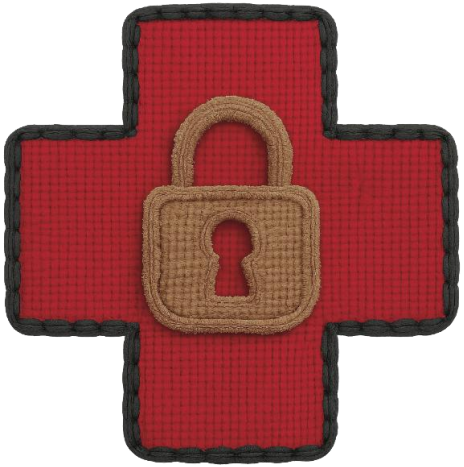
Northeastern University



Medical Device Cybersecurity – Week 13

03/31/2026

Postmarket Activities

Axel Wirth | Chief Security Strategist | Medcrypt
axel@medcrypt.com

Medical Device Cybersecurity
Manufacturer vs Operator Perspective

- Recap – Secure Lifecycle Concept
- Postmarket Activities
- Coordinated Vulnerability Disclosure
- Incident Response Deep Dive

The Secure Development Lifecycle (SDLC) Context

- General Premarket activities
- Postmarket begins after regulatory approval:
  - Release for sale
  - Manufacturing transfer
- Applies to all new products, versions, and updates & patches

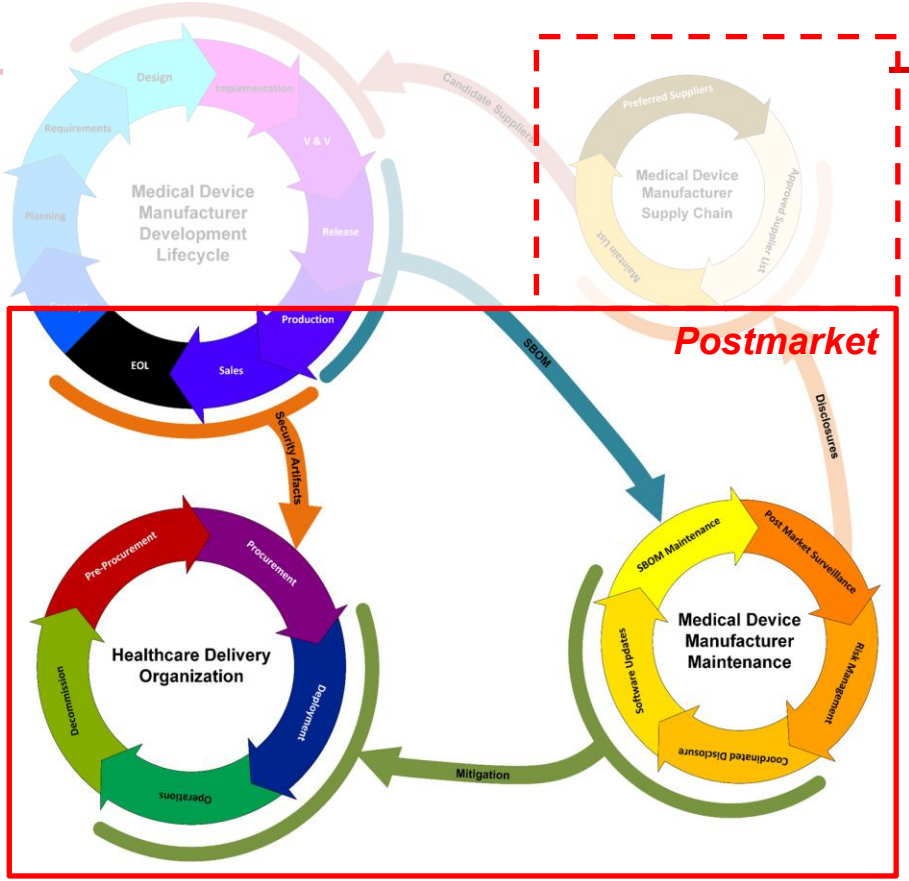
- Supply Chain Management
- Vulnerability Monitoring
- Contract and relationship management

