PRACTICAL
CYBER
BEYOND CYBERSECURITY

ZARACH

MEDMARC
Treated Fairly

MEDMARC'S MITIGATING CYBER RISKS IN DIGITAL MEDICAL DEVICES: AN INTRODUCTION

March 25, 2020

TODAY'S EXPERTS

ELLIOT TURRINI

CYBERSECURITY EXPERT + PRIVACY & CYBER LAWYER

CEO & Founder of Practical Cyber, which specializes in helping medical device manufacturers.

Former federal cybercrime prosecutor, cyberlaw/privacy attorney in private practice & tech company General Counsel.

Cyber risk expert, including ERM and cyber liability insurance.

Editor & Author of Cybercrimes: A Multidisciplinary Analysis.

GERARD NUSSBAUM

STRATEGIC TECHNOLOGY ADVISOR, ATTORNEY

Principal, Zarach Associates.

Bridging Healthcare, Technology, and Law™

Senior strategic advisor to health industry leaders: driving strategy and organizational success.

Editor + Author of *Connected Devices in Healthcare*

1. WHAT’S IN IT FOR YOU?

Mitigate premarket cyber risks arising from design flaws, regulatory approval failures, and clinical trial impediments;

Reduce postmarket cybersecurity costs from vulnerabilities, reporting, and recalls; and

Drive revenue by persuading customers and partners that their devices are cybersecure;

Manage cyber-attacks and PHI data breaches to limit legal liability and regulatory fines.

DEFINITION OF DIGITAL MEDICAL DEVICE

- Per the FDA’s Premarket Cybersecurity guidance, a digital medical device is any device containing software (including firmware) or programmable logic as well as software that is a medical device . . . .” L126-27.
- In layman’s terms, a digital medical device is any device using any form of computer hardware, firmware and/or software.
- Examples to follow

E

SOFTWARE AS MEDICAL DEVICE: KOIOS MEDICAL

E

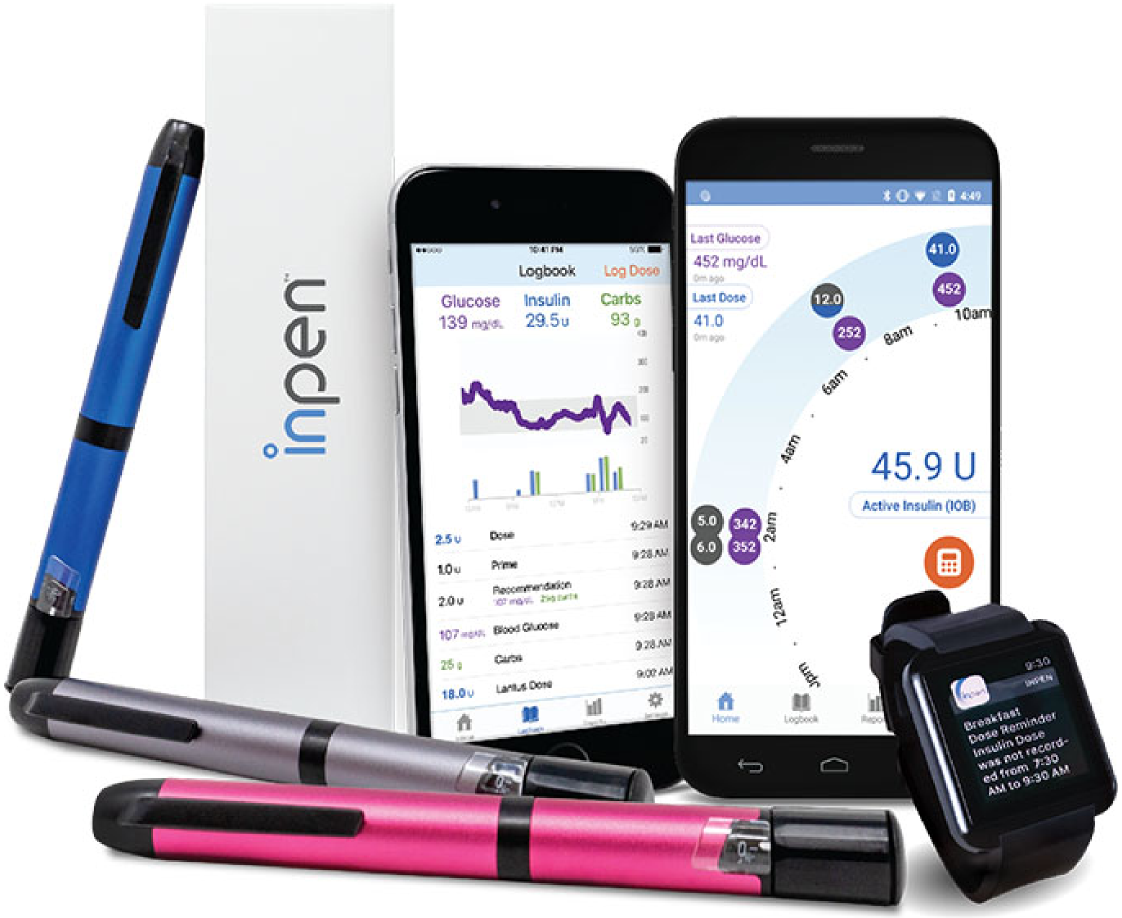
SMART PACEMAKERS: ESSENTIO MRI-SAFE

E

SMART CONTINUOUS GLUCOSE MONITORS

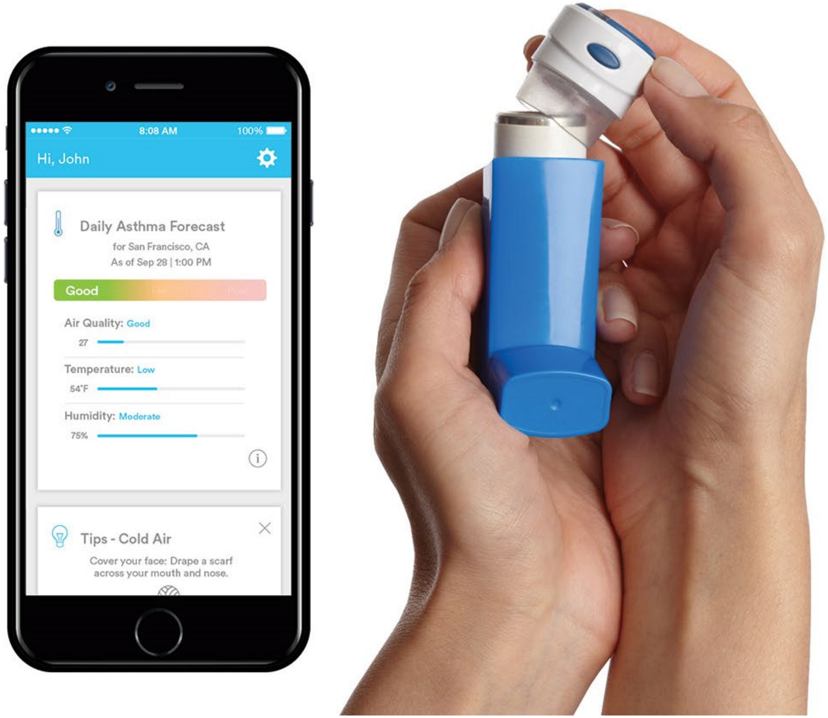
E

SMART INSULIN PENS: INPEN



E

CONNECTED INHALERS: PROPELLER HEALTH



8:08 AM 100%

Hi, John

Daily Asthma Forecast

for San Francisco, CA

As of Sep 28 | 1:00 PM

Good

Air Quality: Good

27

Temperature: Low

54°F

Humidity: Moderate

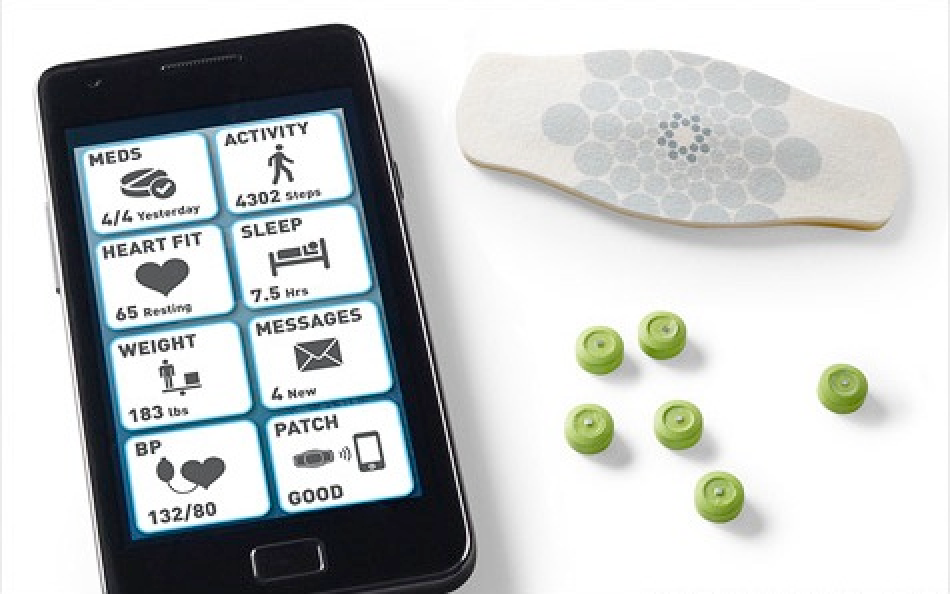
75%

Tips - Cold Air

Cover your face: Drape a scarf across your mouth and nose.

