MEDCON
CONFERENCE
Columbus, OH • April 24-27, 2023
CO-SPONSORED BY THE FDA

Managing Medical Device Cybersecurity Risk in the Healthcare Ecosystem

Fatemeh Razjouyan

Director of Regulatory Policy, International and Global Harmonization

Medtronic

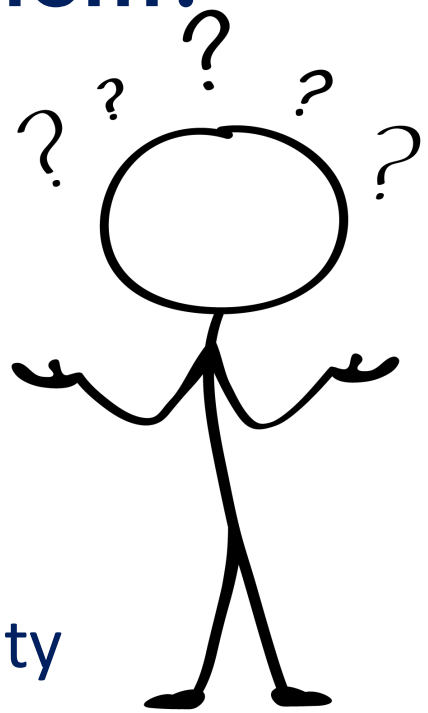
AFDO RAPS HEALTHCARE PRODUCTS COLLABORATIVE

AFDO RAPS

Why are we talking about managing cybersecurity risks?

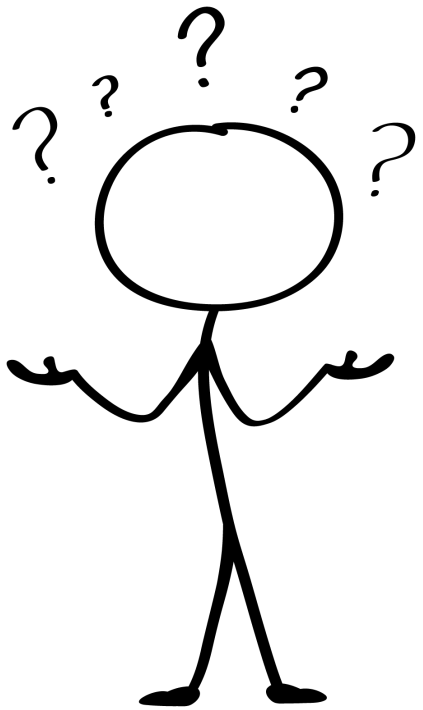
Do you believe your organization is dedicating sufficient attention and resources to addressing cybersecurity risks in the healthcare ecosystem?

1. Yes, we have extensive knowledge and are allocating enough resources
2. Somewhat, we have a basic understanding and are investing moderately in cybersecurity
3. No, our organization lacks knowledge and is not dedicating enough attention or resources to cybersecurity



How would you rate your awareness of the potential cybersecurity risks and patient harm associated with medical devices?

1. Not aware at all
2. Slightly aware
3. Moderately aware
4. Very aware
5. Extremely aware



Agenda

- Cybersecurity and Healthcare – the “why”
- HSCC Joint Security Plan – focused “collaboration”
- FDA thoughts on Cybersecurity – key “opportunities”
- Panel Discussion

Session speakers

Aftin Ross
Senior Special Advisor for Emerging Initiatives
FDA-CDRH

Chris Reed
Director, Regulatory Policy, Digital Health and Product Security
Medtronic

Debra Bruemmer
Senior Manager, Office of Information Security
Mayo Clinic

MEDCON CONFERENCE
COLUMBUS, OH · APRIL 24-27, 2023

Cybersecurity and Healthcare – the "why"

The New York Times

Cyber Attack Suspected in German Woman's Death

Prosecutors believe the woman died from delayed treatment after hackers attacked a hospital's computers. It could be the first fatality from a ransomware attack.

Attack September 10 2020, Article September 18, 2020

The ransomware attack involved servers at the University Hospital Düsseldorf on Sept. 10. Roland Weihrauch/dpa, via ZUMA Press

HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA
Home News Features Interviews
HIPAA and Compliance | Cybersecurity | Cloud | Mobile | Patient Privacy | Data Breaches

UVM Health Continues to Feel Effects of Ransomware Attack

Eight months after a ransomware attack that incurred costs upwards of $63 million, UVM Health continues to experience setbacks and financial losses.

Attack October 2020, Article June 2021

HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA
Home News Features Interviews
HIPAA and Compliance | Cybersecurity | Cloud | Mobile | Patient Privacy | Data Breaches

INTERESTED IN LEARNING MORE ON HEALTHCARE TOP
DISCOVER OUR HEALTHCARE STRATEGIES PODCAST
SUBSCRIBE AND LISTEN NOW

AZ Ransomware Attack Leads to Unrecoverable EHRs, Data Loss

An Arizona medical center will have to rebuild thousands of patient records after a ransomware attack resulted in corrupted EHRs and data loss.

