Medical Device Risk Management and Assessment Methods
Session 3, February 19, 2017
Ken Hoyme, Director, Product Security, Boston Scientific
Steve Abrahamson, Sr. Director Product Cyber Security, GE Healthcare
Phil Englert, Sys. Dir. Technology Operations, Catholic Health Initiatives
Speaker Introduction

Ken Hoyme
Director, Product Security
Boston Scientific

Co-chair AAMI Device Security Working Group
Editorial Board – AAMI BI&T
Speaker Introduction

Phil Englert
System Director Technology Operations
Physical Asset Services Group
Catholic Health Initiatives
Speaker Introduction

Steve Abrahamson, BSME, MBA
Sr. Director, Product Cyber Security
GE Healthcare
Conflict of Interest

Ken Hoyme, MSEE
Has no real or apparent conflicts of interest to report.

Phil Englert
Has no real or apparent conflicts of interest to report.

Steve Abrahamson, BSME, MBA
Has no real or apparent conflicts of interest to report.
Agenda

• Evolution of Medical Device Security Risk Management
• Principles of Security Risk Management
• Risk Assessment Tools
• Security Risk Management Throughout the Medical Device Life Cycle
• Questions and Discussion
Learning Objectives

• Describe Risk Management and Assessment Methodologies Across the Life Cycle of a Medical Device
• Explain Risk Management Methodologies to Support Health System Medical Device Network Design
• Demonstrate the MDISS Risk Assessment Platform (MDRAP) and compare with MDS2
• Discuss the Medical Device Procurement Processes and Strategies to Mitigate Risks
An Introduction of How Benefits Were Realized for the Value of Health IT

Medical Device Security Risk Management and Assessment is essential to realizing value of Health IT via Electronic Secure Data.

Value is reduced through risks to data confidentiality, integrity, and availability!
The Evolution of Vulnerability Management in Medical Device Security
FDA Guidance on COTS Software Patching (Jan 2005)
US Information Security and Privacy Advisory Board
March 2011 - Medical Device Cyber Security Panel

MEETING AGENDA
March 2, 3 and 4, 2011
Homewood Suites by Hilton D.C.
1475 Massachusetts Avenue, NW Washington, DC 20005

*Please note: Speakers/times are subject to change without notice.

Wednesday, March 2, 2011
8:30 A.M. – 9:00 A.M. Welcome and Remarks
Dan Chenok, Chairman, ISPA

Thursday, March 3, 2011
8:30 A.M. – 10:00 A.M. VA Medical Devices
Charlie Gephart, VA Director of IT Field Security Operations
Randy Lediard, VA Director of Field Security Services
Lynnette Sherrill, VA Deputy Director Health Information Security Div
Megan Friel, VHA Director of Health Technology Management
Dr. Dale Nordenberg, Medical Device and EHR Innovation, Safety, and Security Consortium
William Elliott, Director, Government Contract Sales, GE Healthcare Representative
Steven Abrahamson, Program Manager, Product Security, CE Healthcare
US Information Security and Privacy Advisory Board
March 2012 – Letter to OMB

March 30, 2012
The Honorable Jeffrey Zients
Acting Director, US Office of Management and Budget
Washington, DC 20502

Dear Mr. Zients,

I am writing to you as the Chair of the Information Security and Privacy Advisory Board (ISPAB or Board). The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-35) as the Computer System Security and Privacy Advisory Board, and amended by Public Law 107-347, the E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) of 2002. One of the statutory objectives of the Board is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

At the Board meeting of February 1-3, 2012, the Board discussed the issue of maintaining security in medical devices that are increasingly operated by software connected to the public Internet, possibly through wireless connections. The Board heard experts discuss how lack of cybersecurity preparedness for millions of software-controlled medical devices puts patients at significant risk of harm. Specifically, software-controlled medical devices are increasingly available through and exposed to cybersecurity risks on the Internet; examples range from desktop computers controlling radiological imaging to custom embedded software found in pacemakers. With increasing connectivity comes greater functional and manageability, but also increased risks of both unintentional interference and malicious tampering via these communication channels.