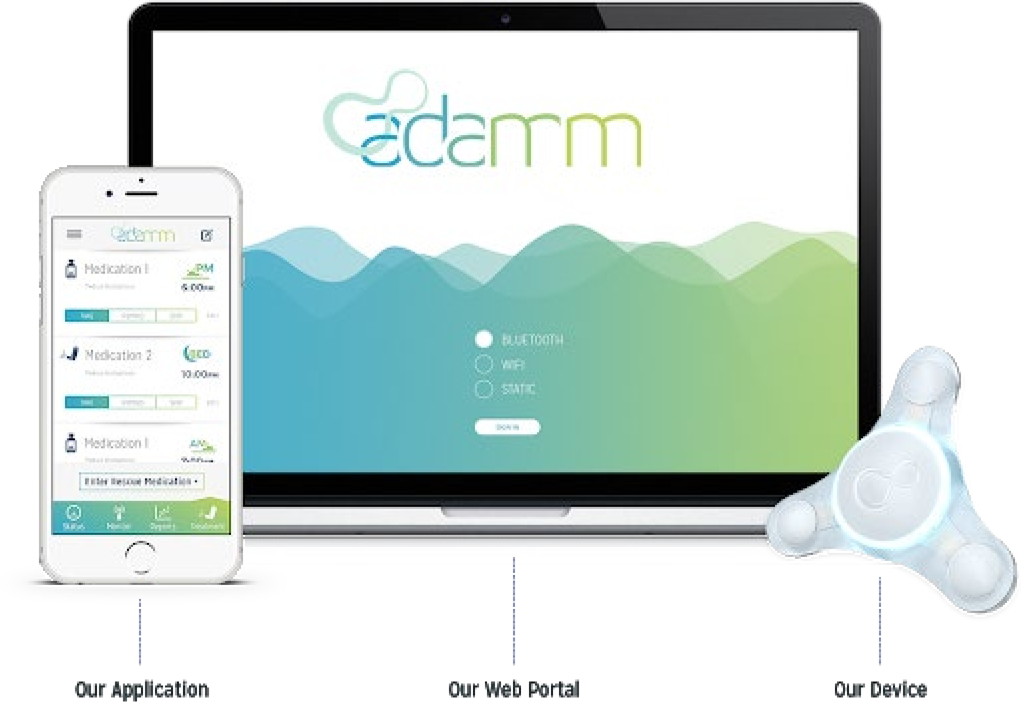
E

INGESTIBLE SENSORS: PROTEUS DIGITAL HEALTH



E

INTELLIGENT ASTHMA MANAGEMENT: ADAMM



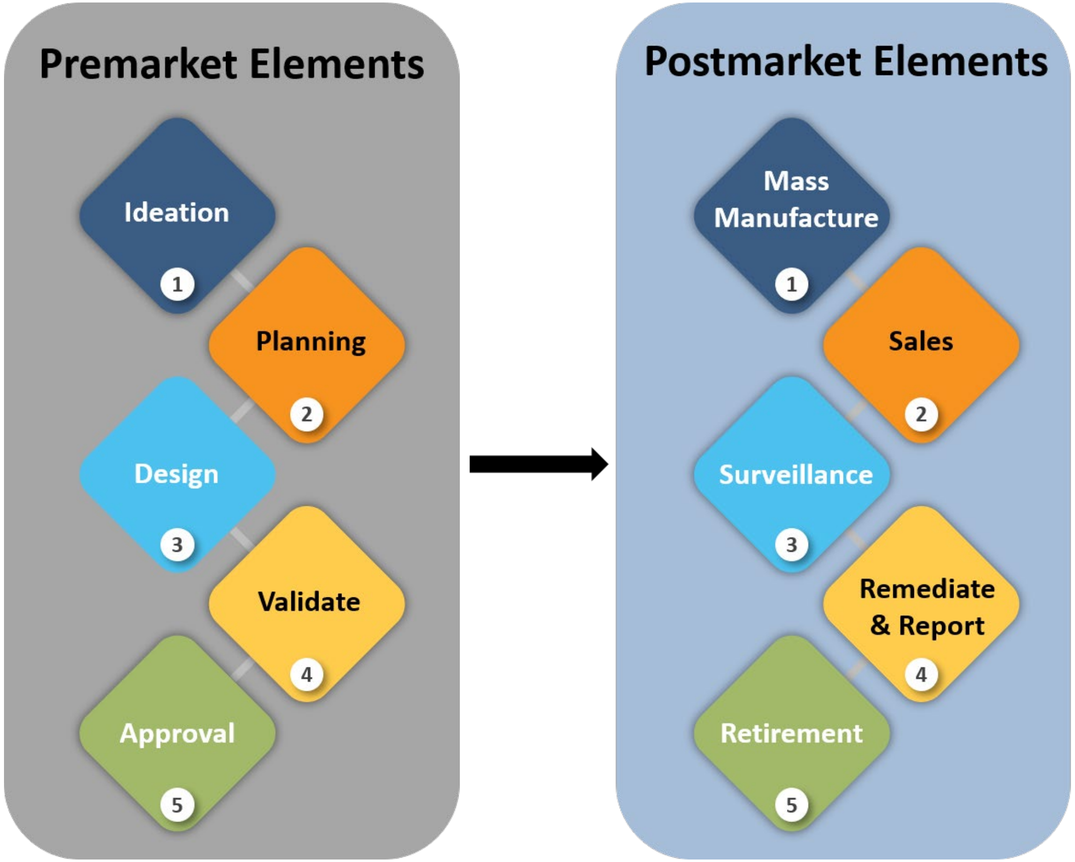
Our Application

Our Web Portal

Our Device

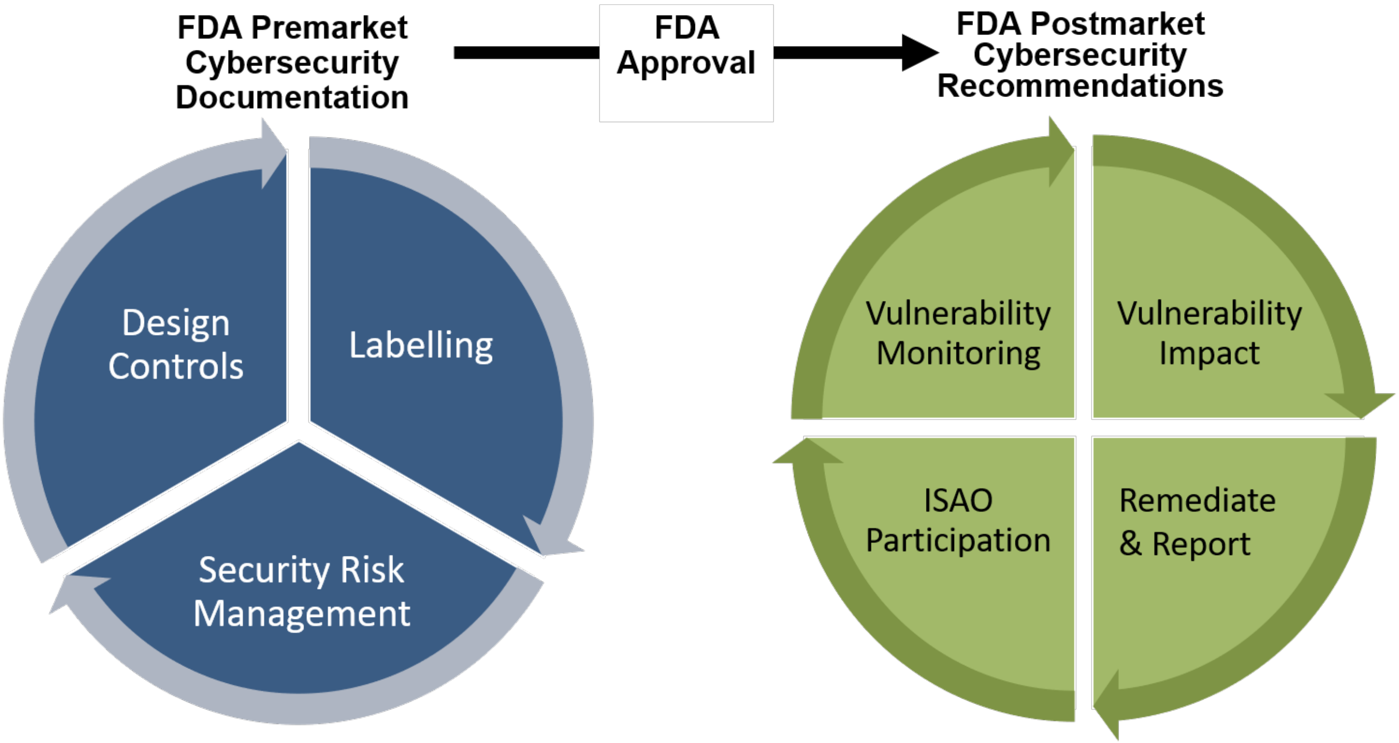
E

QUICK REFRESHER: DEVICE LIFECYLE



G

QUICK REFRESHER: FDA CYBERSECURITY GUIDANCE



E

THE GOALS OF DIGITAL MEDICAL DEVICE CYBERSECURITY

A. Protect Patient Safety & Privacy

B. Deliver Robust Devices Exceeding Expectations

C. Avoid Financial Losses from Device Cyber Risks

C. Avoid Financial Losses from Device Cyber Risks

TOPIC 1: Minimize Premarket Approval Risks & Costs

Regulatory Approval: Many digital medical devices require regulatory approval before commercialization, which require submitting 510(k) and PMA applications, as well as clinical trials.

Actually Not Just Recommendations: While the FDA's Premarket and Postmarket Cybersecurity guidances are recommendations – not regulations – the FDA can delay and/or reject your application because of deficient cybersecurity documentation.

Time Consuming & Expensive: Overcoming the FDA's "cybersecurity" concerns can be time-consuming and expensive

Bottom line: Deficient cybersecurity can substantially increase the costs of bringing a digital medical device to market.

G

C. Avoid Financial Losses from Device Cyber Risks

TOPIC 2: Prepare for Clinical Trial & Sales Risks -- Cybersecurity Expectations

Vigilant Partners & Customer: Clinical trial partners and potential customers vigilantly evaluate the cybersecurity:

- Evaluation can include MDS2 and Hi-Trust Certifications.