HDO Perspective:
- Procurement
- Onboarding
- Maintenance
- Decommissioning

- Patches and Updates
- Documentation
- Risk Communication
  - Vulnerabilities
  - Threats
  - EOL / EOS

The Secure Development Lifecycle (SDLC) Context

- General Premarket activities
- Postmarket begins after regulatory approval:
  - Release for sale
  - Manufacturing transfer
- Applies to all new products, versions, and updates & patches



- Supply Chain Management
- Vulnerability Monitoring
- Contract and relationship management

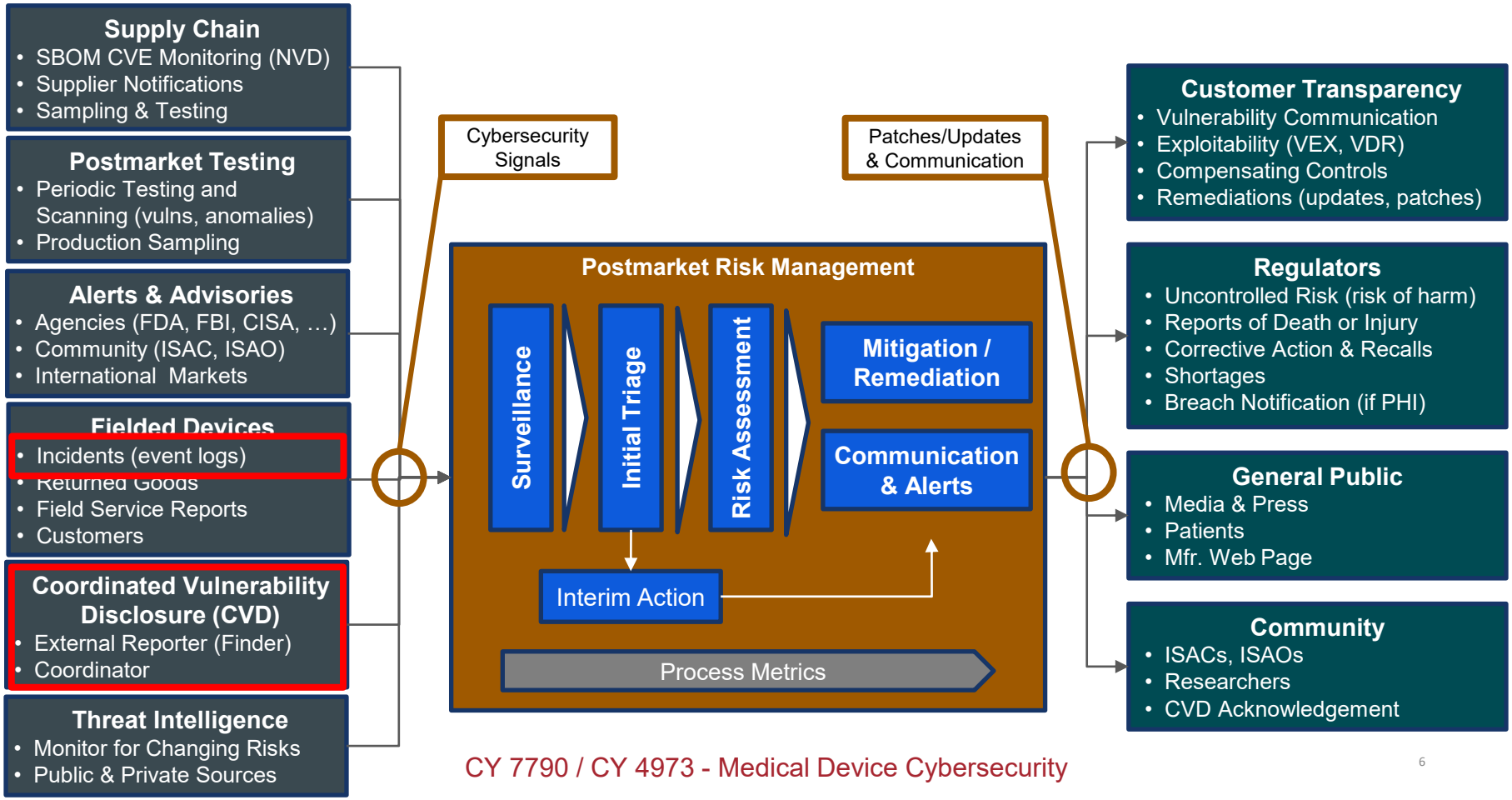
HDO Perspective:
- Procurement
- Onboarding
- Maintenance
- Decommissioning