The Board made the following observations from the panel discussion:

- There is a diffusion of Government responsibility for cybersecurity of medical devices, leading to lack of accountability and oversight.
- Current medical device reporting methods, primarily captured through FDA, are not designed to capture indicators of medical device cybersecurity problems.
- Medical devices used in the home raise additional cybersecurity risks, given the less trustworthy nature of the home environment.
- The Government has multiple ways to address cybersecurity for medical devices, including regulation through FDA, purchasing power through CMS, information distribution through numerous agencies, and education and awareness to home users and medical providers.

Based on the Board’s discussion and findings, we offer a number of recommendations:

1. A single Federal entity (such as FDA) should be assigned responsibility for taking medical device cybersecurity into account during pre-market clearance and approval of devices, and during post-market surveillance of cybersecurity threat indicators at time of use.

2. FDA should collaborate with National Institute of Standards and Technology (NIST) scientists and engineers to research cybersecurity features that could be enabled by default on networked or wireless medical devices in Federal settings. For instance, a
Patients Put at Risk By Computer Viruses
Medical Hacking Poses a Terrifying Threat, in Theory

By Joshua Brustein | August 15, 2013
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 1-800-815-4709 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
HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Though I hadn’t touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system. Next the radio switched to the local hip hop station and began blaring Skee-lo at full volume. I spun the control knob left and hit the power button, to no avail. Then the windshield wipers turned on, and wiper fluid blurred the glass.

As I tried to cope with all this, a picture of the two hackers performing these stunts appeared on the car’s digital display: Charlie Miller and Chris Valasek, wearing their trademark track suits. A nice touch, I thought.
FDA warns of security flaw in Hospira infusion pumps

BOSTON | BY JIM FINKLE

The U.S. Food and Drug Administration on Friday advised hospitals not to use Hospira Inc’s Symbiq infusion system, saying a security vulnerability could allow cyber attackers to take remote control of the system.

The agency issued the advisory some 10 days after the U.S. Department of Homeland Security warned of the vulnerability in the pump, which is used to deliver medications directly into the bloodstream of patients.
THE DOCTOR BILL FROM IDENTITY THIEVES

Unhealthy Rise
Percentage of people saying they were victims of medical identity theft

<table>
<thead>
<tr>
<th>Year</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate</td>
<td>0.2</td>
<td>0.4</td>
<td>0.6</td>
<td>0.8</td>
<td>1.0</td>
</tr>
</tbody>
</table>

*of the 5,000 adult-age U.S. citizens surveyed
Source: Ponemon Institute

THE WALL STREET JOURNAL
FDA Workshop – January 2016

Public Workshop - Moving Forward: Collaborative Approaches to Medical Device Cybersecurity, January 20-21, 2016

The Food and Drug Administration (FDA) is announcing the following public workshop titled “Moving Forward: Collaborative Approaches to Medical Device Cybersecurity.” FDA, in collaboration with the National Health Information Sharing Analysis Center (NH-ISAC), the Department of Health and Human Services and the Department of Homeland Security, seeks to bring together diverse stakeholders to discuss complex challenges in medical device cybersecurity that impact the medical device ecosystem.

The purpose of this workshop was to highlight past collaborative efforts, increase awareness of existing maturity models (i.e. frameworks leveraged for benchmarking an organization’s processes) which are used to evaluate cybersecurity status, standards, and tools in development, and to engage the multi-stakeholder community in focused discussions on unresolved gaps and challenges that have hampered progress in advancing medical device cybersecurity.

- Date, Time and Location
- Federal Register Notice
- Webcast
- Presentations
- Program Book
- Transcripts
Letter from US Senator Barbara Boxer – 05 Feb 2016

Dear Mr. Gorsky, Mr. Flannery, Mr. Spiegel, Mr. Ishrak, and Mr. Shafer:

I am writing to express serious concerns that the cybersecurity vulnerabilities in medical devices are putting the health and safety of patients in California and across the country at risk.