- If not prepared, negotiating for clinical trials and sales can be costly & time-consuming.

Bottom line: to minimize these risks –

- ○ Early on understand the types of cybersecurity controls and processes that your clinical trial partners and future customers will require; and
- ○ Build into your device lifecycle the time, money, and expertise needed to produce this proof before it is needed.

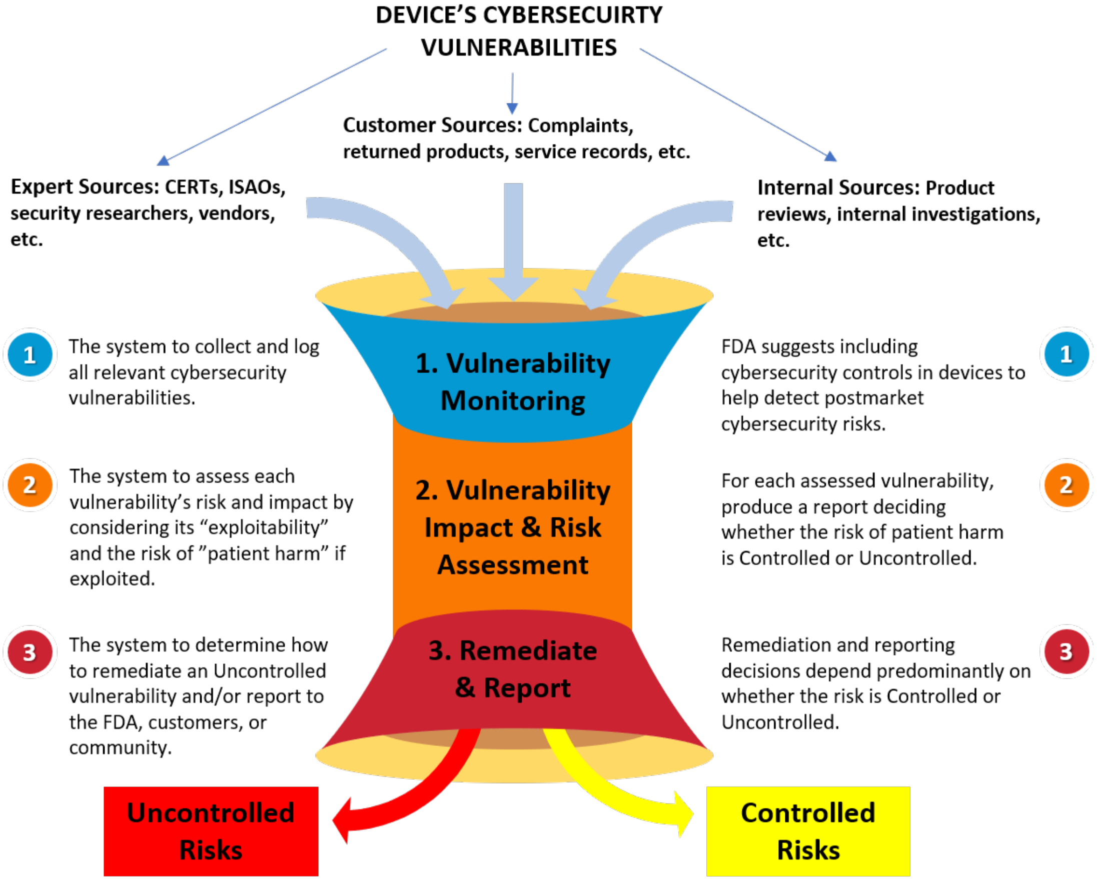
E

C. Avoid Financial Losses from Device Cyber Risks

TOPIC 3: Addressing Unexploited Cybersecurity Vulnerabilities

PART A: Overview

FDA's Postmarket Guidance recommends that digital device manufacturers create three systems to prevent postmarket patient harm



DEVICE'S CYBERSECUIRTY VULNERABILITIES

Expert Sources: CERTs, ISAOs, security researchers, vendors, etc.

Customer Sources: Complaints, returned products, service records, etc.

Internal Sources: Product reviews, internal investigations, etc.

1. Vulnerability Monitoring

1 The system to collect and log all relevant cybersecurity vulnerabilities.

1 FDA suggests including cybersecurity controls in devices to help detect postmarket cybersecurity risks.

2. Vulnerability Impact & Risk Assessment

2 The system to assess each vulnerability's risk and impact by considering its "exploitability" and the risk of "patient harm" if exploited.

2 For each assessed vulnerability, produce a report deciding whether the risk of patient harm is Controlled or Uncontrolled.

3. Remediate & Report

3 The system to determine how to remediate an Uncontrolled vulnerability and/or report to the FDA, customers, or community.