- Patches and Updates
- Documentation
- Risk Communication
  - Vulnerabilities
  - Threats
  - EOL / EOS

Medical Device Cybersecurity
Manufacturer vs Operator Perspective

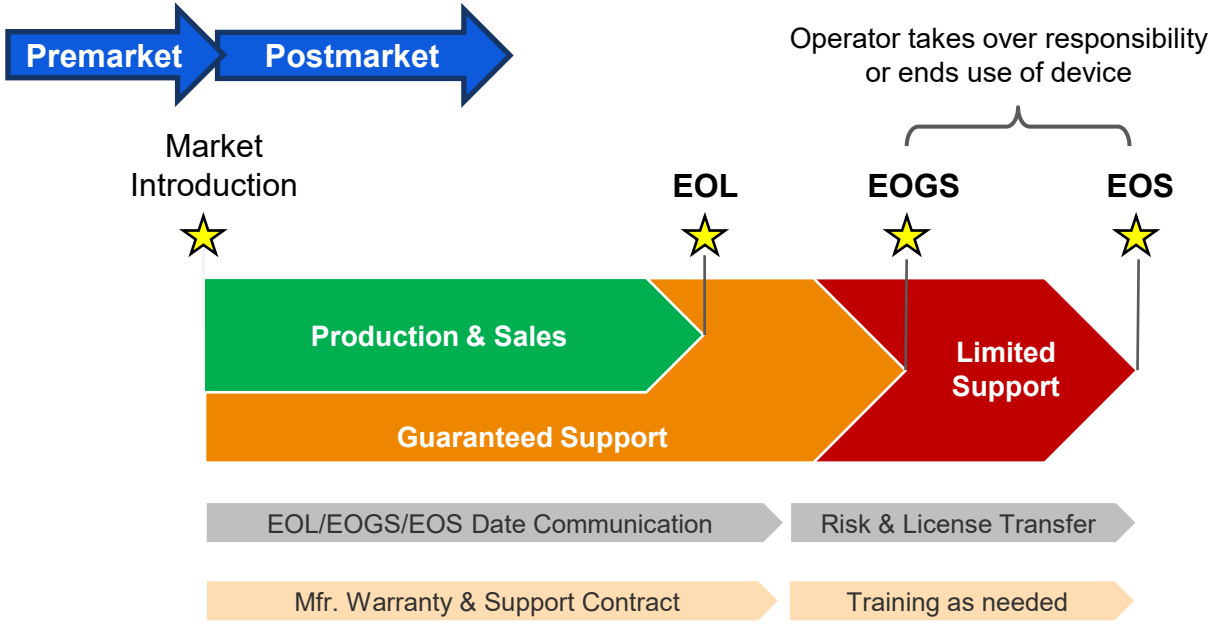
- Recap – Secure Lifecycle Concept
- Postmarket Activities
- Coordinated Vulnerability Disclosure
- Incident Response Deep Dive

General Cybersecurity Postmarket Risk Management Flow



CY 7790 / CY 4973 - Medical Device Cybersecurity

Postmarket in the End-of-Life (EOL) Context



Note – risk should only be transferred if risk is transferrable!

Market Introduction typically requires some formal approval by regional regulators (AKA premarket authorization).