This past spring, an independent security researcher disclosed a vulnerability in certain drug infusion pumps used in hospitals all across the country. The weakness allowed the researcher to infect the device software with malicious code and manipulate the pump’s drug.

"In your response to this letter, please indicate the steps your companies are taking, or plan to take, to address the growing threat of medical device cybersecurity vulnerabilities"
As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up $17,000 In Bitcoin

Across the world, hackers are taking control of networks, locking away files and demanding sizeable ransoms to return data to the rightful owner. This is the ransomware nightmare, one that a Hollywood hospital has been swallowed up by in the last week. The body confirmed it agreed to pay its attackers $17,000 in Bitcoin to return to some kind of normality. Meanwhile, FORBES has learned of a virulent strain of ransomware called Locky that’s infecting at least 90,000 machines a day.

The Hollywood Presbyterian Medical Center’s own nightmare started on 5 February, when staff noticed they could not access the network. It was soon determined hackers had locked up those files and wanted 40 Bitcoins (worth around $17,000) for the decryption key required to unlock the machines. Original reports had put the ransom at 9,000 Bitcoin (worth roughly $3.6 million), but Allen Stefanek, president and CEO of Hollywood
Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5414, Silver Spring, MD 20993-6002; 301-796-4937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-855-854-7599 or 301-403-8019 or secod@fda.hhs.gov.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of the Center Director
Center for Biological Evaluation and Research
Principles of Security Risk Management
Security is Risk Management

Risk = f(\text{asset} \times \text{threats} \times \text{vulnerabilities}) - \text{controls}

Asset = data, device
Threats = malicious actions, malware
Vulnerabilities = exploitable weaknesses in design
Controls = security safeguards to block exploits

Security Controls
- Access
- Authentication
- Accountability/audit
- Media protection
- Others

A simple network model for risk assessment:

Trigger:
- Threat actor with malicious intent

Event:
- Actor gains network access to device

Consequence:
- Actor accesses patient records

Control:
- Access controls

Mitigant:
- Limit data stored on device
Medical Device Security Risk Domains

The three key security properties Confidentiality, Integrity, Availability... mapped to the medical device ecosystem for application of risk management processes.
Consider the Asset

- Confidentiality factors
  - PHI / amount of PHI / type of PHI / whose PHI

- Integrity factors
  - Care criticality / patient safety

- Availability factors
  - Care criticality / business criticality

- Also consider
  - Data flows (content, technology, mapping, boundaries)
Consider the Threats

- Threat actor motivation relative to asset
  - Threat actor capabilities
  - Observed incidents
Consider the Vulnerabilities

• Coding practices

• Software BOM and support (internal, third party)

• Assurance testing / remediation

• Software Updates / Patches
Consider the Controls

- Security controls implemented
- Effectiveness of implementation
- Policies applied / configurability
Re-frame the Risk Function:
Risk = f(asset, threats, vulnerabilities) – controls
becomes
Residual Risk = Inherent Risk – Remediated Risk

Security by Design: Risk-based Controls
AAMI TIR57

- Addresses security risk management in the context of 14971.
- Creates clear linkages between the consideration of safety and security.
- Recognized by the FDA and referenced in their recent postmarket guidance.
Risk Assessment Tools:
MDS2
MDRAP

(Pre-procurement, Post-procurement)
Manufacturer Disclosure Statement for Medical Device Security – MDS²

**DEVICE DESCRIPTION**

<table>
<thead>
<tr>
<th>Device Category</th>
<th>Manufacturer</th>
<th>Document ID</th>
<th>Document Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDS²: Security</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Company Information**

<table>
<thead>
<tr>
<th>Manufacturer Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
</tr>
</tbody>
</table>

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

**MANAGEMENT OF PRIVATE DATA**

Refer to Section 3.2.2 of the standard for the proper interpretation of information requested in this form. Yes, No, NA or See Note

