William Hagestad II

THE FUTURE OF CYBER WARFARE IN HEALTHCARE

23-25 JAN.
2018
The EGG
BRUSSELS

The MedTech Forum

brining HealthTech stakeholders together
THE FUTURE OF CYBER WARFARE IN HEALTHCARE
Cybersecurity Engineering

Smiths Medical has an established cyber security engineering team proactively applying both Pre- and post Market Guidance for the cybersecurity of medical devices as encouraged by the Cyber Division of the FDA

Current & Future State:
• Recruit and hired internationally recognized white hat hacker
• Built nationally recognized cyber security engineering program with:
  • No budget, critical thinking, experience and will to succeed;
  • FDA Cyber Directorate requested Smiths Medical leadership:
    • Coordinated Disclosure TTX’s in Minneapolis & McLean, VA
    • Disclosed Responsibly 10 CVEs:
      • Advisory (ICSMA-16-306-01)
      • Smiths Medical CADD-Solis Medication Safety Software Vulnerabilities
      • Advisory (ICSMA-17-250-02) Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump Vulnerabilities (SEP 2017)
• Actively assess medical devices for both clinical and technological cybersecurity cyber threats
Medical Device Cyber Security Maturity

21 MARCH 2016

Reactive

Blocking & Tackling
- Lack of Executive support
- Underfunded
- Understaffed
- Lack of metrics for reporting
- Set up for failure

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

Compliance Driven
- Control-based security approach
- Align to mandatory regulations
  - EU/PII Data protection
  - FFIEC
  - HIPAA
  - ISO 2700x
  - PCI
  - NCUA

2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.

Risk-Based Approach
- Multi-layered security and risk-based approach
- Using behavior analytics and evaluating new technologies frequently
- Linking events across multiple disciplines

13 JANUARY 2018

Proactive

https://krebsonsecurity.com/2015/04/whats-your-security-maturity-level/
History of Cyber Warfare

1982 - First Cyberattack
1998 - Operation Solar Sunrise
1999 - Chinese Data Exfiltration
2001 - Estonian CyberWar
2002 - Storm Worm
2003 - Botnet Attack on eBay
2004 - Pentagon Security Breach
2005 - Ghost Net
2006 - State Bank of Slovakia Hacked
2007 - Anonymous Attacks
2008 - Operation Aurora
2009 - Sony Playstation Breach
2010 - U.S. Banks Attacks
2011 - RSA Hack & NSA Attacks
2012 - U.S. Chamber of Commerce Attacks
2013 - Stuxnet
2014 - U.S. Drone Hack
2015 - Cybersecurity
2016 - War as a Domain
2017 - Operation Infection
2018 - War as a Tool
2019 - Cybersecurity
2020 - War as a Tool
2021 - Cybersecurity
2022 - War as a Tool
2023 - Cybersecurity
September 10, 2015
Alert Number: 1-091015-PSA
Questions regarding this PSA should be directed to your local FBI Field Office.
Local Field Office Locations: www.fbi.gov/contact-us/field

INTERNET OF THINGS POSES OPPORTUNITIES FOR CYBER CRIME

The Internet of Things (IoT) refers to any object or device which connects to the Internet to automatically send and/or receive data. As more businesses and homeowners use web-connected devices to enhance company efficiency or lifestyle conveniences, their connection to the Internet also increases the target space for malicious cyber actors. Similar to other types of computing devices, like computers or smartphones, IoT devices also pose security risks to consumers. The FBI is warning companies and the general public to be aware of IoT vulnerabilities cybercriminals could exploit and offers some tips on mitigating those cyber threats.

What are some IoT devices?

- Automated devices which remotely or automatically adjust lighting or HVAC
- Security systems, such as security alarms or home cameras, including video monitors used in nurseries and daycare settings
- Medical devices, such as wireless heart monitors or insulin dispensers
- Thermostats
- Wearables, such as fitness devices
- Lighting modules which activate or deactivate lights
- Smart appliances, such as smart refrigerators and TVs
- Office equipment, such as printers
- Entertainment devices to control music or television from a mobile device
- Fuel monitoring systems

How do IoT devices connect?

IoT devices connect through computer networks to exchange data with the operator, businesses, manufacturers, and other connected devices, mainly without requiring human interaction.

What are the IoT risks?