Attack May 2021, Article September 2021

HEALTHCARE INFO SECURITY

Topics | News | Training | Resources | Events | Jobs

TRENDING: A Journey to Mitigate Cyber Risk with Trusted Data • Live Expert Panel | Threat Detection & Incident Re

Fraud Management & Cybercrime , Healthcare , Incident & Breach Response

Hospital Chain's Patient Portals, Other IT Still Offline

CommonSpirit Facilities Still Hampered by Last Week's Cyber Incident

Marianne Kolbasuk McGee (HealthInfoSec) · October 11, 2022

Twitter | Facebook | LinkedIn | Credit Eligible | Get Permission

We are continuing to manage an IT issue that is affecting some of our systems.
Our IT teams are working diligently and we will provide an update as soon as we are able. Our clinics and hospitals remain open and we continue to provide care to patients.
MORE INFORMATION

CHI Health

We apologize for the inconvenience. This site is temporarily unavailable.

Attack Oct 4 2022, Article Oct 12 2022

CHI Health says that its patient portal and other IT systems are still affected by an incident last week involving parent company CommonSpirit.

Change is Slow but it is Happening….

- **Limited financial resources**
  - ~ 70% of healthcare providers have less than 200 beds
  - ~ 80% of medical device vendors have less than 50 employees
- **Medical devices are an "easy" target for cyber attack**
  - Long "shelf life" compared to standard technology
  - Large presence of Windows 7 (unsupported January 2020)
  - Fleet of Windows 10 assets (fully unsupported October 2025)
- **Increased collaboration**
  - Vulnerability disclosures
  - Healthcare industry activities
  - Cross industry activities
  - Global activities
  - Draft legislation

Scope of Healthcare Assets

- Network (e.g., wired, wireless)
- Traditional IT managed assets (e.g., workstations, servers)
- Applications (e.g., traditional and FDA certified applications)
- IoT devices (e.g., card access, refrigerators, infant protection, cameras)
- Medical Devices (e.g., infusion pumps, MRI, medication stations)

Patient Care is delivered through a diverse set of assets …..
Some requiring special handling

Security Approaches, Tools, and Technology

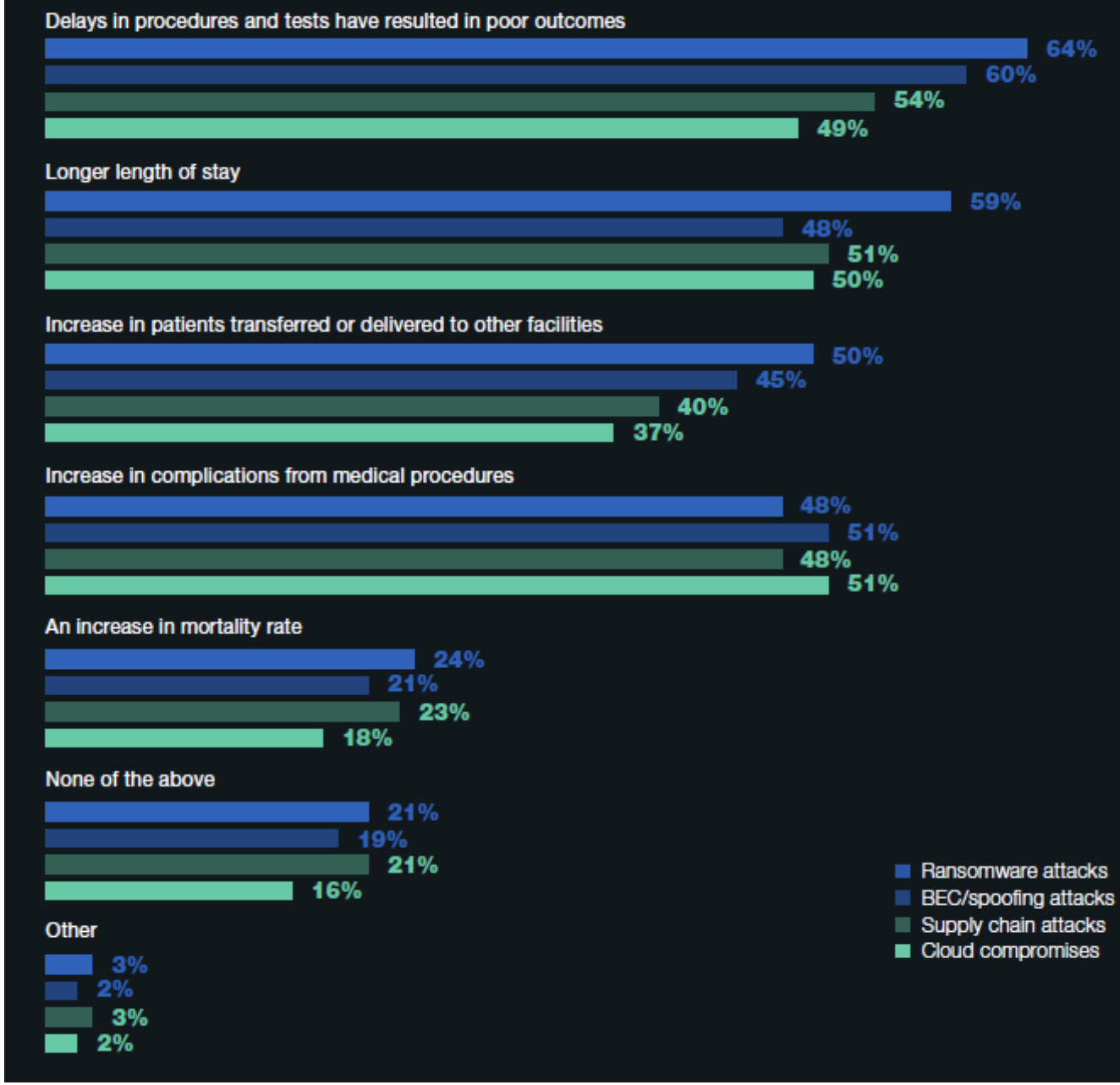
- Network Access Control (NAC)
- Network Segmentation
- Monitoring tools
- Application code scanning
- Vulnerability scanning tools
- Anti-virus, Application Whitelisting
- Patching
- Privileged Access Management tools
- Manage Remote Access tools
- Etc.