EOL: (1) the manufacturer no longer sells the product, and (2) the product has gone through a formal EOL process, including notification to operators and/or users.

EOGS: Point after which the manufacturer no longer guarantees full support.

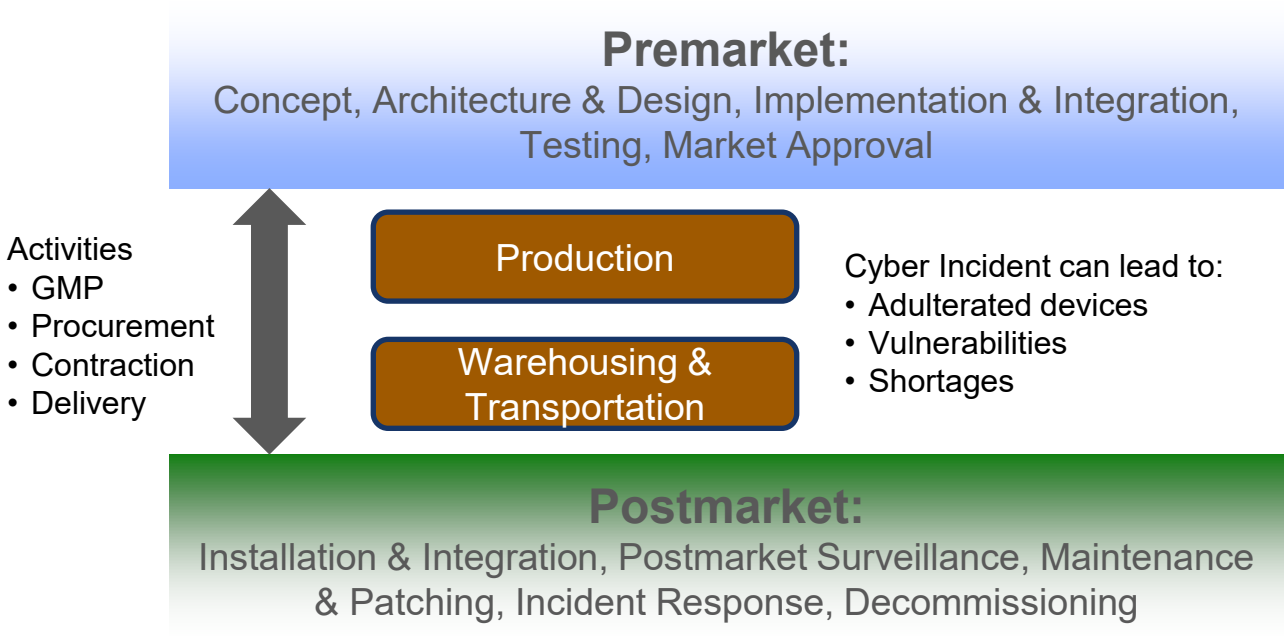
EOS: Point after which the manufacturer has terminated all support activities. Devices comes "legacy" from the hospital perspective.

Note – Mfr. corrective action and recall obligations do not end at EOS!

Decommissioning: End-of-Use from the Hospital / Operator perspective

Source: HSCC: "Health Industry Cybersecurity-Managing Legacy Technology Security (HIC-MaLTS)" https://healthsectorcouncil.org/legacy-tech-security/

From Pre- to Post-Market – The "In-Between"

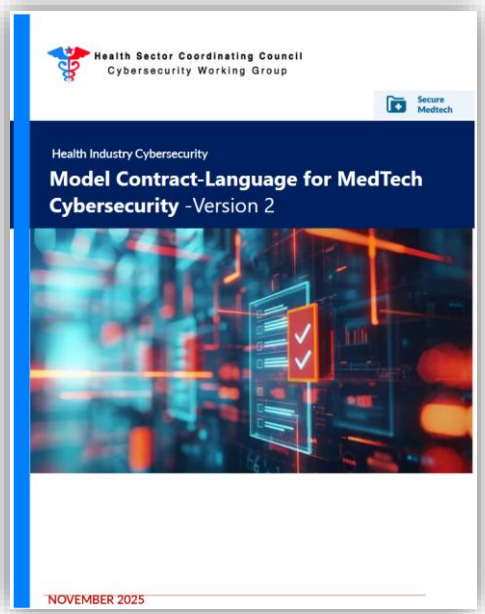


FDA Premarket Cybersecurity Guidance

Regulations exist but not specific to cybersecurity (yet)