Deficient security capabilities and difficulties for patching vulnerabilities in these devices, as well as a lack of consumer security awareness, provide cyber actors with opportunities to exploit these devices. Criminals can use these opportunities to remotely facilitate attacks on other systems, send malicious and spam e-mails, steal personal information, or interfere with physical safety.

Media Alert PSA 1-091015-PSA

Alert
September 10, 2015

INTERNET OF THINGS POSES OPPORTUNITIES FOR CYBER CRIME

The Internet of Things (IoT) refers to any object or device which connects to the Internet to automatically send and/or receive data. As more businesses and homeowners use web-connected devices to enhance company efficiency or lifestyle conveniences, their connection to the Internet also increases the target space for malicious cyber actors. Similar to other types of computing devices, like computers or smartphones, IoT devices also pose security risks to consumers. The FBI is warning companies and the general public to be aware of IoT vulnerabilities cybercriminals could exploit and offers some tips on mitigating those cyber threats.

What are some IoT devices?

- Automated devices which remotely or automatically adjust lighting or HVAC
- Security systems, such as security alarms or home cameras, including video monitors used in nurseries and daycare settings
- Medical devices, such as wireless heart monitors or insulin dispensers
- Thermostats
- Wearables, such as fitness devices
- Lighting modules which activate or deactivate lights
- Smart appliances, such as smart refrigerators and TVs
- Office equipment, such as printers
- Entertainment devices to control music or television from a mobile device
- Fuel monitoring systems

How do IoT devices connect?

IoT devices connect through computer networks to exchange data with the operator, businesses, manufacturers, and other connected devices, mainly without requiring human interaction.

What are the IoT risks?

Deficient security capabilities and difficulties for patching vulnerabilities in these devices, as well as a lack of consumer security awareness, provide cyber actors with opportunities to exploit these devices. Criminals can use these opportunities to remotely facilitate attacks on other systems, send malicious and spam e-mails, steal personal information, or interfere with physical safety.

Media Alert PSA 1-091015-PSA

Alert
September 10, 2015

INTERNET OF THINGS POSES OPPORTUNITIES FOR CYBER CRIME

The Internet of Things (IoT) refers to any object or device which connects to the Internet to automatically send and/or receive data. As more businesses and homeowners use web-connected devices to enhance company efficiency or lifestyle conveniences, their connection to the Internet also increases the target space for malicious cyber actors. Similar to other types of computing devices, like computers or smartphones, IoT devices also pose security risks to consumers. The FBI is warning companies and the general public to be aware of IoT vulnerabilities cybercriminals could exploit and offers some tips on mitigating those cyber threats.

What are some IoT devices?

- Automated devices which remotely or automatically adjust lighting or HVAC
- Security systems, such as security alarms or home cameras, including video monitors used in nurseries and daycare settings
- Medical devices, such as wireless heart monitors or insulin dispensers
- Thermostats
- Wearables, such as fitness devices
- Lighting modules which activate or deactivate lights
- Smart appliances, such as smart refrigerators and TVs
- Office equipment, such as printers
- Entertainment devices to control music or television from a mobile device
- Fuel monitoring systems

How do IoT devices connect?

IoT devices connect through computer networks to exchange data with the operator, businesses, manufacturers, and other connected devices, mainly without requiring human interaction.

What are the IoT risks?

Deficient security capabilities and difficulties for patching vulnerabilities in these devices, as well as a lack of consumer security awareness, provide cyber actors with opportunities to exploit these devices. Criminals can use these opportunities to remotely facilitate attacks on other systems, send malicious and spam e-mails, steal personal information, or interfere with physical safety.
Adversaries in Cyber Space – A Taxonomy