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can this device display, transmit, or maintain private data (including electronic protected health information (ePHI))?</td>
<td>Types of private data elements that may be maintained by the device</td>
<td>Maintain private data temporarily in volatile memory 3 s, until cleared by power-off or read?</td>
<td>Maintain private data temporarily on local media?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can this device display, transmit, or maintain private data (including electronic protected health information (ePHI))?</td>
<td>Types of private data elements that may be maintained by the device</td>
<td>Maintain private data temporarily in volatile memory 3 s, until cleared by power-off or read?</td>
<td>Maintain private data temporarily on local media?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can this device display, transmit, or maintain private data (including electronic protected health information (ePHI))?</td>
<td>Types of private data elements that may be maintained by the device</td>
<td>Maintain private data temporarily in volatile memory 3 s, until cleared by power-off or read?</td>
<td>Maintain private data temporarily on local media?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can this device display, transmit, or maintain private data (including electronic protected health information (ePHI))?</td>
<td>Types of private data elements that may be maintained by the device</td>
<td>Maintain private data temporarily in volatile memory 3 s, until cleared by power-off or read?</td>
<td>Maintain private data temporarily on local media?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can this device display, transmit, or maintain private data (including electronic protected health information (ePHI))?</td>
<td>Types of private data elements that may be maintained by the device</td>
<td>Maintain private data temporarily in volatile memory 3 s, until cleared by power-off or read?</td>
<td>Maintain private data temporarily on local media?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SECURITY CAPABILITIES**

Refer to Section 3.2.3 of the standard for the proper interpretation of information requested in this form. Yes, No, NA or See Note

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTOMATIC LOGOFF (ALOF)</td>
<td>The device's ability to prevent access by unauthorized users if device is left idle for a period of time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Can this device be configured to forcibly authenticate logon (success or failure) after a pre-determined length of inactivity (e.g., auto-logout)?</td>
<td>Success or failure protected?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.1</td>
<td>Is the length of inactivity before auto-logout measured in seconds?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.2</td>
<td>Can auto-logoff be manually initiated (e.g., via a shutdown key or proximity sensor, etc.) by the user?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUDIT CONTROL (ASC)</td>
<td>The ability to audit activity on the device</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>Can the device record or audit events?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2</td>
<td>Indicate what of the following events are recorded in the audit log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2.1</td>
<td>EXECLOG</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2.2</td>
<td>Logging/monitoring of data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2.3</td>
<td>Creation/modification/deletion of data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2.4</td>
<td>Transmission of data through external (e.g., network) connection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2.5</td>
<td>Remote service activity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2.6</td>
<td>Other events (describe in the notes section)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3</td>
<td>Indicate what information is used to identify individual users recorded in the audit log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3.1</td>
<td>User ID</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3.2</td>
<td>Date/time</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUDIT notes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**AUTHORIZATION (AUTM) | The ability of the device to determine the authorization of users |

| 3.1 | Can the device prevent access to unauthorized users through user management or other mechanism? |
| 3.2 | Can users be assigned different privilege levels within an application based on role (e.g., guest, regular users, power users, administrator, etc.)? |
| 3.3 | Can the device configure or operate under restricted administrative privileges (e.g., access operating system or application via local user or remote access)? |

**AUTH notes**

---

81 total questions
Example: Using MDS2 for Risk Management Input

- **Privacy Risk Applicability**
  - Can this device display, transmit, or maintain private data (including electronic Protected Health Information (ePHI))? 

- **Identity & Access Management**
  - Can the device prevent access to unauthorized users through user login requirements or other mechanism?
  - Can users be assigned different privilege levels within an application based on ‘roles’ (e.g., guests, regular users, power users, admin, etc.)?
  - Does the device support user/operator-specific username(s) and password(s) for at least one user?
  - Does the device support unique user/operator-specific IDs and passwords for multiple users?
  - Can the device be configured to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?
  - Can default passwords be changed at/prior to installation?
  - Are any shared user IDs used in this system?
  - Can the device be configured to enforce creation of user account passwords that meet established complexity rules?

- **System/Data Integrity/Encryption**
  - Does the device ensure the integrity of stored data with implicit or explicit error detection/correction technology?
  - Does the device employ any mechanism (e.g., release-specific hash key, checksums, etc.) to ensure the installed update is mfg-authorized?
  - Can the device encrypt data at rest?
  - Is private data encrypted prior to transmission via a network or removable media?

