Risk Management and Cybersecurity for Devices that Contain Software

Seth D. Carmody, Ph.D.
12th Medical Device Quality Congress
March 18, 2015
Main Points

• Establish a Cybersecurity Risk Management Program
• Information sharing and cyber hygiene are important
• Software updates for cybersecurity do not require pre-market review or recall (there are exceptions)
• FDA will not be prescriptive with risk analyses
• Resources and best practices are prevalent
Definitions

**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.

**Threat** - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

*Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*


NIST SP 800-53; SP 800-53A; SP 800-27; SP 800-60; SP 800-37; CNSSI-4009. Note: The definition is Identical to NIST definition (SP 800-53) with the phrase “or the Nation” redacted.
Definitions

- **Cyber hygiene** is a state of diligent control of a device’s operation, exercised in the use environment and considered ‘best practice’ by the security community. This best practice is comprised of safe and proper configuration of available features, least privilege access to control functions and cybersecurity routine servicing. These practices are undertaken in order to maintain and improve cybersecurity. Additional cyber hygiene controls are identified by FDA in the cybersecurity premarket guidance.

http://www.counciloncybersecurity.org/critical-controls/
Healthcare Sector Challenges – We’re not just worried about manufacturing defects anymore!

1. Lack of Cybersecurity Culture
2. Threats
3. Perceived and Real economics
4. Procurement
5. Multiple and Diverse stakeholders
6. Technical Requirements
Security Is Hard – Don’t confuse effort with results

JP Morgan – Got hacked! Resources: $250 Million dollars/year, 1,000 personnel, set to double

When not if: Anthem, Target, Home Depot, Community Health Systems, Sony Pictures

Why: Mutually assured destruction (nation-states) and Money!

Who: Anyone with a computing device and a motive

• http://files.shareholder.com/downloads/ONE/3430314926x0x742267/e2efaf60-814f-430e-869e-6889ba3ec0ec/2013AR_Chairman-CEO_letter.pdf
Why does FDA care about Cybersecurity?

- Networked medical devices facilitate care
- Networked medical devices introduce new risks

- Centers for Disease Control and Prevention (CDC) estimates of annual patient encounters
  - 35 million hospital discharges
  - 100 million hospital outpatient visits
  - 900 million physician office visits
  - Billions of prescriptions

- Most of these encounters likely include a networked medical device
Presidential Policy Directive 8 (PPD-8): National Preparedness Post-Katrina: “federal departments and agencies to work with the whole community to develop a national preparedness goal and a series of frameworks and plans related to reaching specified goals.”

PPD-21: Critical Infrastructure Security and Resilience

Executive Order 13636: Improving Critical Infrastructure Cybersecurity a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure


<table>
<thead>
<tr>
<th>Chemical</th>
<th>Commercial Facilities</th>
<th>Communications</th>
<th>Critical Manufacturing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dams</td>
<td>Defense Industrial Base</td>
<td>Emergency Services</td>
<td>Energy</td>
</tr>
<tr>
<td>Financial Services</td>
<td>Food and Agriculture</td>
<td>Gov’t Facilities</td>
<td>Healthcare and Public Health</td>
</tr>
<tr>
<td>IT</td>
<td>Nuclear</td>
<td>Transportation</td>
<td>Water/Wastewater</td>
</tr>
</tbody>
</table>

Secretary of Homeland Security Implements these directives.
Demonstrated Exploits

• VA Cath Lab temporary closure (1/10) due to malware infecting computers used during interventional cardiac procedures

• “Hacking” of implantable insulin pump, defibrillator

• Security researchers present CDRH with cyber vulnerabilities of medical devices
FDA Goals

- Meet our mission: safe and effective devices
- Raise cyber-security awareness
- Promote safety and security by design by clear regulatory expectation
- Promote proactive vulnerability management
- Minimize reactive approaches
Regulatory Challenges – Secure design starts with a good Process

- Changing the device engages your established resources
  - Software updates for cybersecurity do not require pre-market review or recall (there are exceptions)
- Risk management (clinical and device) engages your established resources
- Verification/Validation engages your established resources
- Cybersecurity Content for Premarket submissions are presented as a subset of your software documentation (engages your established resources)
What FDA Expects

• FDA expects that manufacturers include cybersecurity risk management program activities as part of their existing quality systems, as required by 21 CFR 820.30(g) and complaint handling, internal audit and corrective action requirements of 21 CFR 820.100, to appropriately address all identified vulnerabilities and exploits.
What is the scope of Risk?

- The Homeland Scenario (worst-case): a person’s life is sustained either continuously and or periodically by a medical device (i.e. there are no mitigation(s) of risk)

- What is the likely scenario of a medical device hack?
  - Collateral damage (i.e. unintended), maybe one device, maybe whole hospital. Control cyber hygiene then the homeland scenario

- A networked device is a device under constant threat
  - Do not rely on compensating controls (user implemented control in the use environment (e.g. firewall))
Cybersecurity Risk Management Program

Step 1: Have one (adopt a Cybersecurity culture)

• Premarket
  – 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 and of a vulnerability being exploited;
  – Determination of risk levels and suitable mitigation strategies;
  – Assessment of residual risk and risk acceptance criteria.