<table>
<thead>
<tr>
<th>Adversary Type</th>
<th>Motive</th>
<th>Targets of Opportunity</th>
<th>Methodologies</th>
<th>Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nation States ~ Peace Time</td>
<td>Economic, Military, National Secrets, Political</td>
<td>Commercial Enterprises, Intelligence, National Defense, Governments, National</td>
<td>Military &amp; Intel specific cyber doctrine, hacktivists</td>
<td>Asymmetric use of the cyber domain and kinetic</td>
</tr>
<tr>
<td>Nation States ~ War Time</td>
<td>Economic, Military, Political</td>
<td>Commercial Enterprises, Intelligence, National Defense, Governments, National Infrastructure</td>
<td>Military &amp; Intel specific cyber doctrine, hacktivists</td>
<td>Symmetric use of the cyber domain including kinetic</td>
</tr>
<tr>
<td>Cyber Terrorists &amp; Insurgents</td>
<td>Political</td>
<td>Infrastructure, Extortion and Political Processes</td>
<td>Combination of advanced persistent threats (APT)</td>
<td>A developing and emerging threat since 2012</td>
</tr>
<tr>
<td>Criminal Organizations – RBN</td>
<td>Financial</td>
<td>Intellectual Property Theft, Direct &amp; Indirect pressure, OGA Resources</td>
<td>Use of above with distinct planning</td>
<td>Highly professional, dangerous</td>
</tr>
<tr>
<td>Rogue Organizations – Anonymous, LulzSec</td>
<td>Financial, Military, National Secrets, Political Noteriety</td>
<td>Intellectual Property Theft, Direct &amp; Indirect pressure, OGA Resources</td>
<td>Organic hacking capabilities unsurpassed</td>
<td>Organized yet de-centralized</td>
</tr>
</tbody>
</table>
Worst Case Scenario…..

Boeing airplane hacked by DHS...

What if...

- HVP onboard aircraft connected to vulnerable medical device...
- Nation State Hacker targets HVP...
- Jumps from hacked medical device...
- To Linux-based inflight entertainment system...
- Jumps from easily compromised inflight entertainment system...
- To aircraft flight controls...
- Controls descent of aircraft...
- Augers aircraft into metropolitan CBD...
- Hacked device becomes part of a WMD
What is Security?

How should it apply to Medical Device Manufacturers (MDM)?

How does it apply to Healthcare delivery Organisations (HDO)?
WannaCry
Ransomware Attack
Ransomware

- WannaCry
- Petya/NotPetya

- Apply common cyber security engineering best practices;
- Assume any connected device is vulnerable;
- Become a hard target against skilled adversaries...
- Fundamental situational awareness.....

(1) Initial beacon (skill switch)

(2) Dropper activities
SMBv1 vulnerability attacks
- Set up SMB connection
- Execute SMB protocol
- Query for CGA Vector
- Execute IKEv2
- Steal EAP credentials
- Tackle SMBv1

(3) Diffusion activities
SMBv1 vulnerability attacks
- Set up SMB connection
- Execute SMB protocol
- Query for CGA Vector
- Execute IKEv2
- Steal EAP credentials
- Tackle SMBv1

(4) Ransom activities
Encrypt files
Change filename extensions to WNCRY
Display a ransom Dialog box, etc.

(3)c WannaCry randomly probes IP addresses.
It attacks SMB vulnerabilities.
If it is able to establish a TCP connection.

(3)b WannaCry exploits the SMBv1 vulnerability on operating PCs.

(3) WanteCry probes within the same network.
You became victim of the PETYA RANSOMWARE!

The hard disks of your computer have been encrypted with a military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the xxxxxxx page shown in step 2.

To purchase your key and restore your data, please follow these easy steps:

1. Download the our Browser at http://xxxxxxx.xxx/x.
2. Visit one of the following pages with the our Browser:
   http://xxxxxxxxxxxx.xxx
   http://xxxxxxxxxxxx.xxx
3. Enter your personal decryption code there:
Petya/NotPetya
Active cyber security participation from leadership...

From statement creation to publishing on external website 2 hours – Incredible even with both CEO traveling, no corporate communications staff and yours truly enroute to an FDA event
Overwhelming Guidance's & Standards...
Comparing Medical Device Cybersecurity Requirements:

European Union...Protection of Personal Data

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data...

- General Data Protection Regulation (GDPR)....

After four years of preparation and debate the GDPR was finally approved by the EU Parliament on 14 April 2016. It will enter in force 20 days after its publication in the EU Official Journal and will be directly application in all member states two years after this date. Enforcement date: 25 May 2018 - at which time those organizations in non-compliance will face heavy fines.
### Applicable Directives – for European Medical Industry