Medical Devices and SaMD are not managed like traditional technology

What impact have cyberattacks had on patient care?

(multiple responses allowed)

- Ransomware attacks are more likely to hurt patient safety and care delivery than other cyberattacks.
- 64% stated delayed procedures and tests resulted in poor patient outcomes.
- 50% saw an increase in patients being transferred or delivered to other facilities.
- 24% saw an increase in mortality rate.

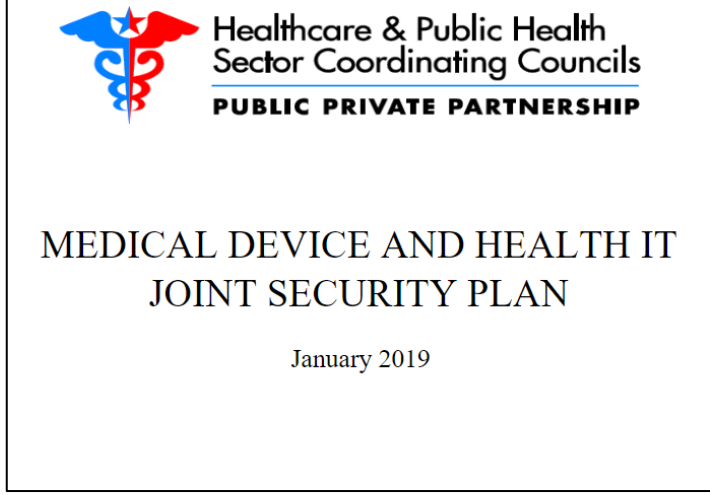


To protect clinical workflows, medical devices need to be secure by design

MEDCON CONFERENCE
COLUMBUS, OH · APRIL 24-27, 2023

HSCC Joint Security Plan – focused "collaboration" and medical device security program best practice