3 Remediation and reporting decisions depend predominantly on whether the risk is Controlled or Uncontrolled.

Uncontrolled Risks

Controlled Risks

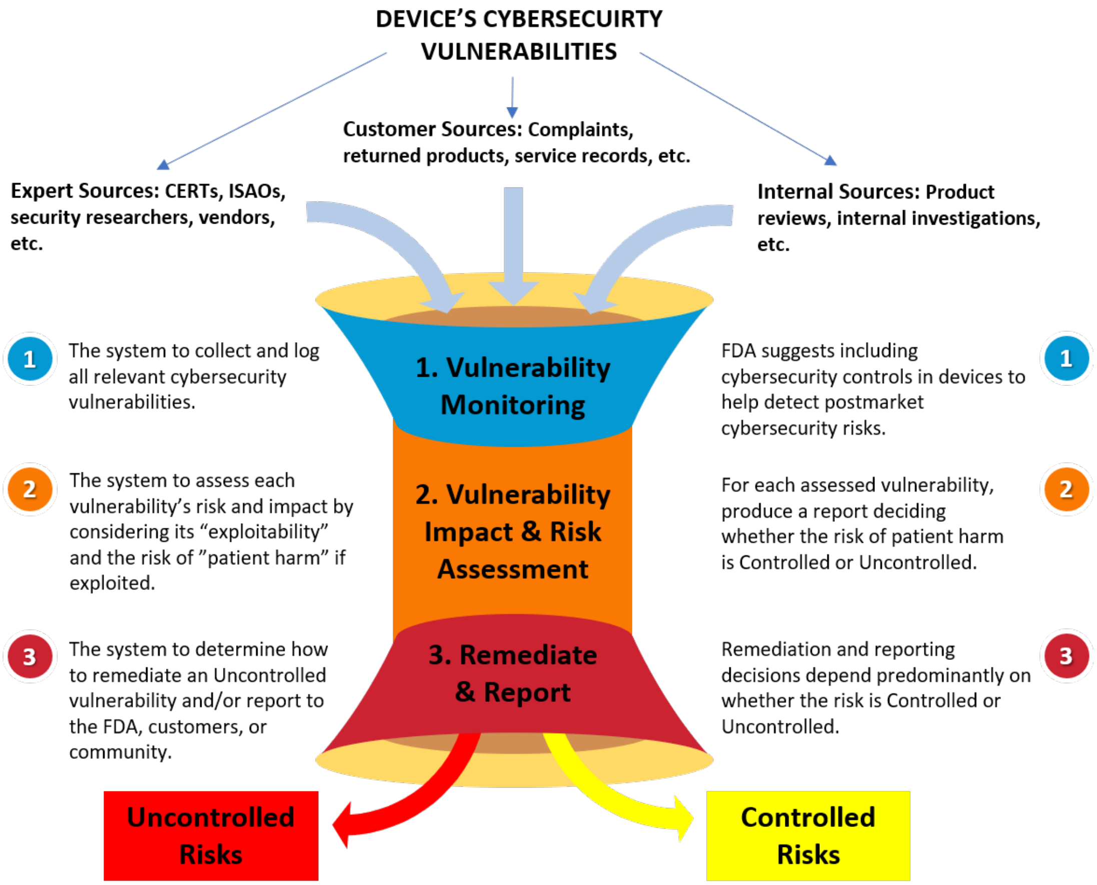
E

C. Avoid Financial Losses from Device Cyber Risks

TOPIC 3: Addressing Unexploited Cybersecurity Vulnerabilities

PART B: Remediate & Report

1. You might have to report and remediate unexploited vulnerabilities
2. This can lead to high costs from reporting, remediation, recalls, and/or regulatory fines
3. Last part of this webinar offers mitigation advice for this topic



DEVICE’S CYBERSECUIRTY VULNERABILITIES

Expert Sources: CERTs, ISAOs, security researchers, vendors, etc.

Customer Sources: Complaints, returned products, service records, etc.

Internal Sources: Product reviews, internal investigations, etc.

1. Vulnerability Monitoring

1 The system to collect and log all relevant cybersecurity vulnerabilities.

1 FDA suggests including cybersecurity controls in devices to help detect postmarket cybersecurity risks.

2. Vulnerability Impact & Risk Assessment

2 The system to assess each vulnerability’s risk and impact by considering its “exploitability” and the risk of ”patient harm” if exploited.

2 For each assessed vulnerability, produce a report deciding whether the risk of patient harm is Controlled or Uncontrolled.

3. Remediate & Report

3 The system to determine how to remediate an Uncontrolled vulnerability and/or report to the FDA, customers, or community.

3 Remediation and reporting decisions depend predominantly on whether the risk is Controlled or Uncontrolled.

Uncontrolled Risks

Controlled Risks

E

C. Avoid Financial Losses from Device Cyber Risks

TOPIC 4: Responding to Exploited Cybersecurity Vulnerabilities

Injuring Patients: can cause same high costs as unexploited + almost unlimited legal liability from lawsuits

PHI Data Breach: can cause same high costs as unexploited + data breach fines and costs that averaged about $4 million on 2018

OVERVIEW OF DIGITAL DEVICE VULNERABILITIES

Main point: Mitigating many of your digital medical device cyber risks starts with understanding the basics of how digital devices are vulnerable to malicious attack. We'll now briefly summarize some of the types of digital device vulnerabilities.

A. Software vulnerabilities

B. Hardware & firmware vulnerabilities

C. Improper system integration, implementation, monitoring and/or end-user error

A. Overview of Software Vulnerabilities – part 1

1. Definition: A flaw or weakness in software that could be accidentally triggered or intentionally exploited to (1) interfere with the software's performance and/or (2) facilitate unauthorized control over the computer system running the software.

2. Most Prevalent Types

- Missing data encryption
- OS command injection
- SQL injection
- Buffer overflow
- Missing authentication for critical function
- Missing authorization
- Unrestricted upload of dangerous file types
- Reliance on untrusted inputs in a security decision
- Cross-site scripting and forgery
- Download of codes without integrity checks
- Use of broken algorithms
- URL redirection to untrusted sites
- Path traversal
- Weak passwords
- Default passwords
- Software that is already infected with virus

A. Overview of Software Vulnerabilities – part 2

3. Regulatory & Legal Responsibilities:

You are responsible for all vulnerabilities in software you create yourself, license, or use. To be clear, that means if you use software that contains vulnerabilities, you will be liable for those vulnerabilities from regulatory and legal perspectives. Your software vulnerability responsible runs throughout the entire device lifecycle, including an affirmative regulatory obligation for postmarket cybersecurity vulnerability monitoring.

4. Secure Coding Best Practices

- **System-wide threat assessment:** Identify specific cyber threats and risks from a system-wide perspective – including known "abuse cases" and publicly available cyber-incidents.
- **Cybersecurity Requirements:** At the requirements stage, create your security-specific requirements to address the specific threats and risks identified in your System-wide Threat Assessment. This stage is critical because it is the point at which security becomes a known development project goal with the appropriate level of risk management, scheduling, and costing.
- **Design and architecture:** When selecting your software design and system architecture, consider both your (1) System-wide Threat Assessment and (2) your Cybersecurity Requirements; and, create testing plans for them.
- **Code development:** Use automation tools such as static analysis and properly implementing security analysis testing can help prevent vulnerabilities.
- **Integration and Test:** After you've developed the first iteration, use subsystem and system testing to find vulnerabilities before integration and deployment to the market. Automated penetration testing tools can be very helpful at this stage.
- **Deployment and maintenance:** Include in the design the ability to update the software and/or firmware. While secure coding practices will reduce vulnerabilities in your marketed products, you must be prepared to remedy newly found vulnerabilities. As you maintain and revise your product, you must continue to apply the same cybersecurity protocols as you did during premarket development.

A. Overview of Software Vulnerabilities – part 3

5. Note about Ensuring the Integrity, Authenticity & Confidentiality of Software Upgrades and Patches

   - Almost all software requires upgrades and patches
   - The upgrade and patching process needs to be properly secured, because it has been a popular vehicle for malicious attack – e.g., the NotPetya worm
   - When that happens, the attacker inserts malicious code into your device via the upgrade and/or patching process.
   - To prevent it, you need the proper encryption system for your upgrading and patching, which companies like Medcrypt do well.

6. Medical Device Software Vulnerability Example -- IPnet

E

B. Overview of Hardware Vulnerabilities – part 1

1. **Definition:** They are an exploitable weakness in the hardware components of a computer system that that could be accidentally triggered or intentionally exploited to facilitate unauthorized control over the computer system.

2. Difference among Hardware, Firmware & Software

- Hardware are tangible/physical components like a CPU or RAM.
- Firmware is a special kind of software semi-permanently installed on hardware to help it function, which can often be changed by special processes.
- Software is a broad term for the programs running on hardware. Familiar kinds of software are operating systems, which provide overall control for computer hardware, and applications, which are optional programs used for a particular job.

3. Different Types

- Hardware backdoors: e.g. time bombs, cheat codes,
- Semiconductor Doping
- Eavesdropping by gaining access to protect memory
- Inducing faults
- Hardware modification with invasive features
- Counterfeiting product assets allowing malicious access
- Side-channel attacks – timing, power analysis, electromagnetic (reading monitor content), fault induction (smart cards)

E

B. Overview of Hardware Vulnerabilities – part 2

4. Meltdown & Spectre Attacks Exploited Hardware Vulnerabilities

- **Cache side-channel attacks:** In 2017, Google's Project Zero identified both Spectre and Meltdown, which are forms of side-channel attacks that take advantage of the ability to extract information from instructions that have executed on a CPU using the CPU cache as a side-channel.

- **Impact:** Meltdown and Spectre exploit critical vulnerabilities in CPUs to steal data stored in the memory of other running programs – e.g., passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents.

- **Federal Gov't Warning:** The US-CERT on January 2, 2018 issued an alert about these attacks.