- **Patching, Security Software, System Hardening, Serviceability**
  - Can relevant OS and device security patches be applied to the device as they become available?
  - Does the device support the use of anti-malware software (or other anti-malware mechanism)? (anti-virus)
  - List the provided for required (separately purchased and/or delivered) operating system(s)?
  - Does the device have external communication capability (e.g., network, modem, etc.)?
  - Are all communication ports which are not required for the intended use of the device closed/disabled?
  - Can the device be serviced remotely?
  - Can the device restrict remote access to/from specified devices or users or network locations (e.g., specific IP addresses)?

- **Audit/Logging**
  - Can the medical device create an audit trail?
  - Login/logout in audit log
  - Display/presentation of data in audit log
  - Creation/modification/deletion of data in audit log
  - Import/export of data from removable media in audit log
  - Receipt/transmission of data from/to external (e.g., network) connection in audit log
  - Remote service activity in audit log
  - User ID recorded in audit log

28 questions
MDRAP - Medical Device Risk Assessment Platform

- Assists healthcare systems and device manufacturers
- Understanding, analyzing and mitigating security risks of medical devices
- [https://mdrap.mdiss.org/Account/Login](https://mdrap.mdiss.org/Account/Login)
### Device Inventory

This is your Device Inventory. You may view/edit any of these by clicking on the title. To add a new Device, click the Add Device button.

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Device Description &amp; Model</th>
<th>In Service Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>10/31/2016</td>
</tr>
</tbody>
</table>
MDS2 Library

The MDRAP MDS2 Library is a publicly available repository of Manufacturer’s Disclosure Statement forms collected and made available by the MDRAP & MDISS User Community.

Search MDS2 Library...

<table>
<thead>
<tr>
<th>Device Description &amp; Model</th>
<th>Software Revision</th>
<th>Release Date</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 2 device</td>
<td>Manufacturer</td>
<td>02/05/2016</td>
<td></td>
</tr>
<tr>
<td>(FRN) Pump, Infusion</td>
<td>System Manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>v3.3.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Assessments

This is a list of your Assessments. You may view/edit any of these by clicking on the title. To add a new Assessment click the add new button to the right.
Create Assessment

To add a new Assessment, first select a Device in your Inventory.

Manufacturer
Device Description & Model
located at: [Redacted]
(CARDIAC CATH LAB)
Manufacturer

Device Description & Model

located at (ANESTHESIA)
Class 2 device
(BSZ) Gas-Machine, Anesthesia

Serial #: [REDACTED]
Asset Tag ID: [REDACTED]
In Service Date: 07/16/2015
Select the Risk Assessment Questionnaire form to use

The MDISS Questionnaire is the recommended default for risk assessment and scoring.

The MDISS Questionnaire risk assessment form is based on the MDS2 Manufacturer’s Disclosure form and includes some additional details. It is designed to be compatible with the MDISS risk scoring analytics model and is the preferred and recommended risk assessment form for use with MDRAP.
MDISS Assessment for

Device Model

43.8% completed

Assessment last updated on 1/6/2017 5:20:49 PM

Malware Detection / Protection

Estimate the Adverse Consequences of the failure of Malware Detection / Protection

- Unauthorized access of Sensitive Data by someone other than the owner or
Malware Detection / Protection

Use the mini-questionnaire below to estimate the Level of Effort to remediate the risk of the failure of Cybersecurity Product Upgrades. (To edit any part of the mini-questionnaire just click on the question row)