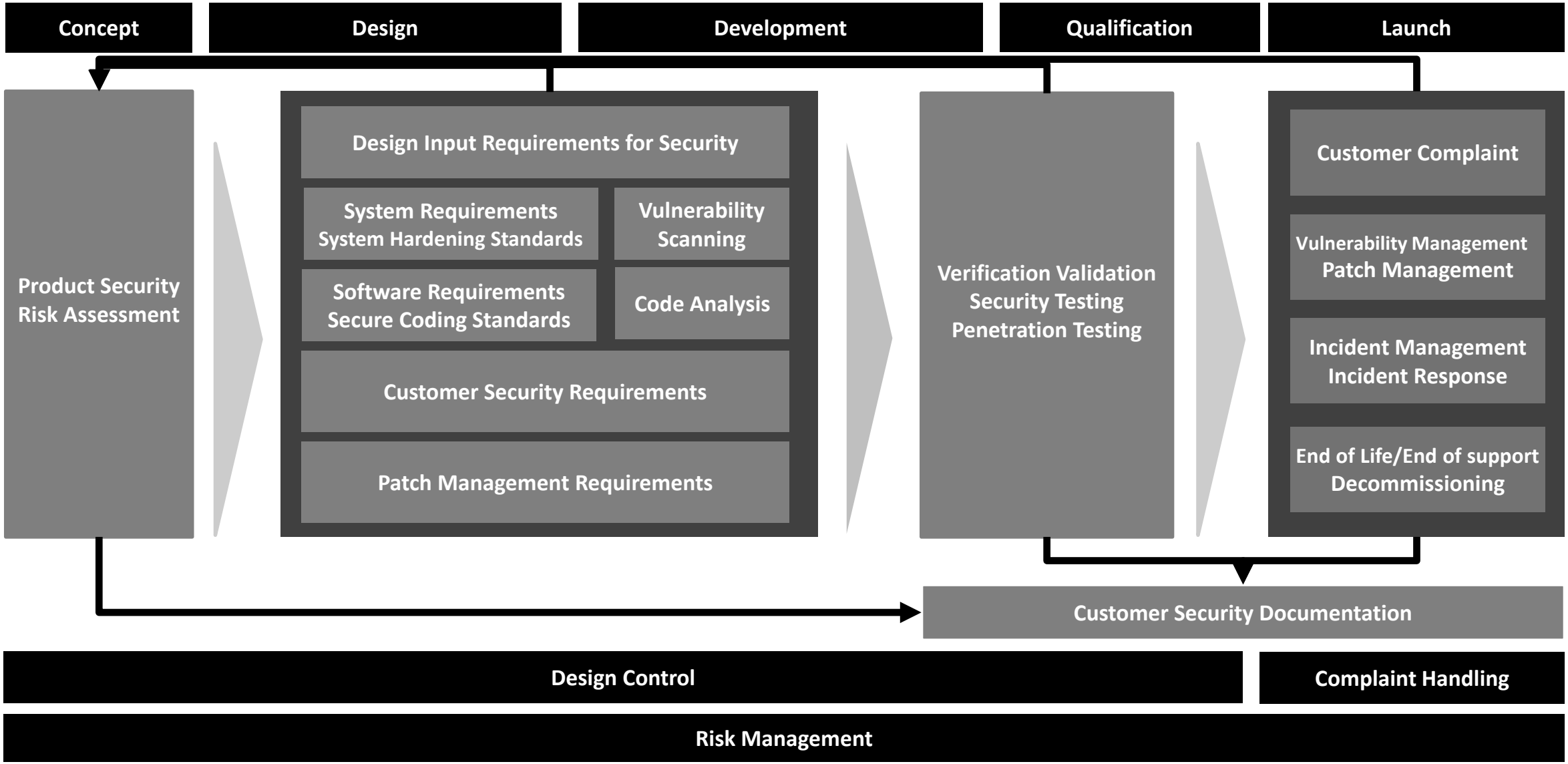
Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