- **Device manufacturers affected:** The following companies all report issues relating to these attacks: Abbott, BD, GE, Honeywell, J&J Medtronic, OSIsoft, Drager, Philips, Siemens, Beckman Coulter, Emerson, Rockwell, etc.

- **Remediation:** Millions of computers had to be patched at significant costs, & one of the software patches degraded CPU performance.

E

C. Improper Integration, Implementation, and/or End-User Error

1. Understand Shared Cyber Risks & Joint/Several Liability: Devices typically generate shared cyber risks with deploying healthcare delivery organizations for which there is joint and several liability. This means that you have vested interest in how your devices are integrated, implemented and used.

2. A System Integration Example: When medical device as software was installed on a cardiology workstation that supported a cardiac procedure, the software came with specially configured antivirus software. But, the hospital's IT staff reconfigured the antivirus software to meets its internal specifications; and that reconfiguration impeded the software's performance.

3. An Implementation & End-user Example: A related issue is user authentication failure – i.e. failure to require user authentication for critical functions and other authentication vulnerabilities can leave devices susceptible to attack. One common example is the use of "hard-coded" user credentials used across a fleet of devices.

4. Important Mitigations: Your cybersecurity strategy should mitigate these share risks via (1) proper labeling and instructions of use, (2) training and (3) contracts that shift these risks to your customers.

E

MITIGATION ADVICE & SUGGESTIONS

1. Cybersecurity Governance Matters

2. A Proper System-Wide Threat & Risk Analysis

3. Good Design, Smart Engineering & Proper Labeling

4. Postmarket Implementation Challenges

5. Using Insurance

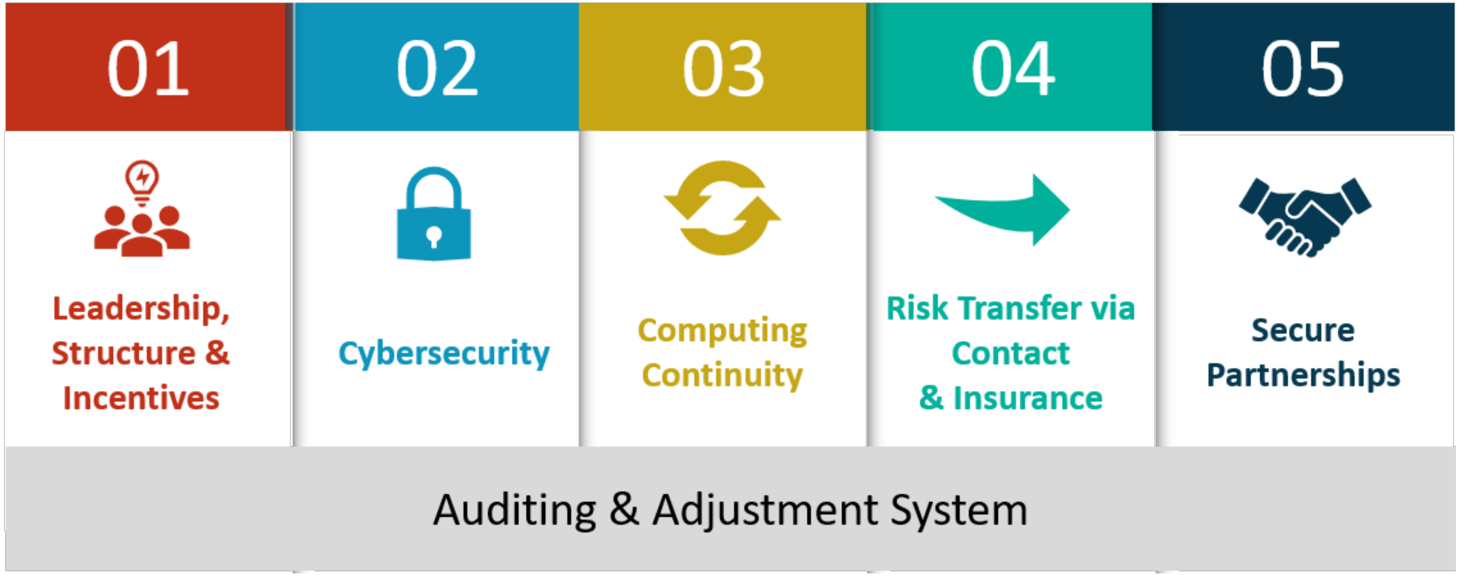
6. Questions

E

1. Cybersecurity Governance Matters

A. OVERALL CYBER RISK MITIGATION

- Identify and Quantify all your Operational & Device Cyber Risks
- Allocate your limited mitigation resources among the 5 Cyber Risk Mitigation Tools:

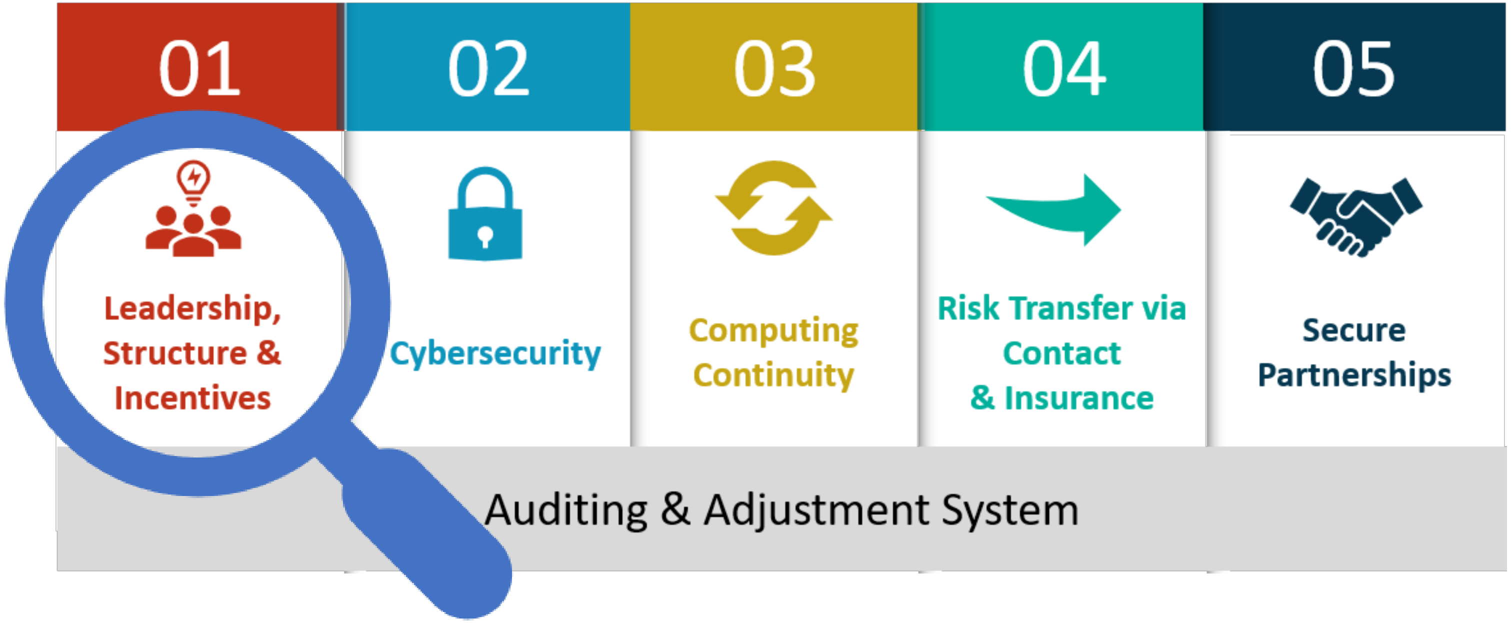


01
Leadership, Structure & Incentives
02
Cybersecurity
03
Computing Continuity
04
Risk Transfer via Contact & Insurance
05
Secure Partnerships
Auditing & Adjustment System

