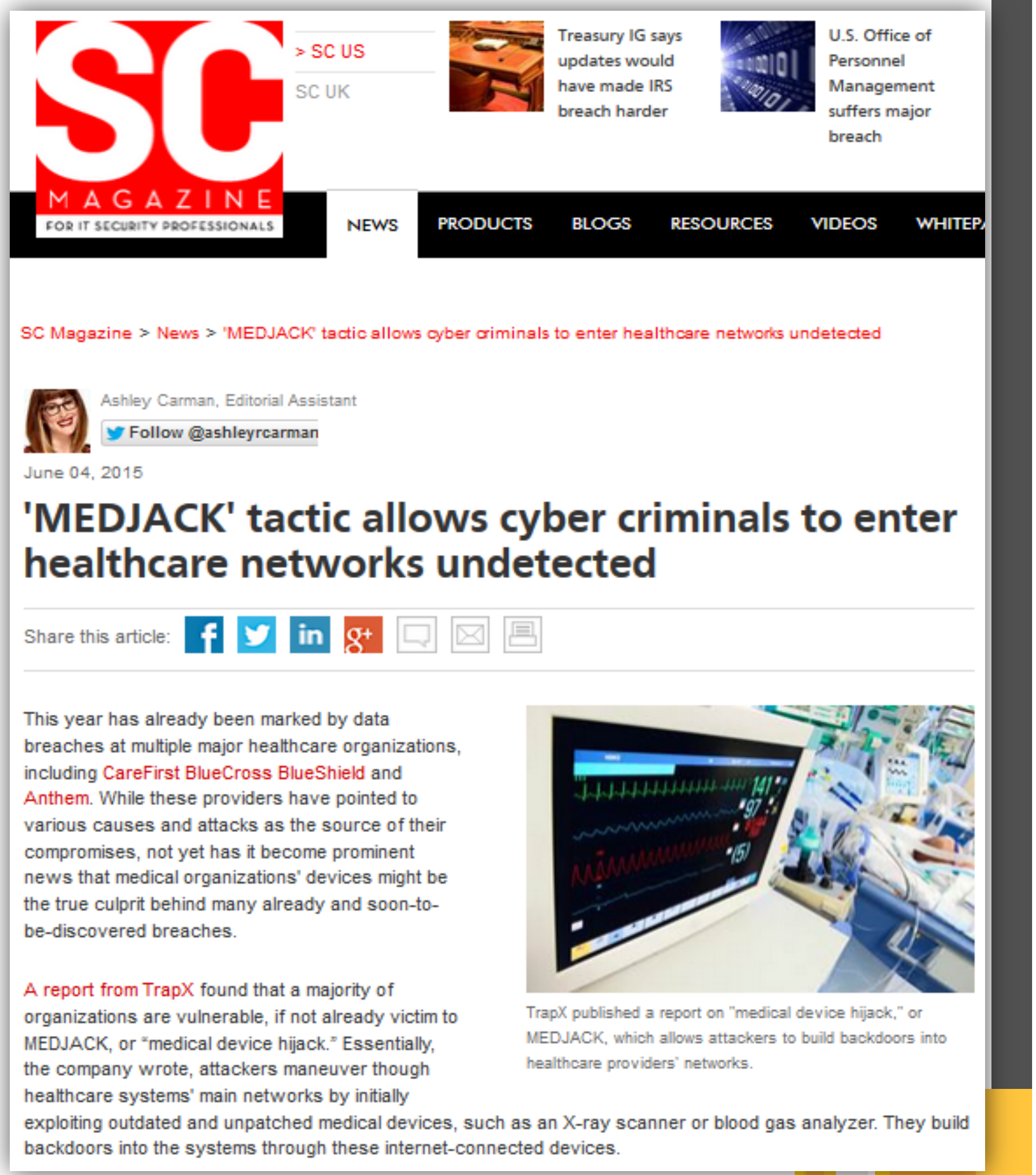
What happened?

A portable ultrasound diagnostic machine was stolen from [redacted] on the evening of December 2 or the early morning of December 3, 2010. Since then and after notifying law enforcement, [redacted] has been working to determine what data may have been on the machine's hard drive in order to accurately identify affected patients.

We believe the ultrasound machine may have contained limited data on a small number of patients seen at the hospital from December 26, 2006 to December 2, 2010. Patient health information on the machine is limited to patient names, dates of birth, blood pressure, height, weight, and limited health information in the form of ultrasound images of patient's hearts. Approximately 8,000 patient procedures were performed on the ultrasound machine. However, [redacted] believes only a very small fraction of the 8,000 patients' information was actually contained on the device because the data is regularly purged and overwritten. Therefore, [redacted] is not able to determine exactly which patients' information was on the device. Out of an abundance of caution, [redacted] is notifying all patients that could have information contained on the device.