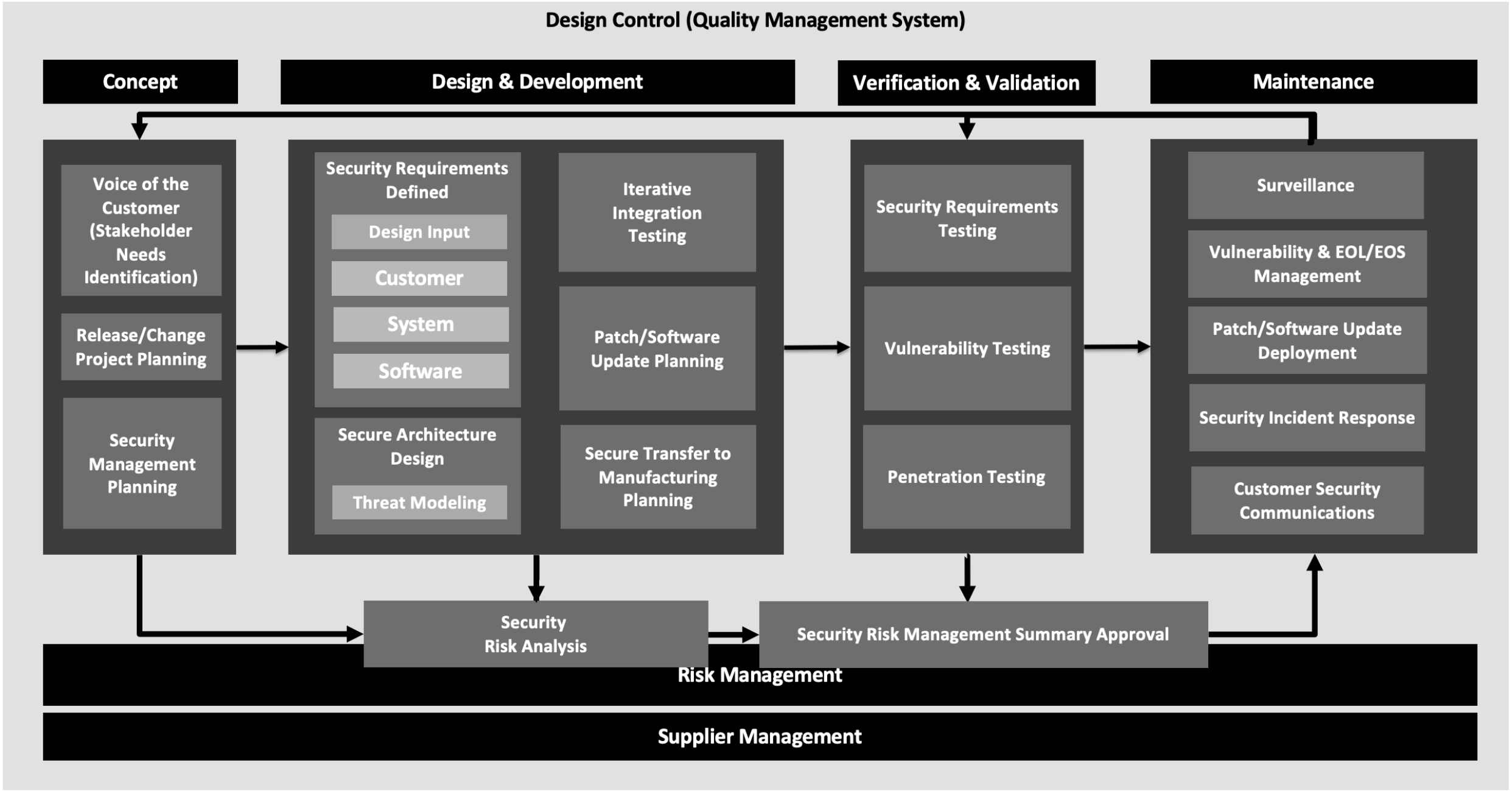


Joint Security Plan (JSP) Background

- In 2015, Congress established Health Care Industry Cybersecurity (HCIC) Task Force in response to the Cybersecurity Act of 2015
  - Identify challenges facing the healthcare industry related to securing and protecting itself against cybersecurity threats
  - Engage cross-industry experts
- In 2017, several MDMs engaged HDOs in a collaborative effort to address the HCIC Task Force Report imperative #2 "Increase the security and resilience of medical devices and health IT"
- In 2019, Healthcare Sector Coordinating Council (HSCC) published the Joint Security Plan (JSP)
  - 48 cross-industry participants
  - Medical Device Manufacturers (MDM)
  - Healthcare Delivery Organizations (HDO)
  - Food & Drug Administration (FDA)
- Ongoing, HSCC serves as the governance body for JSP updates based on learnings and new needs. **An update to the JSP is planned for release in 2023.**

ORIGINAL – FROM JSP 2019




Design Control (Quality Management System)
Concept
Design & Development
Verification & Validation
Maintenance
Voice of the Customer (Stakeholder Needs Identification)
Release/Change Project Planning
Security Management Planning
Security Requirements Defined
Design Input
Customer
System
Software
Secure Architecture Design
Threat Modeling
Iterative Integration Testing
Patch/Software Update Planning
Secure Transfer to Manufacturing Planning
Security Requirements Testing
Vulnerability Testing
Penetration Testing
Surveillance
Vulnerability & EOL/EOS Management
Patch/Software Update Deployment
Security Incident Response
Customer Security Communications
Security Risk Analysis
Security Risk Management Summary Approval
Risk Management
Supplier Management

HSCC Joint Security Plan – Version 2 (Update!)

Verion 2 Focus:

1. Refresh document, not re-write it
2. Add supporting information to benefit smaller organizations
3. Incorporate 2022 MDIC benchmark study learnings
4. Update to include newer relevant document references (i.e., IEC 81001-5-1:2021, HSCC Managing Legacy Technology Security, HSCC Medical Device Vulnerability Communications Toolkit)

***Key Accomplishments*:**

1. Updated design control process flow (draft on previous slide)
2. Draft in process by cross-industry members
3. Incorporated HICUP concepts noting HDO actions to control environment