- OJ L 169 of 12 July 1993

<table>
<thead>
<tr>
<th>Scope, field of application, definition</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEDDEV 2.1/1 (14 kB) Definitions of &quot;medical devices&quot;, &quot;accessory&quot; and &quot;manufactured April 1994&quot;</td>
<td></td>
</tr>
<tr>
<td>MEDDEV 2.1/2 rev.2 (14 kB) Field of application of directive &quot;active implantable medical devices&quot; April 1994</td>
<td></td>
</tr>
<tr>
<td>MEDDEV 2.1/2.1 (12 kB) Treatment of Computers Used to Program Implantable Pulse Generators February 1998</td>
<td></td>
</tr>
<tr>
<td>MEDDEV 2.1/3 rev.3 (183 kB) Borderline products, drug-delivery products and medical devices incorporating as integral part, an ancillary medicinal substance or an ancillary human blood derivative December 2009</td>
<td></td>
</tr>
<tr>
<td>MEDDEV 2.1/4 (21 kB) Interface with other directives – Medical devices/directive89/336/EEC relating to electromagnetic compatibility and directive 89/686/EEC relating to personal protective equipment March 1994</td>
<td></td>
</tr>
<tr>
<td>MEDDEV 2.1/5 (10 kB) Medical devices with a measuring function June 1998</td>
<td></td>
</tr>
<tr>
<td>MEDDEV 2.1/6 (514 kB) Qualification and Classification of stand alone software July 2016</td>
<td></td>
</tr>
</tbody>
</table>

While there are Euro Commission directives...

Also, ISO’s...

**July 2012** EN ISO 14971:2012, Medical devices — Application of risk management to medical devices

**American Standards...**

**May 2016** TIR5 “Principles for medical device security — Risk management”


2018 © The MedTech Forum. All rights reserved - Reproduction in whole or in part is prohibited.
US Food & Drug Administration – Cyber Division


b) Guidance for Industry Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software issued January 14, 2005

c) Medical Device Development Tools, Draft Guidance, Food and Drug Administration Staff issued 14 November 2013

d) Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, Guidance for Industry and Food and Drug Administration Staff issued October 2, 2014

e) Infusion Pumps Total Product Life Cycle Guidance for Industry and FDA Staff issued December 2, 2014

f) Postmarket Management of Cybersecurity in Medical Devices, Draft Guidance for Industry and Food and Drug Administration Staff issued on January 22, 2016

g) Updated recommendations on submitting a new 510(k) for device modifications August 5, 2016

h) Deciding When to Submit a 510 K for a software change to an existing device issued August 8, 2016


j) **Deciding When to Submit a 510(k) for a Change to an Existing Device, Guidance for Industry and Food and Drug Administration Staff Document issued on October 25, 2017**

k) **Deciding When to Submit a 510(k) for a Software Change to an Existing Device, Guidance for Industry and Food and Drug Administration Staff Document issued on October 25, 2017**
US Food & Drug Administration – Cyber Division

Risk of Patient Harm?

Is the Risk Controlled or Uncontrolled?

YES

UNCONTROLLED

Does the risk meet these criteria?
1. No Adverse Events
2. Remediation within Timeline
3. Active Participant in ISAO

YES

Not Required to Report to the FDA

NO

Must Report to the FDA per 21 CFR 806

Changes are routine updates and patches, device enhancements.
THE FUTURE OF CYBER WARFARE IN HEALTHCARE

- Global environment is very asymmetric & challenging...
- Medical devices considered part of IoT...why is this important?
- IoT considered part of Critical Infrastructure Protection...by EU & many nations

Vulnerable medical devices = IoT...Leading to national security threats ...

2018 © The MedTech Forum. All rights reserved – Reproduction in whole or in part is prohibited.
Healthcare Delivery Cyber Security Leadership Actions

Wireless infusion pump ecosystems, if not secured properly, can possibly contribute to the following HDO cyber risks;

- access by malicious actors
- loss or corruption of enterprise information and patient data and health record
- a breach of protected health information
- loss or disruption of healthcare services via ransomware (e.g.; WannaCry & Petya) or other known common vulnerabilities & exploits (CVE)
- damage to an organization’s reputation, productivity, and bottom-line revenue

Sky is not falling....or has it already fallen....?
## Medical Device Threat Vectors

<table>
<thead>
<tr>
<th>Data</th>
<th>Device</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Data Backup</td>
<td>Insecure Configurations</td>
<td>Insecure Network Configurations</td>
</tr>
<tr>
<td>No Data Integrity</td>
<td>Hardcoded Passwords</td>
<td>Insufficient Firewall Rules</td>
</tr>
<tr>
<td>No Data Validation</td>
<td>No Tamper Detection</td>
<td>Unencrypted Network Communication</td>
</tr>
<tr>
<td>Weak Authentication</td>
<td>Insufficient Patching</td>
<td>Lack of Segmentation</td>
</tr>
<tr>
<td>Weak Authorization</td>
<td>Legacy Operating Systems</td>
<td>Lack of Segregation</td>
</tr>
<tr>
<td>No Anti-Virus Protection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weak/Insufficient Access Control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indefensible BIOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimal to Zero Logging</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
HEALTHCARE ALREADY INVOLVED IN FUTURE CYBER WARFARE