1. Cybersecurity Governance Matters

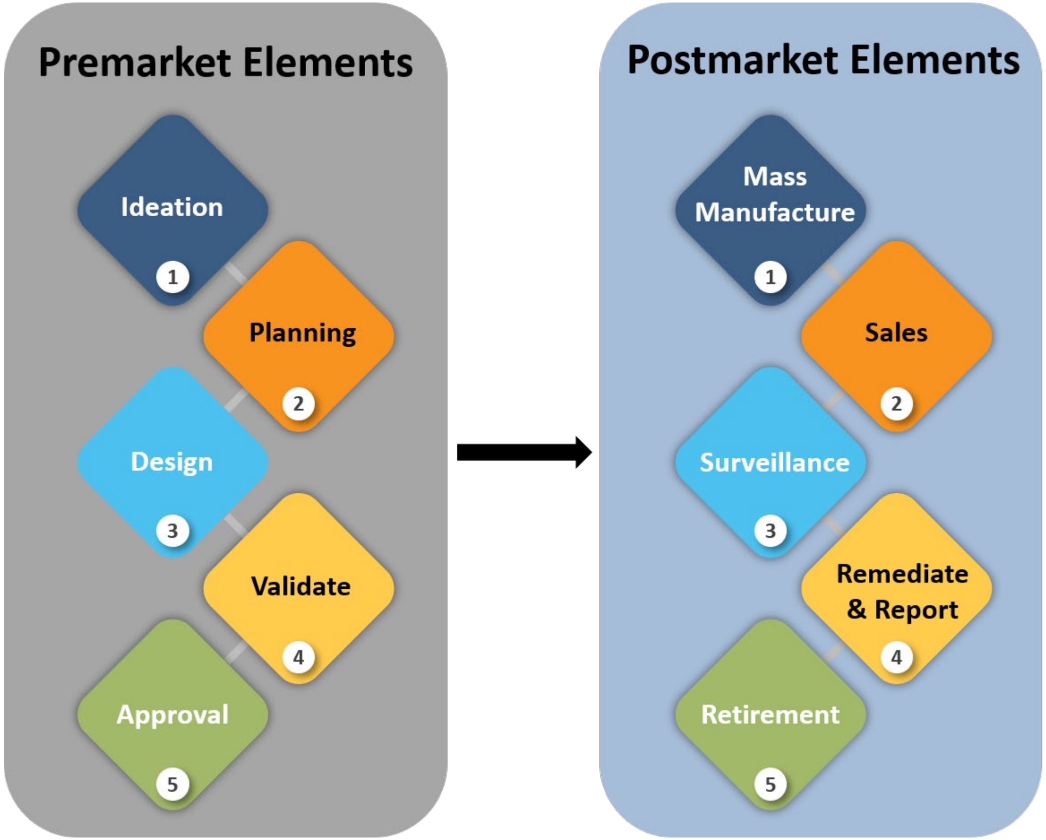
A. OVERALL CYBER RISK MITIGATION

- Identify and Quantify all your Operational & Device Cyber Risks
- Allocate your limited mitigation resources among the 5 Cyber Risk Mitigation Tools:


01
Leadership, Structure & Incentives
02
Cybersecurity
03
Computing Continuity
04
Risk Transfer via Contact & Insurance
05
Secure Partnerships
Auditing & Adjustment System

1. Cybersecurity Governance Matters

B. MITIGATION STRATEGY FOR FULL DEVICE LIFECYCLE



G

1. Cybersecurity Governance Matters

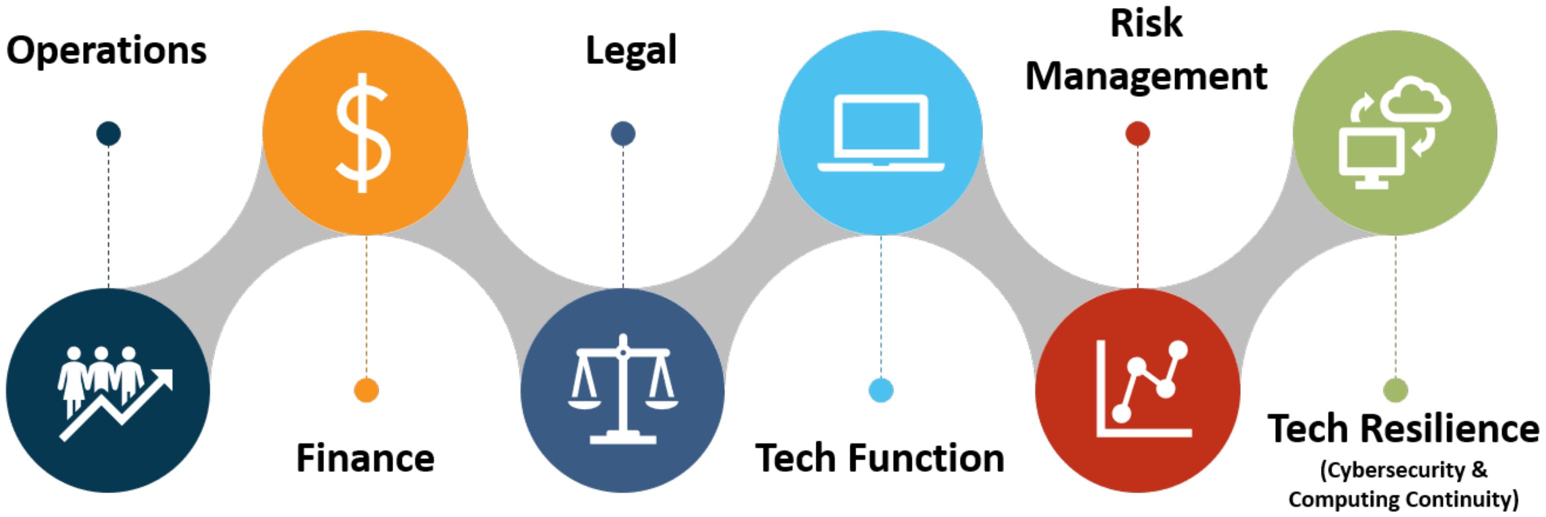
C. BOARD OF DIRECTORS & C-SUITE

Proper Knowledge: properly educate themselves about your organization's unique cyber risks and the amounts of money at stake – particularly your digital device risks

Foresight: recognize the significant value of incorporating strong cybersecurity during the design, engineering, and implementation phases of your digital device lifecycle– because wise upfront investments pay off in the long run

1. Cybersecurity Governance Matters

D. THE RIGHT MULTIDISCIPLINARY TEAM



G

1. Cybersecurity Governance Matters

E. CYBERSECURITY LEADERSHIP CHALLENGES

Operational v. Device Cyber Risk Mitigation: Almost always some connection. Similar skill sets with some materials differences.

Product Line or Device Cybersecurity Leader: Allows for concentration on device issues. Must have ability to communicate freely to C-Suite & Board. Coordinates with operational mitigation.

Outsource v. Full-time: Talented, full-time CISO or Device Cybersecurity Leader can be very expensive. Some consultants like Practical Cyber can fill both roles for far less.

2. A Proper System-Wide Threat & Risk Analysis

FDA & Design Best Practices: FDA Premarket Cybersecurity Guidance and secure software coding and IoT device design best practices all say start with a System-Wide Threat & Risk Analysis.

Must Have Enough Detail: Should include a "system diagram" and "cybersecurity bill of materials" for the full product lifecycle – otherwise you will miss too many threats and risks.

Leverage External Expertise: Significant cyber-threat expertise is needed for a system-wide threat & risk analysis. Younger medical device manufacturers can often benefit from engaging external expertise to help with (1) the threat & risk analysis, (2) cybersecurity design controls, and (3) cybersecurity engineering.

3. Good Design, Smart Engineering & Proper Labeling

A. CYBERSECURITY DESIGN CONTROL ISSUES

FDA Premarket Approval: Recommends explaining how you use a long list of cybersecurity "design controls" divided into (1) Identify & Protect Device Assets & Functionality and (2) Detect, Respond & Recover.

Design Controls Save Money: Vulnerabilities can cause huge postmarket costs – e.g., legal liability for patient harm and even high costs for unexploited vulnerabilities. Remediating vulnerabilities after commercialization can be more expensive than preventative efforts

.

Quantify Threats & Risks: This provide excellent value. But, quantifying a system-wide threat & risk analysis requires significant cyber-threat expertise. Younger medical device manufacturers can often benefit from engaging external expertise to help with (1) the threat & risk analysis, (2) cybersecurity design controls, and (3) cybersecurity engineering.

E

3. Good Design, Smart Engineering & Proper Labeling

B. CYBERSECURITY ENGINEERING ISSUES

What is it?: When you build, integrate, and test/validate your device – particularly:

- Buying or building trustworthy hardware components;
- Licensing, procuring, or coding trustworthy software such as operating systems and device analysis systems
- Integrating and testing/validating your components

Tips to consider: **When using these tips, consider the full device lifecycle –**

Hardware: Hardware components have different cybersecurity issues. Before procurement, assess the cybersecurity of every component.

Software: Most device vulnerabilities have come from software. Not easy to create secure software or assess the security of procured software.

Strong Quality Management: This involves ample testing/validation after integration, including all possible interactions with end-users. Ensure that your devices are properly manufactured and that your engineering was done well.

3. Good Design, Smart Engineering & Proper Labeling

C. CYBERSECURITY LABELING & INSTRUCTIONS OF USE

What are they?: All documentation and/or training to help all end-users – e.g., healthcare practitioners, healthcare support staff (e.g. IT personnel), and patients – avoid actions that add any cybersecurity vulnerability that increases the risk of patient.