But then …. Recently Reported

- MedJack Medical Device Hijack
- APT exploit of outdated / unpatched medical devices
- Compounded by difficulty to detect and remediate
- “Near perfect target”
- Challenges observed:
  - Limited IT visibility
  - Unprotected / unpatched
  - Entry point to the network
  - Common, widespread vulnerabilities
- This is not hypothetical anymore – Devices are being exploited!
  - Pivot point to enter network
  - Invisible to IT security


SC MAGAZINE
FOR IT SECURITY PROFESSIONALS
> SC US
SC UK
Treasury IG says updates would have made IRS breach harder
U.S. Office of Personnel Management suffers major breach
NEWS
PRODUCTS
BLOGS
RESOURCES
VIDEOS
WHITEP
Share this article:

SC Magazine > News > 'MEDJACK' tactic allows cyber criminals to enter healthcare networks undetected

Ashley Carman, Editorial Assistant

Follow @ashleyrcarman

June 04, 2015

'MEDJACK' tactic allows cyber criminals to enter healthcare networks undetected

This year has already been marked by data breaches at multiple major healthcare organizations, including CareFirst BlueCross BlueShield and Anthem. While these providers have pointed to various causes and attacks as the source of their compromises, not yet has it become prominent news that medical organizations' devices might be the true culprit behind many already and soon-to-be-discovered breaches.

TrapX published a report on "medical device hijack," or MEDJACK, which allows attackers to build backdoors into healthcare providers' networks.

A report from TrapX found that a majority of organizations are vulnerable, if not already victim to MEDJACK, or "medical device hijack." Essentially, the company wrote, attackers maneuver though healthcare systems' main networks by initially exploiting outdated and unpatched medical devices, such as an X-ray scanner or blood gas analyzer. They build backdoors into the systems through these internet-connected devices.

http://www.scmagazine.com/trapx-profiles-medjack-threat/article/418811/

MedJack – Medical Device Hijack

TrapX Whitepaper (5/7/15)

- 3 hospitals, 3 different medical devices (blood gas, x-ray, PACS)
- We already knew that devices are:
  - Vulnerable
  - Unpatched / EOL Operating Sys.
  - No security defense
  - No event detection
- New: APT using devices as pivot point for a lateral attack
- Lack of device security:
  - Enabled exploit
  - Kept it undetected
- The whitepaper discusses 3 example exploits, but we don't know how extensive this is!

TRAPX SECURITY

ANATOMY OF AN ATTACK

MEDJACK (Medical Device Hijack)

RESEARCH by TrapX Labs

"We use the term MEDJACK, or medical device hijack, to frame what we see as the attack vector of choice in healthcare. Attackers know that medical devices on the network are the easiest and most vulnerable points of entry. The MEDJACK is designed to rapidly penetrate these devices, establish command and control and then use these as pivot points to hijack and exfiltrate data from across the healthcare institution. " *Moshe Ben Simon, Co-Founder & VP, TrapX Security, General Manager, TrapX Labs*

Authored By: TrapX Labs - A Division of TrapX Security, Inc.

Date: May 7, 2015

http://deceive.trapx.com/AOAMEDJACK_210_Landing_Page.html

Different Stakeholder Objectives

Device Manufacturers

Protect Intellectual Property

- Design Documents and Formularies
- Clinical Trial Data
- Business Strategy, Financials, M&A

Assure Device Cybersecurity

- Regulatory Compliance
- Device Cyber-protection
- Encryption & Data Integrity
- Code Signing, Device Certs

Manage Operations

- Manufacturing Integrity & Availability
- Maintenance & Support Access
- Supply Chain Management

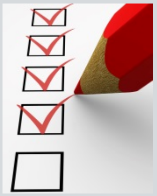
Healthcare Providers

Mitigate Business Risk

- Protect Reputation & Revenue
- Demonstrate Compliance
- Reduce Risk of Fines & Legal Exposure
- Audit preparedness