- Strategic & Tactical Challenges...
  - Medical Devices are considered vulnerable IoT devices
  - Delayed threat intel sharing -
  - Medical Device Manufacturers slow to implement cyber security engineering – 2 years NEW in most cases
  - HealthCare data breaches costly cybercrime – Current annual sunk cost $7.3BN Euros
  - HealthCare records very valuable to cyber criminals, more so than personal financial data
  - Ransomware clear and present danger –
    - WannaCry, NotPetya
  - Nation States – Democratic People’s Republic of Korea motivated to infect IoT via ransomware
HEALTHCARE CYBER WARFARE vs MEDICAL DEVICE MANUFACTURERS

PATIENT CARE AND PATIENT SAFETY MUST BE A SHARED PRIORITY OF EFFORT!

- Different expectations force cyber security change...

Your Devices are perfect for Clinical use...
Cyber use....
Well, we need to deliver care not cybersecurity!
our devices could be used for intentional harm...

Our Devices are good enough...
Clinical use not cyber use....
No one would use our devices for intentional harm...

http://www.frost.com/c/10024/home.do
<table>
<thead>
<tr>
<th>Cybersecurity Engineering Tasks</th>
<th>Importance//Relevance</th>
</tr>
</thead>
<tbody>
<tr>
<td>FDA Guidance - Postmarket Management of Cybersecurity in Medical Devices</td>
<td>Begin building continuity of cybersecurity engineering around Smiths-Medical infusion pumps in accordance with FDA Draft Guidance – NOT OPTIONAL</td>
</tr>
<tr>
<td>NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems Revision 1 2012</td>
<td>Medical Infusion Pump Risk &amp; Vulnerability Assessments - Comprehensive self-assessment of our entire medical infusion pump architecture determining known cybersecurity vulnerabilities of medical infusion pump architecture... Through tactical cybersecurity actions identify &amp; understand risks</td>
</tr>
<tr>
<td>NIST SP 800-53 Rev. 5 (DRAFT) Security and Privacy Controls for Information Systems and Organizations</td>
<td>Map NIST Security Controls to Device Design Controls, mitigate known vulnerabilities in order to proactively mitigate ALL cyber risk to patients</td>
</tr>
<tr>
<td>Apply NIST’s Cybersecurity Framework (CSF) Version 1.1 (DRAFT) &amp; NIST Cybersecurity Framework (CSF) Reference Tool</td>
<td>Utilise crosswalk functionality of NIST CSF Ref Tool mapping to cybersecurity engineering standards</td>
</tr>
<tr>
<td>Member of National Health – Information Sharing and Analysis Center (NH-ISAC)</td>
<td>Achieve collaborative situational awareness of cyber security threats directly impacting US healthcare community – actionable cyber intelligence participation</td>
</tr>
<tr>
<td>FDA recommended Vulnerability &amp; Coordinated//Responsible Disclosure Policies</td>
<td>Create proactive public identification and handling capability to identify cyber risks &amp; vulnerabilities to Smiths-Medical infusion pumps</td>
</tr>
<tr>
<td>Participate in NIST National Cyber Center of Excellence (NCCoE) medical infusion pump evaluation program – NIST SPECIAL PUBLICATION 1800-8 Securing Wireless Infusion Pumps In Healthcare Delivery Organizations</td>
<td>Drive &amp; participate in cyber security standards in wireless environments for medical infusion pumps</td>
</tr>
</tbody>
</table>