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who will do the work to mitigate the security risk?</td>
<td>Manufacturer</td>
</tr>
<tr>
<td>Will the manufacturer need to seek FDA approval for device modifications required for the security mitigation?</td>
<td>Yes</td>
</tr>
<tr>
<td>Does the manufacturer acknowledge &amp; address the risk in a timely and collaborative manner?</td>
<td>No</td>
</tr>
<tr>
<td>MDFSS</td>
<td>MDISS Assessment for</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>43.8%</td>
<td>located in Surgery (In Patient)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CH</th>
<th>Assessment for</th>
<th>MFG</th>
<th>Device Model</th>
<th>Manufacturer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MFG</td>
<td></td>
<td>Device Model</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>located in Surgery (In Patient)</td>
<td>last modified 08/18/2016</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Score</td>
<td>Percentage</td>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------</td>
<td>------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>Management of Private Data</td>
<td>4</td>
<td>100.00%</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Other Questions Affecting Exposure</td>
<td>6</td>
<td>100.00%</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Automatic Logoff</td>
<td>5</td>
<td>100.00%</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Audit Controls</td>
<td>5</td>
<td>100.00%</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Authorization</td>
<td>3</td>
<td>100.00%</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Cyber Security Product Upgrades</td>
<td>7</td>
<td>100.00%</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>LOE</td>
<td>Likelihood</td>
<td>Risk</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----</td>
<td>------------</td>
<td>------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Malware Detection / Protection</td>
<td>6</td>
<td>4.867</td>
<td>4.5</td>
<td>* Device requires Internet Access.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>* Malware must be cleaned by manufacturer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>* Malware notification out of band.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>* No Virus Protection</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>* Periodic scans are insufficient protection.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>* Virus Patterns cannot be updated by device owner.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>* Virus patterns must be manually updated.</td>
</tr>
</tbody>
</table>
Managing Security Risks Throughout the Product Lifecycle
Collaborative Risk Management

Manufacturer
- Design
- Develop
- Sell
- Install
- Service
- Monitor
- Update
- Dispose
- Operate
- RemEDIATE
- Remove

Healthcare Provider
- Feature Needs
- Risk Mgmt
- Connect
Vulnerabilities

A design characteristic that a threat actor can exploit to compromise the device/asset confidentiality, integrity, availability.

Consider:

- Related failure modes and failure impacts
- Deliberate design decision vs. bug
- Actual/observed exploits

- What is the risk?
Another Look at Risk

\[ \text{Risk} = f(\text{Likelihood, Impact}) \]

\[ \text{Risk} = f(\text{assets, threats, vulnerabilities}) - \text{controls} \]

- Asset = data, device
- Threats = malicious actions, malware
- Vulnerabilities = exploitable weaknesses in design
- Controls = security safeguards to block exploits (access controls, authentication, etc.)

\[ \text{Likelihood} = f(\text{threat actor motivation, capability, ease of exploit}) - \text{controls} \]

\[ \text{Impact} = f(\text{threat actor motivation, asset value, type of harm}) - \text{mitigants} \]

Motivation or Intent – what the threat actor seeking to gain:
- Cyber Criminals = $
- Nation States = political/economic/offensive advantage
- Hactivists = cause promotion
- Malicious Actor = desire to cause harm
Progressing from Compliance to Collaboration

Health Delivery Organizations
- Compliance
- Business Risk Management
- Collaborative Solutions

Healthcare Device Manufacturers
- Compliance
- Business Risk Management

#HIMSS17
FDA Postmarket Guidance
Perspective of Health Delivery Org.

- Active participation in an ISAO. Promotes collaborative approach and encourages transparent sharing
- Medical devices, interoperable systems, and legacy devices
- Pre-emptively address cybersecurity vulnerabilities – clear risk analysis elements
- Reiterates ‘routine updates and patches’ including COTS, do not require 806 reporting
- Goal to address vulnerabilities prior to exploit & response timeframes
- Loss of confidential data are not considered “patient harms”
A Summary of How Benefits Were Realized for the Value of Health IT

Medical Device Security Risk Management and Assessment is essential to realizing value of Health IT via Electronic Secure Data.

Evaluate and implement controls to implement device hardening and reducing the vulnerability footprint resulting in more secure data.

Value is reduced through risks to data confidentiality, integrity, and availability!
Questions

Contact us:
• Steve Abrahamson  steven.abrahamson@ge.com
• Ken Hoyme  ken.hoyme@bsci.com
• Phil Englert  philenglert@catholichealth.net