***Next Steps*:**

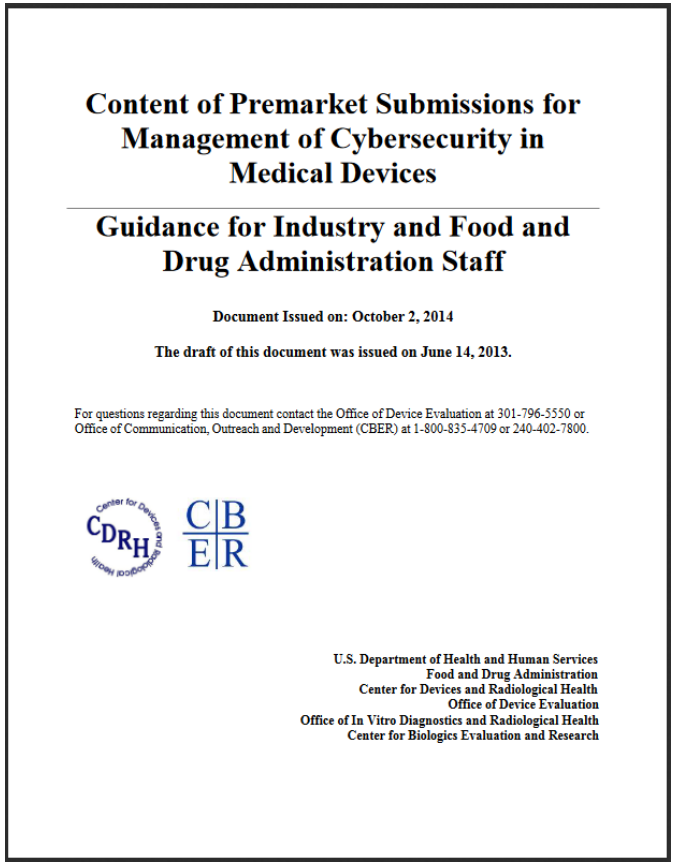
1. Complete draft for HSCC membership review (Q2 2023)
2. Publish JSP version 2 (Q3 2023)

FDA Thoughts on Cybersecurity

Bottom Line Up Front

- Medical device cybersecurity is a patient safety issue
- *"Whole of community/shared responsibility"* approach: Collaboration is key and we need your help
- Security spans across the total product lifecycle
- Impact on critical infrastructure within and across sectors
- Shifting the mindset:
  - Consider scenarios beyond "intended use"
  - Integrate threat modeling
  - Beware of using probabilistic determinations—these can yield a false sense of security
- Foster culture and create incentives that encourage proactive behavior, *especially for information-sharing*
- **Medical device cybersecurity is dynamic and FDA continues to adapt and evolve our approaches as new information becomes available**
- Major strides made AND acceleration necessary

Total Product LIFE CYCLE GUIDANCE APPROACH



Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

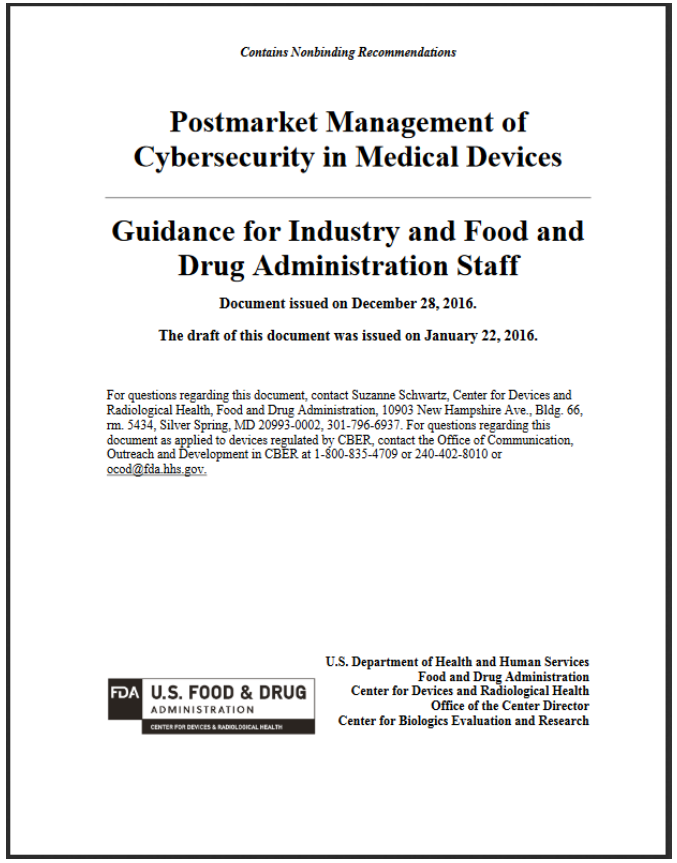
Guidance for Industry and Food and Drug Administration Staff