Compliance: Use the FDA's Premarket Cybersecurity Guidance "labeling check list" when creating your labeling and instructions of use documentation. Include that documentation in your premarket 510(k) and PMA submissions.

Economic Benefits of Clear & Effective

1. Reduce customer service and/or technological support costs
2. Facilitate sales
3. Reduce liability when end-user contravention leads to an exploited vulnerability

TIP

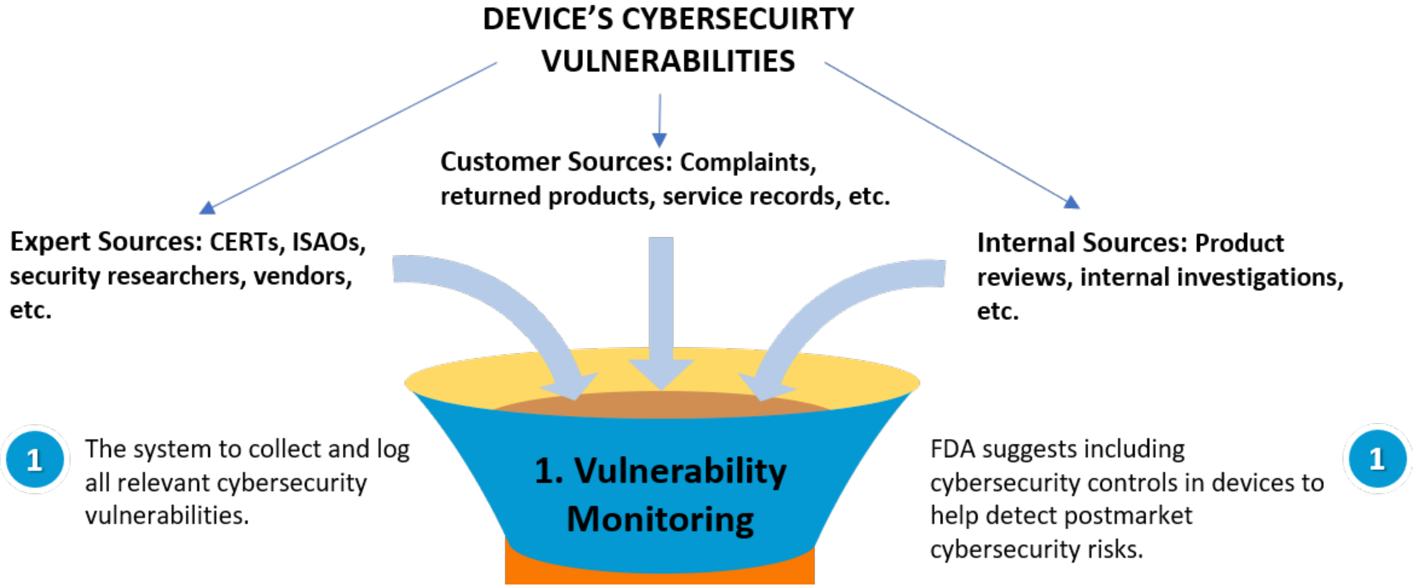
Modify agreements and SLAs to reflect advantages from clear & effective labeling and instructions of use

E

4. Postmarket Implementation Challenges

A. POSTMARKET VULNERABILIT MONITORING – ignorance can hurt a lot (part 1)

Compliance: FDA's Postmarket Cybersecurity Guidance recommends diligently and proactively searching for vulnerabilities from 3 sources: customers, internal & external.



DEVICE'S CYBERSECUIRTY VULNERABILITIES

Customer Sources: Complaints, returned products, service records, etc.

Expert Sources: CERTs, ISAOs, security researchers, vendors, etc.

Internal Sources: Product reviews, internal investigations, etc.

1. Vulnerability Monitoring

1 The system to collect and log all relevant cybersecurity vulnerabilities.

FDA suggests including cybersecurity controls in devices to help detect postmarket cybersecurity risks. 1

4. Postmarket Implementation Challenges

A. POSTMARKET VULNERABILIT MONITORING – ignorance can hurt a lot (part 2)

Customer Sources: Good relationships with the cybersecurity personnel at your customer HDOs can yield valuable info about cybersecurity and end-user satisfaction. Some put vulnerability reporting functions on their websites.

External Sources: FDA's Postmarket Guidance recommends using the CVSS. Also, consider monitoring the darkweb and developing relationships with key medical device cybersecurity researchers.

ISAO Participation: Participating in an Information Sharing and Analysis Organization ("ISAO") can be a good source of info about cybersecurity design controls, vulnerabilities, and other issues. FDA gives manufacturers that actively participate some postmarket reporting advantages.

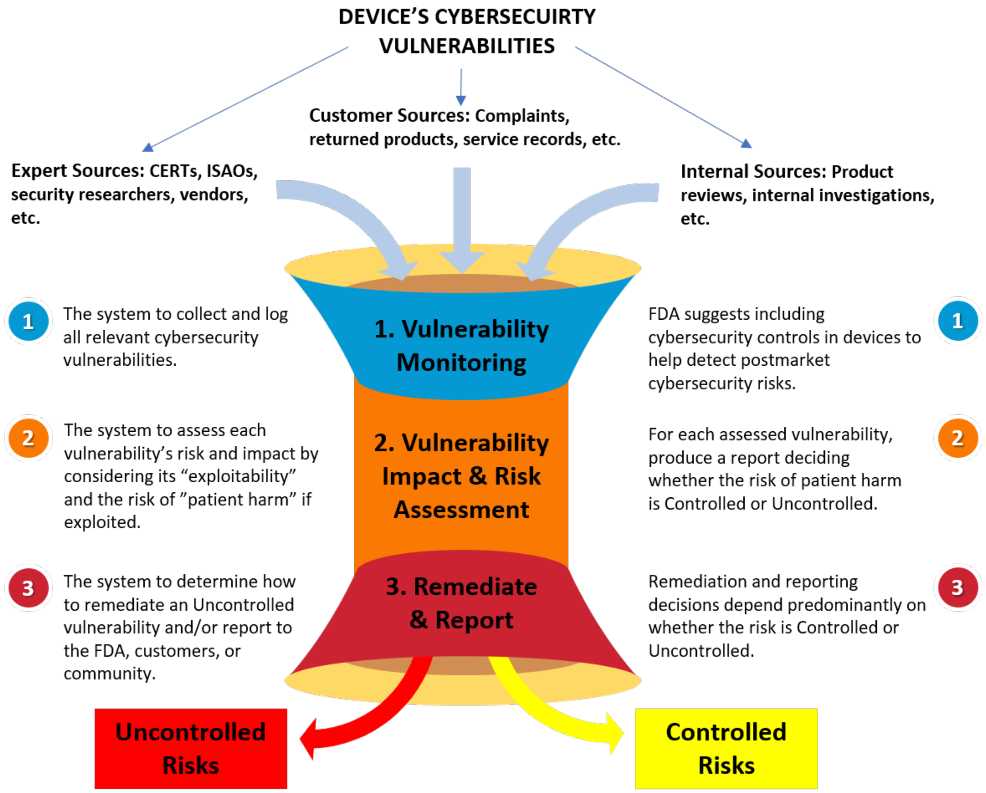
Harm From Failure to Identify Vulnerabilities: (1) Higher probability of an exploited vulnerability injuring patients. (2) Increased exposure to regulatory liability even for unexploited vulnerabilities. (3) Negative press that hurts your ability to raise money and/or make future sales.

E

4. Postmarket Implementation Challenges

B. POSTMARKET REMEDIATION & REPORTING – part 1

Compliance: FDA's Postmarket Cybersecurity Guidance recommends systems for (1) assessing the Impact and Risks of cybersecurity vulnerabilities and (2) Remediating and reporting the significant vulnerabilities (i.e., "Uncontrolled Risks").



DEVICE'S CYBERSECUIRTY VULNERABILITIES

Expert Sources: CERTs, ISAOs, security researchers, vendors, etc.

Customer Sources: Complaints, returned products, service records, etc.

Internal Sources: Product reviews, internal investigations, etc.

1. Vulnerability Monitoring

1 The system to collect and log all relevant cybersecurity vulnerabilities.

1 FDA suggests including cybersecurity controls in devices to help detect postmarket cybersecurity risks.

2. Vulnerability Impact & Risk Assessment

2 The system to assess each vulnerability's risk and impact by considering its "exploitability" and the risk of "patient harm" if exploited.

2 For each assessed vulnerability, produce a report deciding whether the risk of patient harm is Controlled or Uncontrolled.