Assure Patient Safety

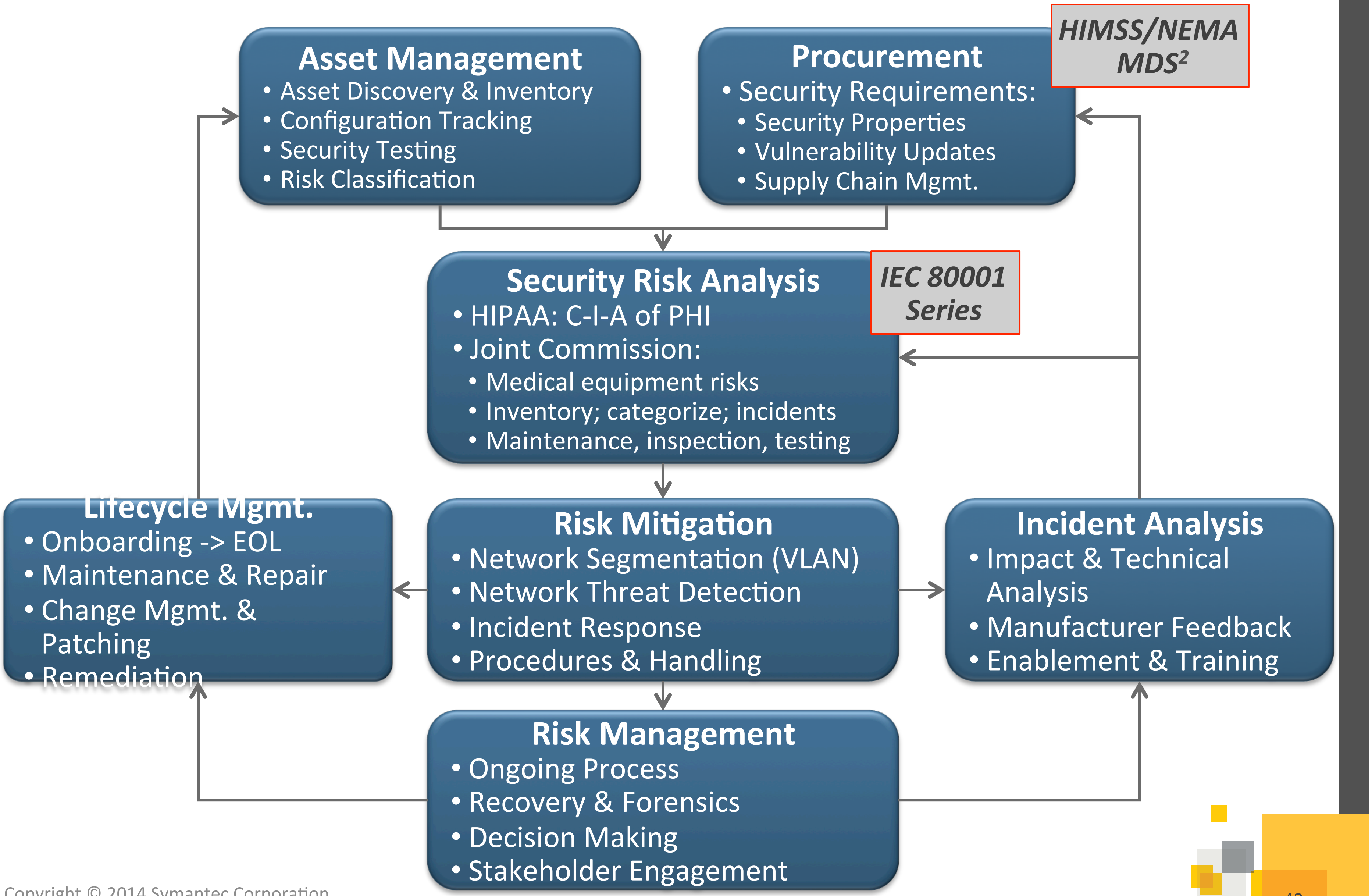
- Operational Reliability
- Reduce Breach Risk
- Prevent Criminal Attack
- Maintenance & Patching



Demonstrate Compliance

- Risk Management
- Confidentiality, Integrity, Availability
- Enterprise Security Posture
- Incident Response

Best Practices Approach – Healthcare Providers



Asset Management
- Asset Discovery & Inventory
- Configuration Tracking
- Security Testing
- Risk Classification

Procurement
- Security Requirements:
  - Security Properties
  - Vulnerability Updates
  - Supply Chain Mgmt.

HIMSS/NEMA MDS²

Security Risk Analysis
- HIPAA: C-I-A of PHI
- Joint Commission:
  - Medical equipment risks
  - Inventory; categorize; incidents
  - Maintenance, inspection, testing

IEC 80001 Series

Lifecycle Mgmt.
- Onboarding -> EOL
- Maintenance & Repair
- Change Mgmt. & Patching
- Remediation

Risk Mitigation
- Network Segmentation (VLAN)
- Network Threat Detection
- Incident Response
- Procedures & Handling

Incident Analysis
- Impact & Technical Analysis
- Manufacturer Feedback
- Enablement & Training