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



Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices

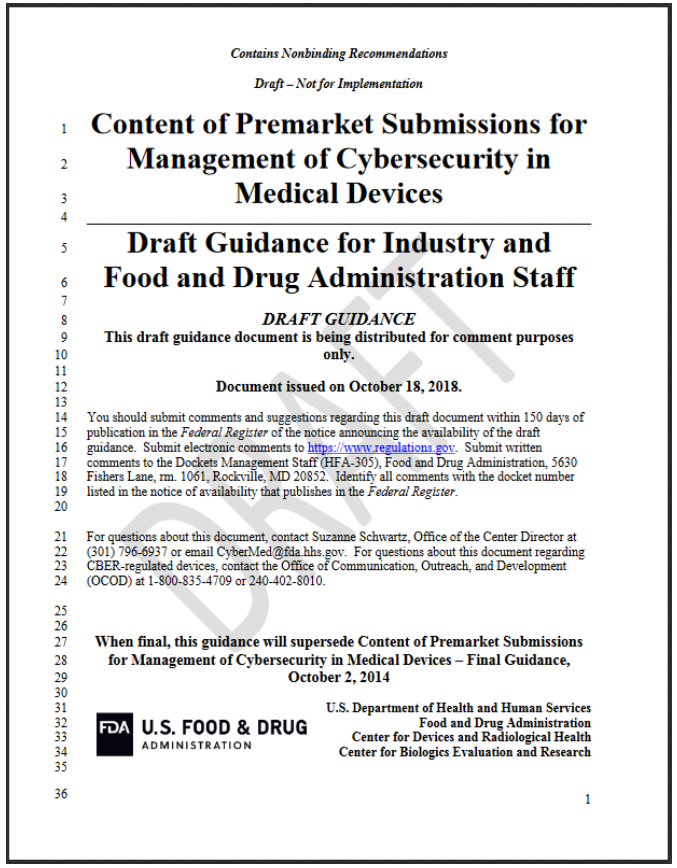
Guidance for Industry and Food and Drug Administration Staff

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. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@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 Biologics Evaluation and Research



Contains Nonbinding Recommendations

Draft – Not for Implementation

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE
This draft guidance document is being distributed for comment purposes only.

Document issued on October 18, 2018.

You should submit comments and suggestions regarding this draft document within 150 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit electronic comments to https://www.regulations.gov. Submit written comments to the Dockets Management Staff (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. Identify all comments with the docket number listed in the notice of availability that publishes in the *Federal Register*.

For questions about this document, contact Suzanne Schwartz, Office of the Center Director at (301) 796-6937 or email CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010.

When final, this guidance will supersede Content of Premarket Submissions for Management of Cybersecurity in Medical Devices – Final Guidance, October 2, 2014

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

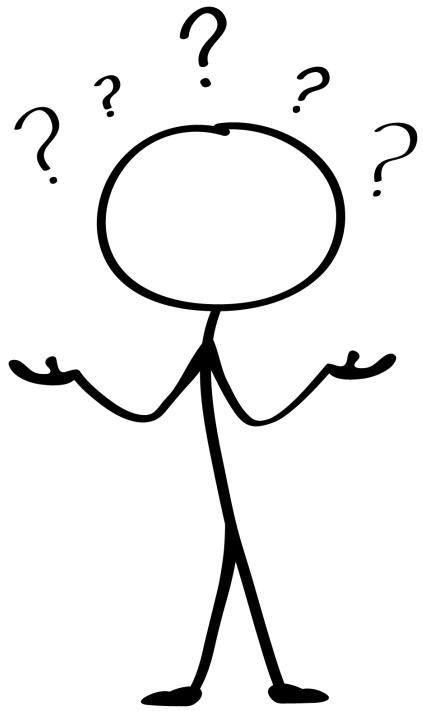
1

Panel Discussion

Are you aware of the new Cybersecurity regulatory authority the FDA has through the Consolidated Appropriations Act, 2023 (Omnibus – Patch Act)?

1. Yes

2. No



Topic#1: Consolidated Appropriations Act, 2023 (a.k.a., Omnibus, Patch Act)

- FDA Final RTA Guidance:

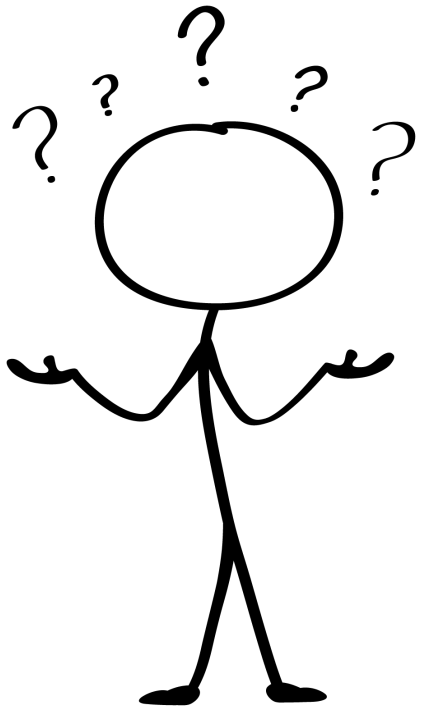
  https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-refuse-accept-policy-cyber-devices-and-related-systems-under-section

- FDA FAQ:

  https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity-medical-devices-frequently-asked-questions-faqs

What do you think is the biggest legacy device challenge?