Review of Smith’s Medical risk assessments using NIST SP 800-57

<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Respond</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recover</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PR.AC</td>
<td>PR.AV</td>
<td>Asset Management</td>
</tr>
<tr>
<td>PR.BE</td>
<td>PR.GV</td>
<td>Business Environment</td>
</tr>
<tr>
<td>PR.BA</td>
<td>PR.RA</td>
<td>Governance</td>
</tr>
<tr>
<td>PR.RM</td>
<td>PR.RM.GV</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>PR.RM.RA</td>
<td>PR.RM.RA.GV</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>PR.DS</td>
<td>PR.DS.GV</td>
<td>Data Security</td>
</tr>
<tr>
<td>PR.IP</td>
<td>PR.IP.GV</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td>PR.MA</td>
<td>PR.MA.GV</td>
<td>Maintenance</td>
</tr>
<tr>
<td>PR.FT</td>
<td>PR.FT.GV</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE.DE</td>
<td>DE.DE.GV</td>
<td>Security Continuation Monitoring</td>
</tr>
<tr>
<td>DE.DP</td>
<td>DE.DP.GV</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS.EP</td>
<td>RS.EP.GV</td>
<td>Response Planning</td>
</tr>
<tr>
<td>RS.CO</td>
<td>RS.CO.GV</td>
<td>Communications</td>
</tr>
<tr>
<td>RS.AN</td>
<td>RS.AN.GV</td>
<td>Analysis</td>
</tr>
<tr>
<td>RS.MM</td>
<td>RS.MM.GV</td>
<td>Mitigation</td>
</tr>
<tr>
<td>RS.IM</td>
<td>RS.IM.GV</td>
<td>Improvements</td>
</tr>
<tr>
<td>BC.RP</td>
<td>BC.RP.GV</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td>BC.CO</td>
<td>BC.CO.GV</td>
<td>Communications</td>
</tr>
<tr>
<td>BC.IM</td>
<td>BC.IM.GV</td>
<td>Improvements</td>
</tr>
</tbody>
</table>
Review of Smith’s Medical risk assessments through NIST SP 800-30...
Strategic & tactical components of our risk management framework

How we conduct risk & vulnerability assessments of medical infusion pumps

a. Identify known Common Vulnerabilities and Exposures (CVE)

b. Categorize CVEs by technology component

c. Identify primary & secondary compensating controls

d. Assign risk evaluation parameters...traditionally the 5 x 5 matrix
   i. Severity (s)
   ii. Probability (p)
   iii. Detection (d)

Calculate Risk Probability Number (RPN) for;
   i. Primary compensating controls – existing designed security
   ii. Secondary compensating controls – future design security

f. Calculate Common Vulnerability Score based upon CVSS version 3.0 (2015)

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
https://www.certsi.es/en/blog/cvss-3-en
Adversary Capability Assessment Reference Tables

(a) CYBER ADVERSARY CAPABILITIES & CHARACTERISTICS
(b) CYBER ADVERSARY INTENT CHARACTERISTICS
(c) CYBER ADVERSARY TARGETING CHARACTERISTICS
(d) RANGE OF EFFECTS FOR NON-ADVERSARIAL THREAT SOURCES

Adversary Threat Events Reference Tables

a) Threat Events (Characterized by Tactics, Techniques/Technology & Procedures/Protocols - TTPs)

b) Description of Adversarial Threat Event

### Categories of Risk Control

<table>
<thead>
<tr>
<th>Number</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Identify</td>
<td>Develop the organizational understanding of risk to systems, assets, data, and capabilities by introducing the business context within the function to support critical functions and the related cybersecurity risk analysis. Understanding the business context, the mission, and support critical functions, and the related cybersecurity risk is essential for business continuity. Examples of outcomes within this function include: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.</td>
</tr>
<tr>
<td>2</td>
<td>Protect</td>
<td>Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The functional design supports the ability to identify and assess the impact of potential cybersecurity events. Examples of outcomes within this function include: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.</td>
</tr>
<tr>
<td>3</td>
<td>Detect</td>
<td>Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect function enables timely detection of cybersecurity events. Examples of outcomes within this function include: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.</td>
</tr>
<tr>
<td>4</td>
<td>Respond</td>
<td>Develop and implement the appropriate activities to take action on identifying potential cybersecurity events. The Respond function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcomes within this function include: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.</td>
</tr>
<tr>
<td>5</td>
<td>Recover</td>
<td>Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities of services that were impacted due to a cybersecurity event. The Recover function supports timely recovery of normal operations to reduce the impact from a cybersecurity event. Examples of outcomes within this function include: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.</td>
</tr>
</tbody>
</table>