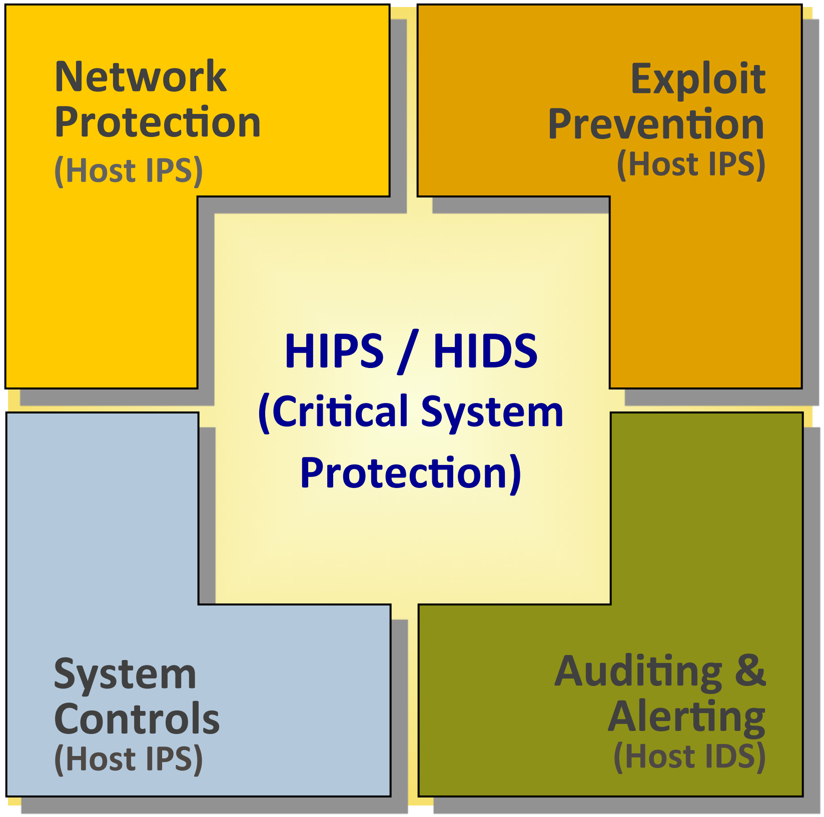
Risk Management
- Ongoing Process
- Recovery & Forensics
- Decision Making
- Stakeholder Engagement

Update-less On-Device Security

(Host Intrusion Prevention/Detection as alternative to Antivirus)

- Close back doors (block ports)
- Limit network connectivity by application
- Restrict traffic flow inbound and outbound

- Restrict apps & O/S behaviors
- Protect systems from buffer overflow
- Intrusion prevention for day-zero attacks
- Application control



Network Protection (Host IPS)

Exploit Prevention (Host IPS)

HIPS / HIDS (Critical System Protection)

System Controls (Host IPS)

Auditing & Alerting (Host IDS)

- Lock down configuration & settings
- Enforce security policy
- De-escalate user privileges
- Prevent removable media use

- Monitor logs and security events
- Consolidate & forward logs for archives and reporting
- Smart event response for quick action

Note alignment with FDA Cybersecurity Guidance

Network Security Gateway

Identify:

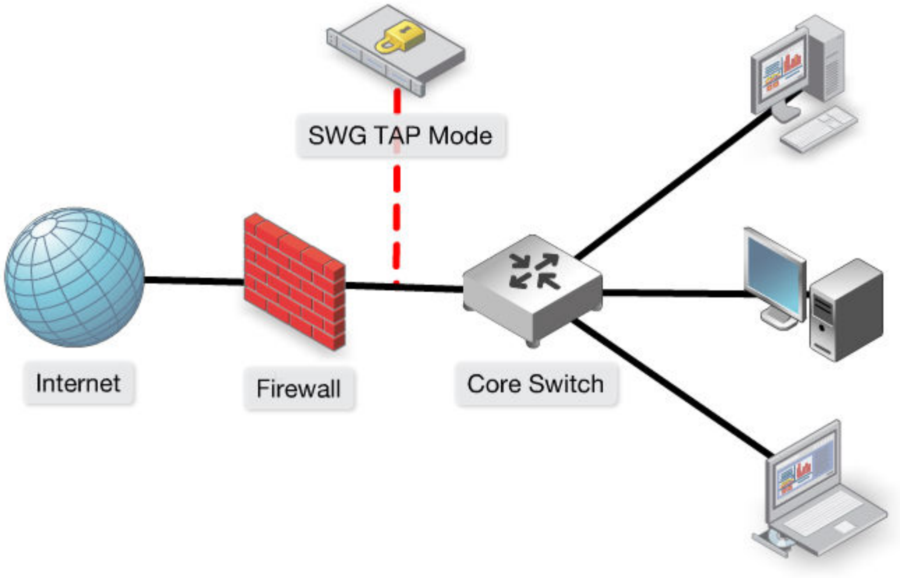
- Compromised systems, e.g. botnets
- Malicious web traffic, e.g. connection to known C&C servers
- Sources of malware re-infection

Prevent:

- External attacks & infiltration
- Data loss

Deliver:

- URL Filtering
- Phone Home Signature Detection
- Behavioral Correlation Algorithm
- Support Remediation
- Logging & Reporting
- Specific Advanced Threat Protection/Detection features (next generation)



Summary: Operational Security to Patient Safety`

Cyber Security

- Device security
- Operational reliability
- “System of systems” risks
- Remediation
- Resilience and recovery

Data Protection

- Privacy and operational objectives:
  - PHI = HIPAA compliance
  - Protect device configuration and settings

Patient Safety

- Risk trade-off:
  - Not all devices are the same
- Complex risk and impact:
  - Patient harm
  - Care delivery
  - National security

Availability – Integrity – Confidentiality

A-I-C priority vs. C-I-A priority in IT

Thank you!