1. Understanding roles and responsibilities between manufacturer and customers
2. Incentives to eliminate the use of devices deemed "end of support" by the manufacturer

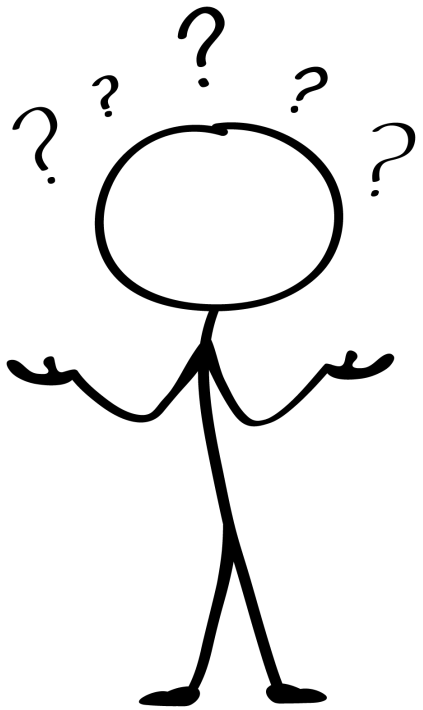


Topic#2: Legacy

- HSCC Managing Legacy Technology Security: https://healthsectorcouncil.org/legacy-tech-security/

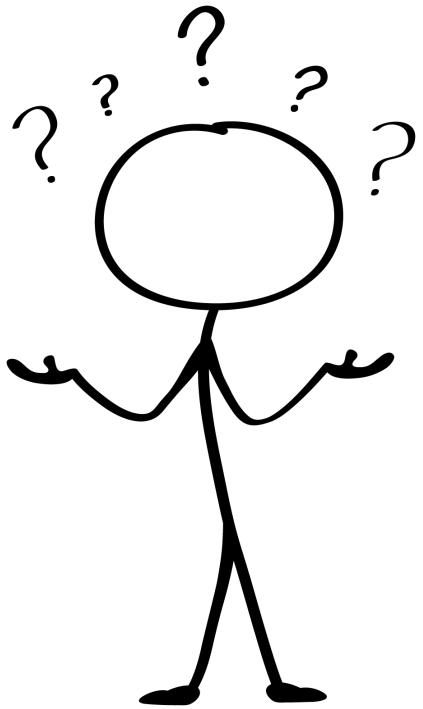
For your products, do you provide regular updates and patches to address cybersecurity vulnerabilities?

1. Yes
2. No
3. Unsure



What do you think your customer's biggest challenges are with respect to vulnerability management?

1. Receiving information about vulnerabilities
2. Applying recommended actions in a timely manner
3. Understanding the recommended actions

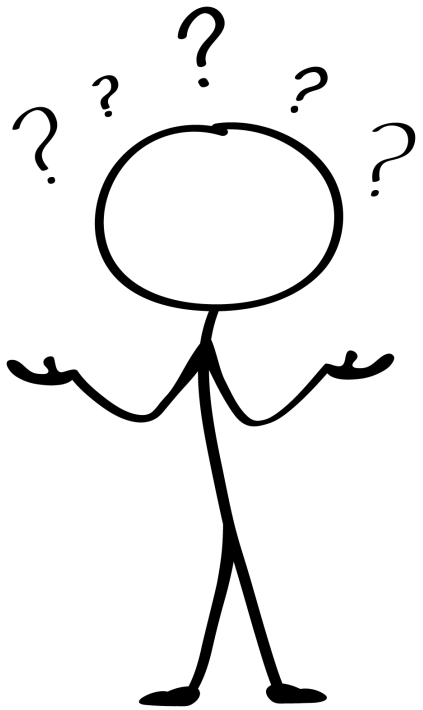


Topic#3: Vulnerability Management

- HSCC Joint Security Plan:
  https://healthsectorcouncil.org/the-joint-security-plan/
  Note: New version planned for Q3 2023 release.
- HSCC MedTech Vulnerability Communicatiosn Toolkit:
  https://healthsectorcouncil.org/wp-content/uploads/2022/04/Health-Industry-MedTech-Vulnerability-Communications-Toolkit.pdf

Are you designing remote access into products that enable:

1. Customers are provided control over the tool/method used to enter their environment
2. Customers have minimal control over the tool/method used to enter their environment



Topic#4: Operational Management

Thank you

Chris Reed, Medtronic, Co-chair HSCC Joint Security Plan Task Group
chris.reed@medtronic.com

Debra Bruemmer, Mayo Clinic, Co-chair HSCC Joint Security Plan Task Group
bruemmer.debra@mayo.edu

Aftin Ross, FDA, Co-chair HSCC Joint Security Plan Task Group
Aftin.Ross@fda.hhs.gov