• Post Market
  – Engage in post market surveillance and Information Sharing and Analysis Organizations (ISAOs)
  – Assess the device impact and clinical impact of vulnerabilities and exploits
  – Address the risk; actions taken should be commensurate with the risk
  – Disseminate, Incorporate and Iterate
Cybersecurity Risk Management Program
Step 2: Produce objective evidence, show us

• Premarket Evidence
  – Device design features that mitigate cybersecurity risk
  – Subset of software documentation (Premarket Submissions for Software contained in medical devices
    • Software description, hazards, requirements, design spec, traceability, development environment, Verification and Validation, revision history, and unresolved anomalies (vulnerabilities?)

• Post Market
  – Produce objective evidence that could include policies, procedures, CAPAs, complaints, information sharing, etc.
What documentation is FDA looking for?

- **Hazard analyses**
  - Evaluate both intentional and unintentional cybersecurity risk
    - Provide information on the risk analyzed
  - Controls established to mitigate risk
    - Provide information on the controls put in place
    - Provide information on the appropriateness of the controls to mitigate identified risk
  - Matrix that links cybersecurity controls to the risk being mitigated
  - Summary documentation on
    - Plan to provide validated patches / updates
    - Plan to assure device integrity
  - Cybersecurity control instructions pertaining to use environment
  - A systematic plan for providing patches and updates to operating systems or medical device software.
CDRH/FDA Activities

- **Guidance**
  - Premarket (Final 2014)
  - Post market (*under development*)
  - Wireless Technology (Final 2013)
  - Cybersecurity for Networked Devices with OTS Software (2005)
  - Interoperability (*under development*)
  - MDDS (Medical Device Data Systems - Final 2015)
  - MMA (Mobile Medical Applications – Final 2015)

- **Recognized Standards**
  - Cybersecurity (2013)
  - Interoperability (2013)

- **Public Communication**
  - Premarket Guidance webinar (10/29/2014)
  - FDA/DHS workshop (2014)
  - Safety Communication to Stakeholders (2013)
  - Cybersecurity for networked medical devices shared responsibility (2009)

- **Organization**
  - Established CSWG of Subject Matter Experts (2013)
  - Established Cyber Incident Response Team under EMCM (2013)
  - Premarket Rounds – Cybersecurity (11/17/2014)

http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/ucm373213.htm
CDRH/FDA Ongoing Activities

Regulatory clarity
- Premarket expectations
- Post market expectations

Stakeholder collaboration
- Device industry
- Healthcare organization
- Federal partners
- Researchers & experts

Enable a platform for maintaining Cybersecurity Awareness

Post market surveillance
Best Practices and Tools

• Adopt a cybersecurity culture (Start with NIST):
  – Robust Cybersecurity cultures exist across multiple economic sectors including the financial, utility, and defense sectors.
  – Risk mitigation during total product life cycle from conception to obsolescence
  – Information Sharing (with all stakeholders)
  – Identify, Protect, Detect, Response, Recover
  – Integrate and Iterate
  – Hire/contract with, appropriate personnel
  – Security first, implement design features as well as compensating controls
  – Cyber hygiene (configuration, access control, etc.)

http://www.counciloncybersecurity.org/critical-controls/
http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/ucm373213.htm
### Cyber Security Construct

**Identify** - Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

**Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

**Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

**Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

**Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Cybersecurity Relationship to 14971

Figure E.1 — Pictorial representation of the relationship of hazard, sequence of events, hazardous situation and harm

New partnership with Department of Homeland Security
- Coordinating incident response with ICS-CERT
- Participating in EO13636-PPD21 Integrated Task Force WGs
- DHS-led Cyber-Physical Functional Exercise (Cracked Domain) planners and players

Enhanced communication & partnering with HHS
- Integrated Task Force (ITF)
- HHS/Critical Infrastructure Protection
- Cyber Threat Analysis Center (CTAC)

Strengthen collaboration with NIST through standards and Cybersecurity Framework Working Group

New collaboration with National Health Information Sharing and Analysis Center (NH-ISAC)

Engaging proactively with diverse stakeholders
- Outreach/education of hospital, healthcare & medical device community (users and industry)
Main Points

• Establish a Cybersecurity Risk Management Program
• Information sharing and cyber hygiene are important
• Software updates for cybersecurity do not require pre-market review or recall (there are exceptions)
• FDA will not be prescriptive with risk analyses
• Resources and best practices are prevalent
CDRH Cybersecurity Contacts

– Office of the Center Director (OCD) – Suzanne Schwartz
– Office of In vitro Diagnostics and Radiological Health (OIR) – Seth Carmody
– Office of Device Evaluation (ODE) – Linda Ricci
– Office of Compliance (OC) – John Murray
– Office of Science and Engineering Laboratories (OSEL) – Brian Fitzgerald

• Thank you!
• Questions?