Axel Wirth

axel_wirth@symantec.com
(617) 999 4035

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

Industry Best Practices and Standards

- IEC 80001 Series: “Application of Risk Management for IT-Networks Incorporating Medical Devices”
- MDS^2: “Manufacturer Disclosure Statement for Medical Device Security”
- IEC 62443 Series: “Industrial Automation and Control System Security”
    - Not healthcare, but listed as FDA “recognized standard”
- The Joint Commission – Accreditation Standard EC.02.04.01
    - Manages medical equipment risks.
    - Inventory; categorize risk; incident history.
    - Maintenance, inspection, and testing.
- Veterans Administration “Medical Device Protection Program (MDPP)”
- Industry Organizations:
    - NH-ISAC – National Health Health Information Sharing and Analysis Center
    - MDISS – Medical Device Innovation, Safety and Security Consortium
    - IHE PCD – Patient Care Device Working Group, Medical Equipment Management (MEM)
    - AAMI/UL 2800 – Interoperable Medical Device Interface Safety
    - CE-IT Community (ACCE, AAMI, HIMSS)

IEEE: Building Code for Medical Device Software Security

- Nov. 2014 Workshop
- Released May 2015
- Addressing device manufacturers' secure SW design needs.
- Key Elements:
  - Avoid vulnerabilities
  - Cryptography
  - SW integrity
  - Impede attackers
  - Enable detection
  - Safe degradation
  - Restoration
  - Maintain operations
  - Support privacy

IEEE CYBER SECURITY

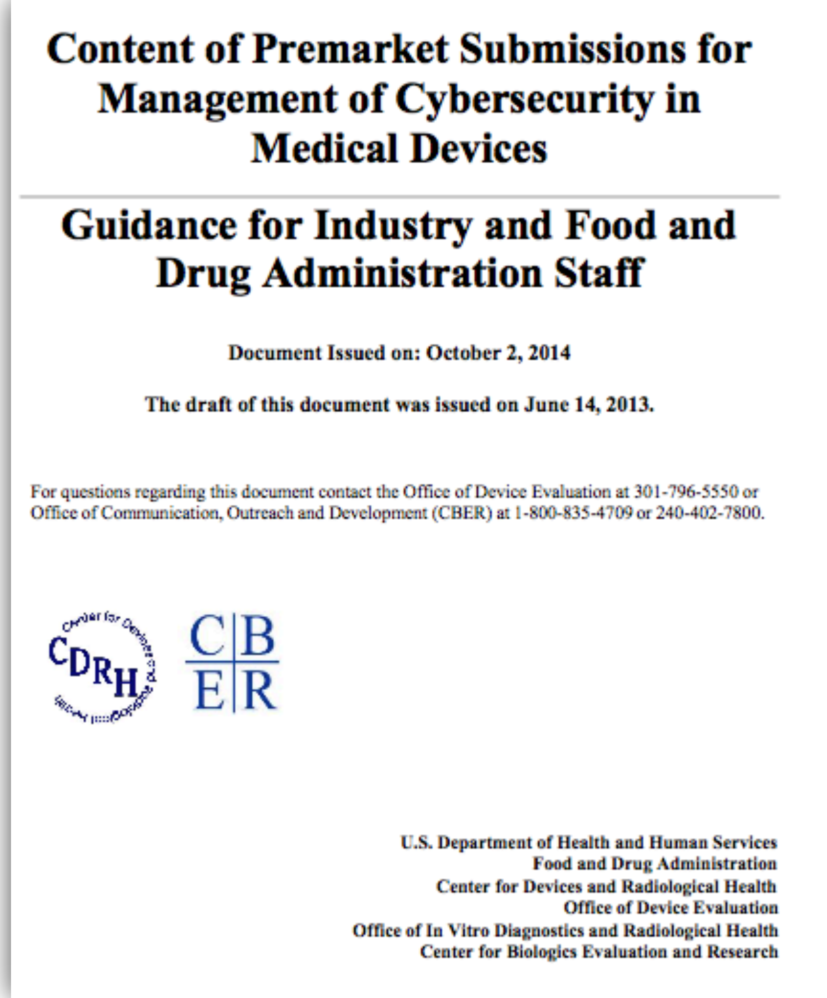
Building Code for Medical Device Software Security

Tom Haigh and Carl Landwehr

IEEE IEEE computer society

READ ON!

http://cybersecurity.ieee.org/images/files/images/pdf/building-code-for-medica-device-software-security.pdf



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document Issued on: October 2, 2014

The draft of this document was issued on June 14, 2013.