3. Remediate & Report

3 The system to determine how to remediate an Uncontrolled vulnerability and/or report to the FDA, customers, or community.

3 Remediation and reporting decisions depend predominantly on whether the risk is Controlled or Uncontrolled.

E

4. Postmarket Implementation Challenges

B. POSTMARKET REMEDIATION & REPORTING – part 2

Impact & Risk Assessment: System to assess each vulnerability's risk and impact by considering "exploitability" and risk of "patient harm".

Produce reports whether patient harm risk is Controlled or Uncontrolled.

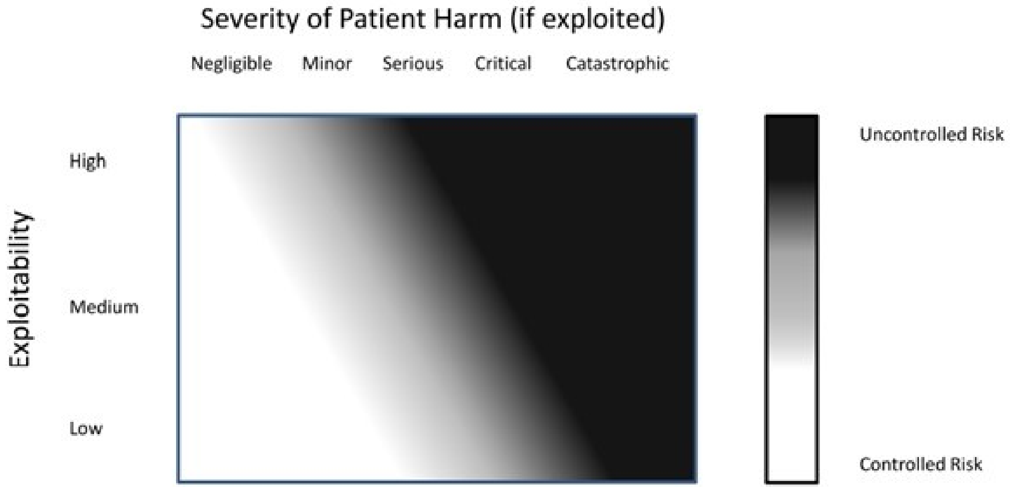


Figure – Evaluation of Risk of Patient Harm. The figure shows the relationship between exploitability and severity of patient harm, and can be used to assess the risk of patient harm from a cybersecurity vulnerability. The figure can be used to categorize the risk of patient harm as controlled or uncontrolled.

4. Postmarket Implementation Challenges

B. POSTMARKET REMEDIATION & REPORTING – part 3

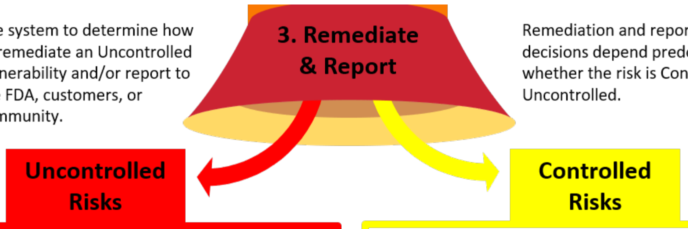
Report & Remediate: The system to determine how to remediate an Uncontrolled vulnerability and/or report to the FDA, customers, or community.

Remediation and reporting decisions depend predominantly on the results of your impact and risk assessment for that specific vulnerability.

Decisions are complex and can greatly influence your postmarket costs. Make sure you have the requisite expertise.

3 The system to determine how to remediate an Uncontrolled vulnerability and/or report to the FDA, customers, or community.

Remediation and reporting decisions depend predominantly on whether the risk is Controlled or Uncontrolled. 3



Uncontrolled Risks

DEFINITION: Unacceptable residual risk of patient harm from insufficient risk mitigations and controls.

REMEDIATE: "As quickly as possible," remediate via compensating and/or new controls to "acceptable" risk.

TEST: Test all changes (e.g. software validation per 21 CFR 820.30(g)) to ensure remediation efficacy.

DOCUMENT: Properly document all changes as required by 21 CFR 820, including "the timeline rational for" your "remediation plan."

CUSTOMER/COMMUNITY REPORTING: Disclose info about controls and residual risks so customers and the community can make informed decisions.

FDA REPORTING: Report to the FDA per 21 CFR 806 unless (1) "reported under 21 CFR parts 803 or 1004" or (2) the "following circumstances are met:"

- No "known serious adverse events or deaths associated with the vulnerability;"
- As soon as possible but within 30 days, you notify customers/community about the vulnerability, identify interim compensating controls, and develop a remediation plan to reduce to an acceptable risk;
- As soon as possible but within 60 days, you fix the vulnerability, test the fix, and distribute "the deployable fix" to customers/community that reduces the residual risk to "acceptable;" and
- You "actively participate" in an ISAO "that shares vulnerabilities and threats that impact medical devices" and provide it with your customer/community notification.

Report the vulnerability and your remediation plan in any annual report that so requires – e.g. PMA devices per 21 CFR 814.84.

Controlled Risks

DEFINITION: Sufficiently low (acceptable) risk of patient harm.

LABELLING: Might require changes to labelling.

REMEDIATE: Remediation is not mandatory. But, consider "additional control(s) as part of defense-in-depth." Vulnerabilities solely related to PHI "would be typically considered a cybersecurity routine update or patch."

REPORTING: No need to report "routine updates and patches." But, for "premarket approval (PMA) devices with periodic reporting requirements under 21 CFR 814.84," report routine updates and patches in (annual) report."

E

4. Postmarket Implementation Challenges

B. POSTMARKET REMEDIATION & REPORTING – part 4

Robust Cyber-Incident Mitigation System: Essential that you have a robust cyber-incident mitigation system that covers both operational and device risks.

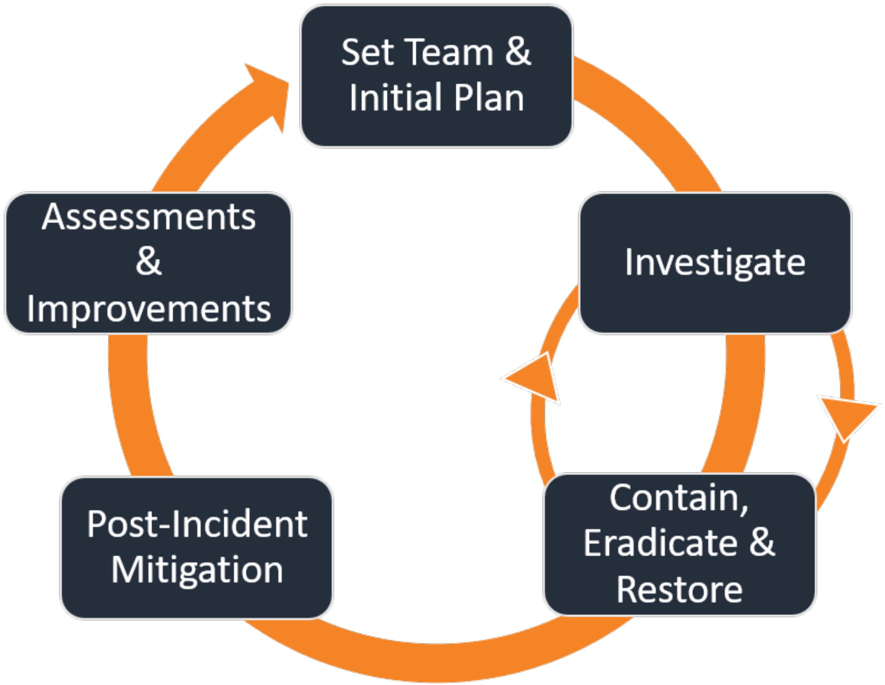
Go beyond the traditional incident response plan.

Deploy your full Multidisciplinary team.

Be able to react immediately.

You must practice regularly.

CYBER-INCIDENT MITIGATION SYSTEM



5. Using Insurance

- Potential Insurance Coverages
- Interactions among Various Coverages
- Insurers’ Cyber Risk Review
- Manufacturer’s Representations to Insurer
- Contractual Indemnifications & Coverage Collisions
- Insurance Coverage of Other Parties

6. Questions: FAQs

If you have additional questions, please contact either use of using the information below:

ELLIOT TURRINI

CYBERSECURITY EXPERT + PRIVACY & CYBER LAWYER

201-572-4957

Elliot@PracticalCyber.Com

www.PracticalCyber.Com

GERARD NUSSBAUM

STRATEGIC TECHNOLOGY ADVISOR, ATTORNEY

312-620-9507

gerard@zarachassociates.com