FDA Postmarket Cybersecurity Guidance

Addressing the “In-Between”



https://healthsectorcouncil.org/wp-content/uploads/2025/11/MC2v2.pdf

https://www.fda.gov/media/187159/download?attachment

Note:
Any production incident can affect cyber and non-cyber devices

Medical Device Cybersecurity
Manufacturer vs Operator Perspective

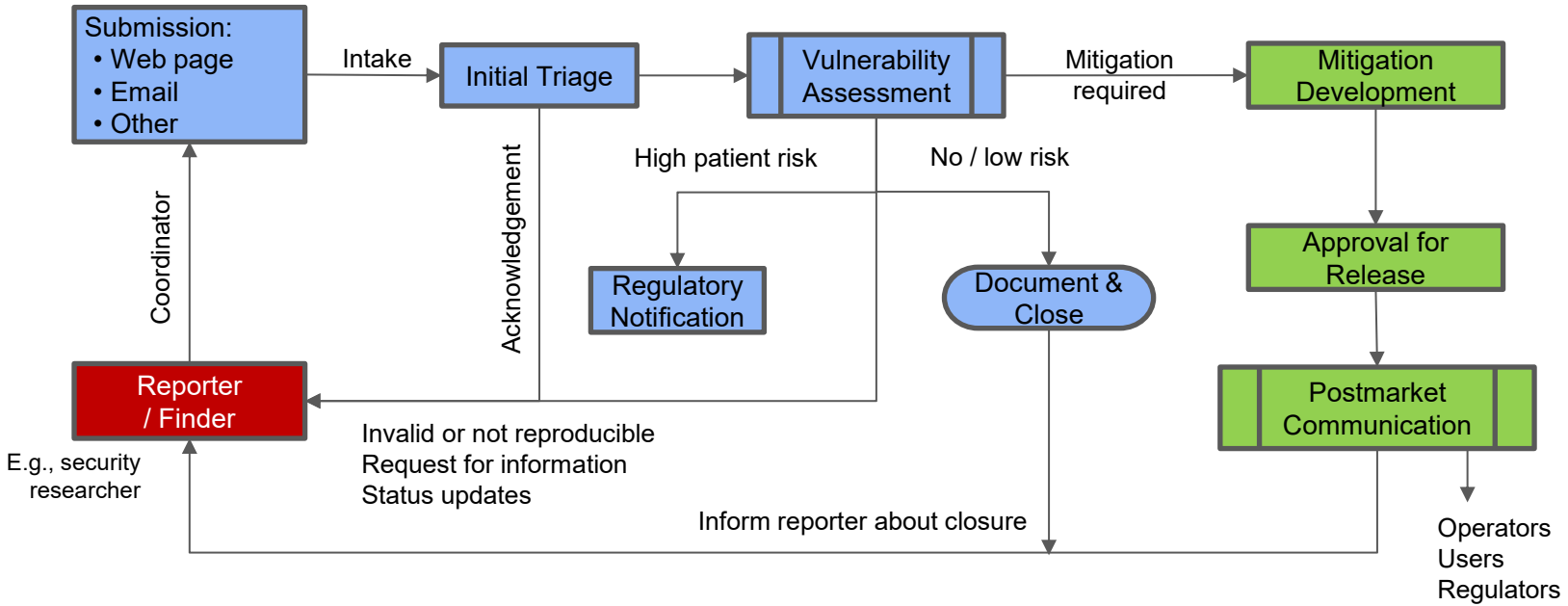
- Recap – Secure Lifecycle Concept
- Postmarket Activities
- Coordinated Vulnerability Disclosure
- Incident Response Deep Dive