### Risk Concepts

- **RISK**: combination of probability of occurrence of harm & severity of harm
- **HAZARD**: potential source of harm
- **HAZARDOUS SITUATION**: circumstance in which people, property, or environment are exposed to one or more hazard(s)
- **HARM**: physical injury or damage to the health of people, or damage to property or environment
- **SEVERITY**: measure of possible consequences of a hazard
- **RISK ANALYSIS**: systematic use of available information to identify hazards & estimate the risk
- **RISK ESTIMATION**: process used to assign values to the probability of occurrence of harm & severity of that harm
- **RISK EVALUATION**: process of comparing estimated risk vs. given risk criteria to determine acceptability of risk
- **RISK ASSESSMENT**: overall process comprising a risk analysis and a risk evaluation
- **RISK CONTROL**: process in which decisions are made and measures implemented by which risks are reduced to, or maintained within, specified levels
- **RESIDUAL RISK**: risk remaining after risk control measures have been taken

---

[ISO 14971: Medical Device Risk Management](https://www.iso.org/standard/63577.html)
Common Vulnerability Resources

Based upon named examples of commonly known vulnerabilities, which includes;

i. Vulnerabilities with exploits
ii. Cross Site Request Forgery
iii. Sql injection
iv. Memory corruption
v. Gain Information
vi. Code Execution
vii. File Inclusion
viii. Cross Site Scripting
ix. HTTP Response
x. DOS Attack
xi. Buffer Overflow
xii. Gain Privilege
xiii. Directory Traversal
xiv. Bypass ‘something’

https://www.cvedetails.com/index.php
Common Vulnerability Resources – US GOV

Overview of Cyber Vulnerabilities

ICS systems are vulnerable to cyber attack from inside and outside the control system network. To understand the vulnerabilities associated with control systems, you must know the types of communications and operations associated with the control system as well as have an understanding of the deviations they allow. This guidance provides a high-level overview of these topics but does not discuss detailed exploits used by attackers to accomplish intrusion.

- Understanding Control System Cyber Vulnerabilities
- Access to the Control System LAN
- Common Network Architectures
- Dial-Up Access to the RTUs
- Vendor Support
- IT Controlled Communication Gear
- Corporate VPNs
- Database Links
- Purity Configured Firewalls
- Power Utility Links
- Discovery of the Process
- Control of the Process
- Sending Commands Directly to the Data Acquisition Equipment
- Exploiting the HMI Screen
- Changing the Database
- Man-in-the-Middle Attack

https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities
https://www.us-cert.gov/related-resources
### Common Vulnerability Resources

**OWASP Top 10 - 2017**

#### OWASP Top 10 – 2013 (Previous) vs OWASP Top 10 – 2017 (New)

<table>
<thead>
<tr>
<th>OWASP Top 10 – 2013 (Previous)</th>
<th>OWASP Top 10 – 2017 (New)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 – Injection</td>
<td>A1 – Injection</td>
</tr>
<tr>
<td>A2 – Broken Authentication and Session Management</td>
<td>A3 – Broken Authentication and Session Management</td>
</tr>
<tr>
<td>A3 – Cross-Site Scripting (XSS)</td>
<td>A3 – Cross-Site Scripting (XSS)</td>
</tr>
<tr>
<td>A4 – Insecure Direct Object References - Merged with A7</td>
<td>A4 – Broken Access Control (Original category In 2003/2005)</td>
</tr>
<tr>
<td>A5 – Security Misconfiguration</td>
<td>A5 – Security Misconfiguration</td>
</tr>
<tr>
<td>A6 – Sensitive Data Exposure</td>
<td>A6 – Sensitive Data Exposure</td>
</tr>
<tr>
<td>A7 – Missing Function Level Access Control – Merged with A4</td>
<td>A7 – Insufficient Attack Protection (NEW)</td>
</tr>
<tr>
<td>A8 – Cross-Site Request Forgery (CSRF)</td>
<td>A8 – Cross-Site Request Forgery (CSRF)</td>
</tr>
<tr>
<td>A9 – Using Components with Known Vulnerabilities</td>
<td>A9 – Using Components with Known Vulnerabilities</td>
</tr>
<tr>
<td>A10 – Unvalidated Redirects and Forwards - Dropped</td>
<td>A10 – Underprotected APIs (NEW)</td>
</tr>
</tbody>
</table>

---

- Preventing Harm Patients – Most Important!
- Deterring, Preventing more Ransomware incidents such WannaCry or Petya/NotPetya
- Designing cyber security into medical devices, not as an afterthought...

Desired Future State...

- Teach, mentor & Encourage smaller manufacturers;
- More active participation by all of Smiths Medical;
- Desire for an FDA Cyber assist visit...
Questions / Feedback?
Thank you.

Bill Hagestad,
Senior Principal Cyber Security Engineering