For questions regarding this document contact the Office of Device Evaluation at 301-796-5550 or Office of Communication, Outreach and Development (CBER) at 1-800-835-4709 or 240-402-7800.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of Device Evaluation
Office of In Vitro Diagnostics and Radiological Health
Center for Biologics Evaluation and Research

FDA Guidance (Oct. 2014):

- Identify & Protect
  - Limit access to trusted users
  - Ensure trusted content
- Detect, Recover, Respond
  - Detect, recognize, log, and act upon security incidents
  - Actions to be taken
  - Protect critical functionality
  - Recover device configuration
- Cybersecurity documentation
  - Hazard analysis, mitigation, design considerations
  - Traceability matrix (cybersecurity controls to risks)
  - Update and patch management
  - Manufacturing integrity
  - Recommended security controls

http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

IEC 80001 Series

Application of Risk Management for IT-Networks Incorporating Medical DevIces

IEC 80001-1: Roles, responsibilities and activities

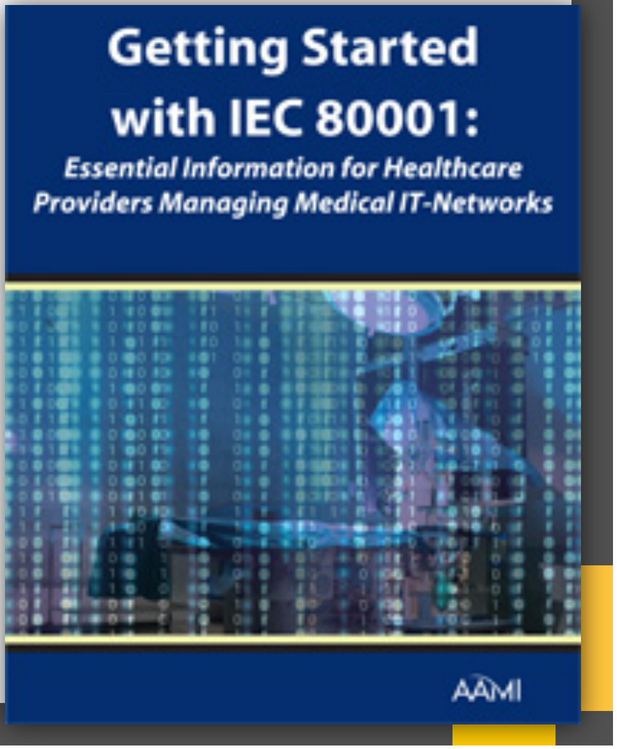
IEC 80001-2-1: Step by step risk management of medical IT-networks – Practical applications and examples

IEC 80001-2-2: Guidance for the disclosure and communication of medical device security needs, risks and controls

IEC 80001-2-3: Guidance for wireless networks

IEC 80001-2-4: General implementation guidance (under development)

IEC 80001-2-5: Guidance for distributed alarm systems (under development)



Getting Started with IEC 80001:

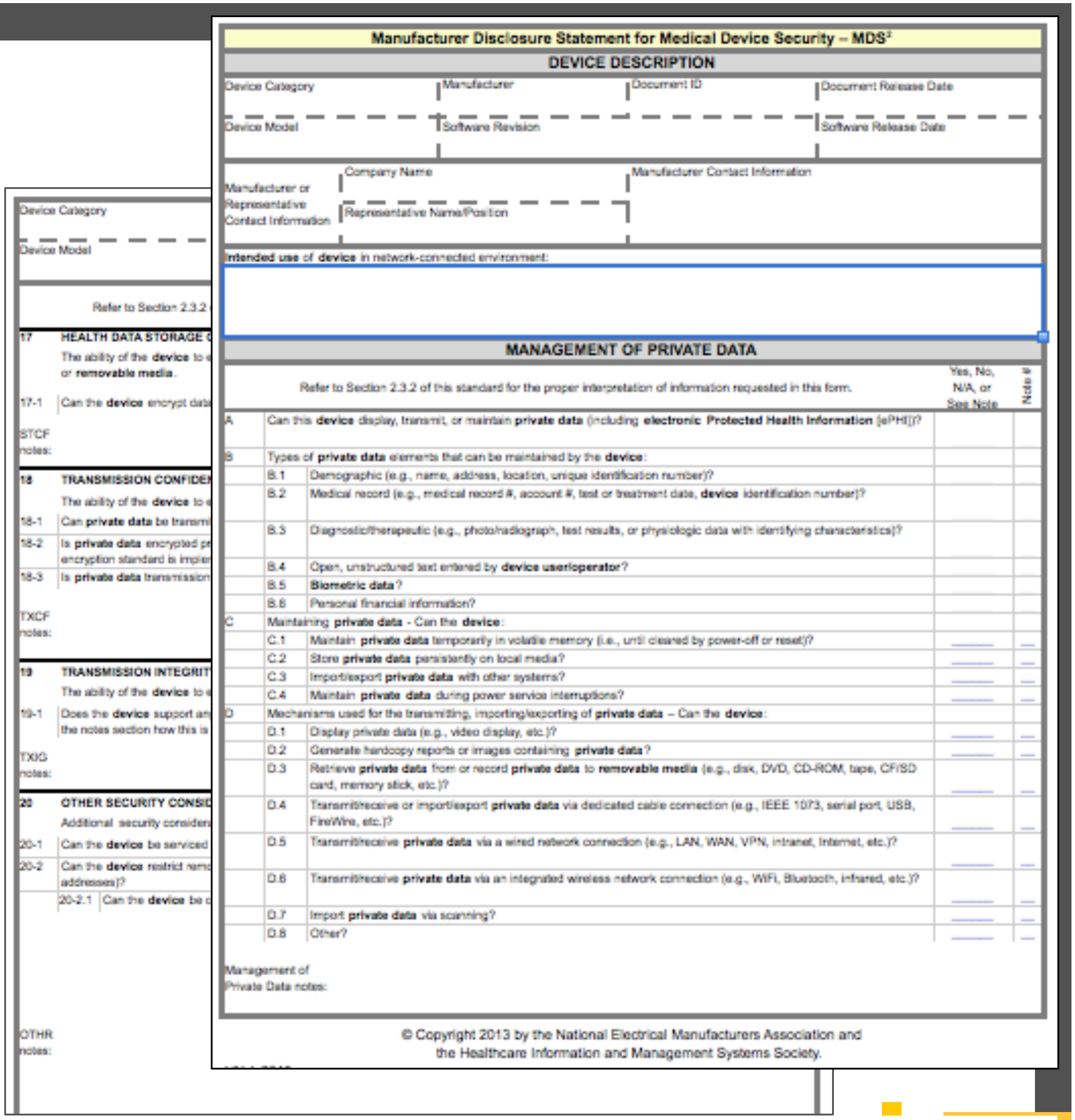
Essential Information for Healthcare Providers Managing Medical IT-Networks

AAMI

Asset & Supply Chain Management

- Manufacturer Disclosure Statement for Medical Devices Security (MDS^2)
- Medical Device Security should be part of the Procurement Process:
  - RFP Language
  - Request NEMA MDS^2
- Developed in cooperation by HIMSS and NEMA

- New version Oct. 2013
- More detailed (2 -> 6 pages)
- Now harmonized with IEC 80001 technical controls



Device Category
Device Model
Refer to Section 2.3.2
17 HEALTH DATA STORAGE C
The ability of the **device** to
or **removable media**.
17-1 Can the **device** encrypt data
STCF notes:
18 TRANSMISSION CONFIDEN
The ability of the **device** to
18-1 Can **private data** be transmi
18-2 Is **private data** encrypted pr
encryption standard is implen
18-3 Is **private data** transmission
TXCF notes:
19 TRANSMISSION INTEGRIT
The ability of the **device** to
19-1 Does the **device** support any
the notes section how this is
TXIG notes:
20 OTHER SECURITY CONSID
Additional security consider
20-1 Can the **device** be serviced
20-2 Can the **device** restrict remo
addresses)?
20-2.1 Can the **device** be
OTHR notes:

Manufacturer Disclosure Statement for Medical Device Security – MDS^2

DEVICE DESCRIPTION

Device Category | Manufacturer | Document ID | Document Release Date
Device Model | Software Revision | Software Release Date

Manufacturer or Representative Contact Information | Company Name | Representative Name/Position | Manufacturer Contact Information

Intended use of **device** in network-connected environment:

MANAGEMENT OF PRIVATE DATA

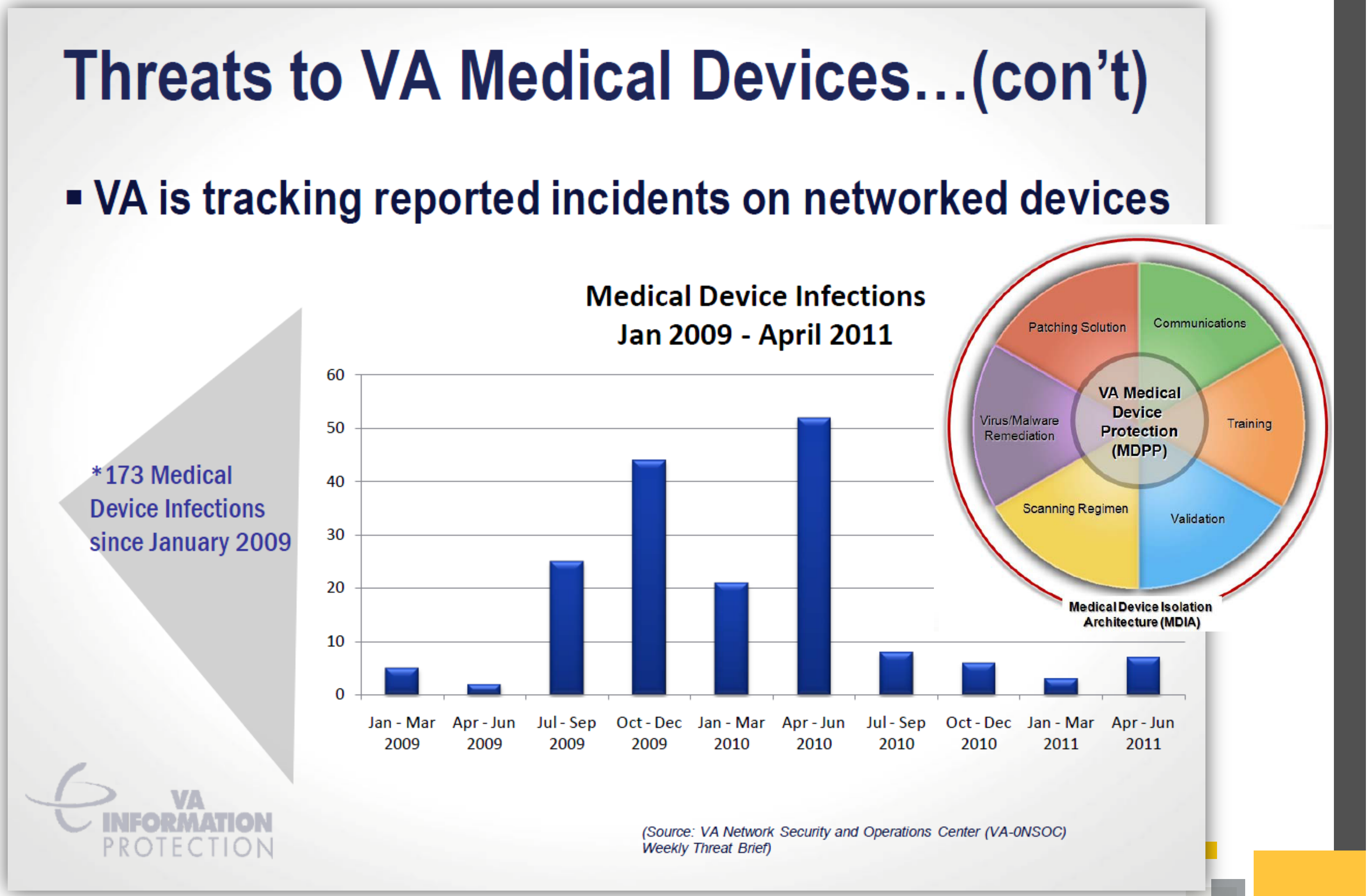
		Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #
A		Can this **device** display, transmit, or maintain **private data** (including **electronic Protected Health Information** [ePHI])?		
B		Types of **private data** elements that can be maintained by the **device**:		
	B.1	Demographic (e.g., name, address, location, unique identification number)?		
	B.2	Medical record (e.g., medical record #, account #, test or treatment date, **device** identification number)?		
	B.3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?		
	B.4	Open, unstructured text entered by **device user/operator**?		
	B.5	**Biometric data**?		
	B.6	Personal financial information?		
C		Maintaining **private data** - Can the **device**:		
	C.1	Maintain **private data** temporarily in volatile memory (i.e., until cleared by power-off or reset)?		
	C.2	Store **private data** persistently on local media?		
	C.3	Import/export **private data** with other systems?		
	C.4	Maintain **private data** during power service interruptions?		
D		Mechanisms used for the transmitting, importing/exporting of **private data** – Can the **device**:		
	D.1	Display private data (e.g., video display, etc.)?		
	D.2	Generate hardcopy reports or images containing **private data**?		
	D.3	Retrieve **private data** from or record **private data** to **removable media** (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?		
	D.4	Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?		
	D.5	Transmit/receive **private data** via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?		
	D.6	Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?		
	D.7	Import **private data** via scanning?		
	D.8	Other?		

Management of Private Data notes:

© Copyright 2013 by the National Electrical Manufacturers Association and
the Healthcare Information and Management Systems Society.

http://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

Segregation (VLAN Network, Access Control)



Threats to VA Medical Devices…(con't)

- VA is tracking reported incidents on networked devices

*173 Medical Device Infections since January 2009

(Source: VA Network Security and Operations Center (VA-0NSOC) Weekly Threat Brief)

From: "VA Medical Device Protection Program (MDPP)", presented at the NIST Health Security Conference, May 11, 2011