Coordinated Vulnerability Disclosure (CVD)

- Security research vs. manufacturer / operator:
  - The CVD concept evolved based on behavior patterns in traditional areas such as commercial software or the Internet; e.g.; operating systems, web servers, …
  - If an external party (e.g., white hat hacker) finds a vulnerability, what to do?
  - Full disclosure – bad because attackers can act faster than defenders
  - No disclosure – better but still not great because adversaries still may find it
  - Early concept of “Responsible Vulnerability Disclosure” later renamed to “Coordinated Vulnerability Disclosure (CVD)”
  - Note – the concept is specifically designed for researchers and software vendors to coordinate public disclosure.
  - Non-researcher vulnerabilities also need to be communicated, so those two functions overlap!
- Hence, we have two standards governing this:
  - ISO/IEC 29147:2018: Information technology — Security techniques — Vulnerability disclosure
  - ISO/IEC 30111: Information technology — Security techniques — Vulnerability handling processes
  - Note the difference: CVD vs general vulnerability handling and communication

Coordinated Vulnerability Disclosure (CVD)

Full disclosure (bad) – no disclosure (better but not ideal) – coordinated disclosure (best)



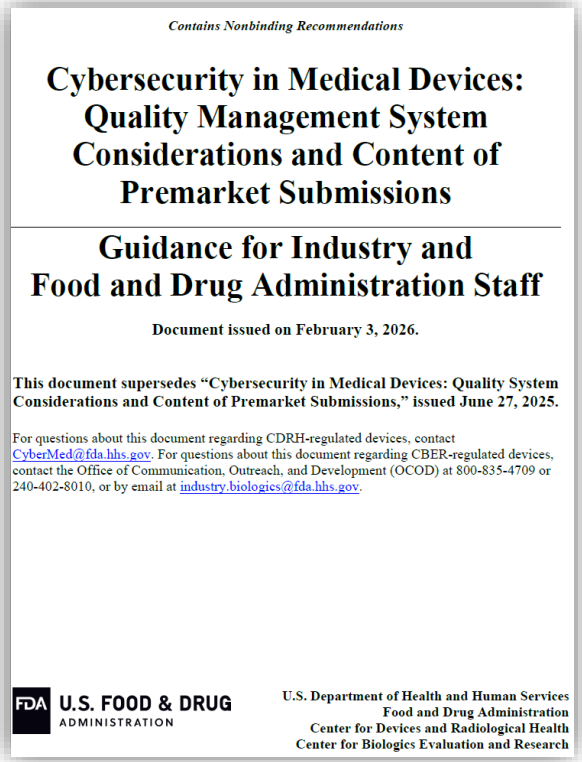
ISO/IEC 29147:2018: Information technology — Security techniques — Vulnerability disclosure

Unique to CVD

General Vuln. Communication process

CY 7790 / CY 4973 - Medical Device Cybersecurity

Sometimes You Can't Win



Contains Nonbinding Recommendations

Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions

Guidance for Industry and Food and Drug Administration Staff

Document issued on February 3, 2026.

This document supersedes "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions," issued June 27, 2025.

For questions about this document regarding CDRH-regulated devices, contact CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 800-835-4709 or 240-402-8010, or by email at industry.biologics@fda.hhs.gov.

FDA U.S. FOOD & DRUG ADMINISTRATION

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. Plans and Procedures (Section 524B(b)(1))

Section 524B(b)(1) of the FD&C Act requires manufacturers of cyber devices to submit to FDA "a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities and exploits, including coordinated vulnerability disclosure and related procedures" in their premarket submissions. We recommend that the plan contain the information recommended for the Cybersecurity Management Plan described in Section VI.B. In particular, such a plan should address the items discussed below.

First, FDA considers that coordinated vulnerability disclosure (CVD) and related procedures, as required in section 524B(b)(1) of the FD&C Act, could include:

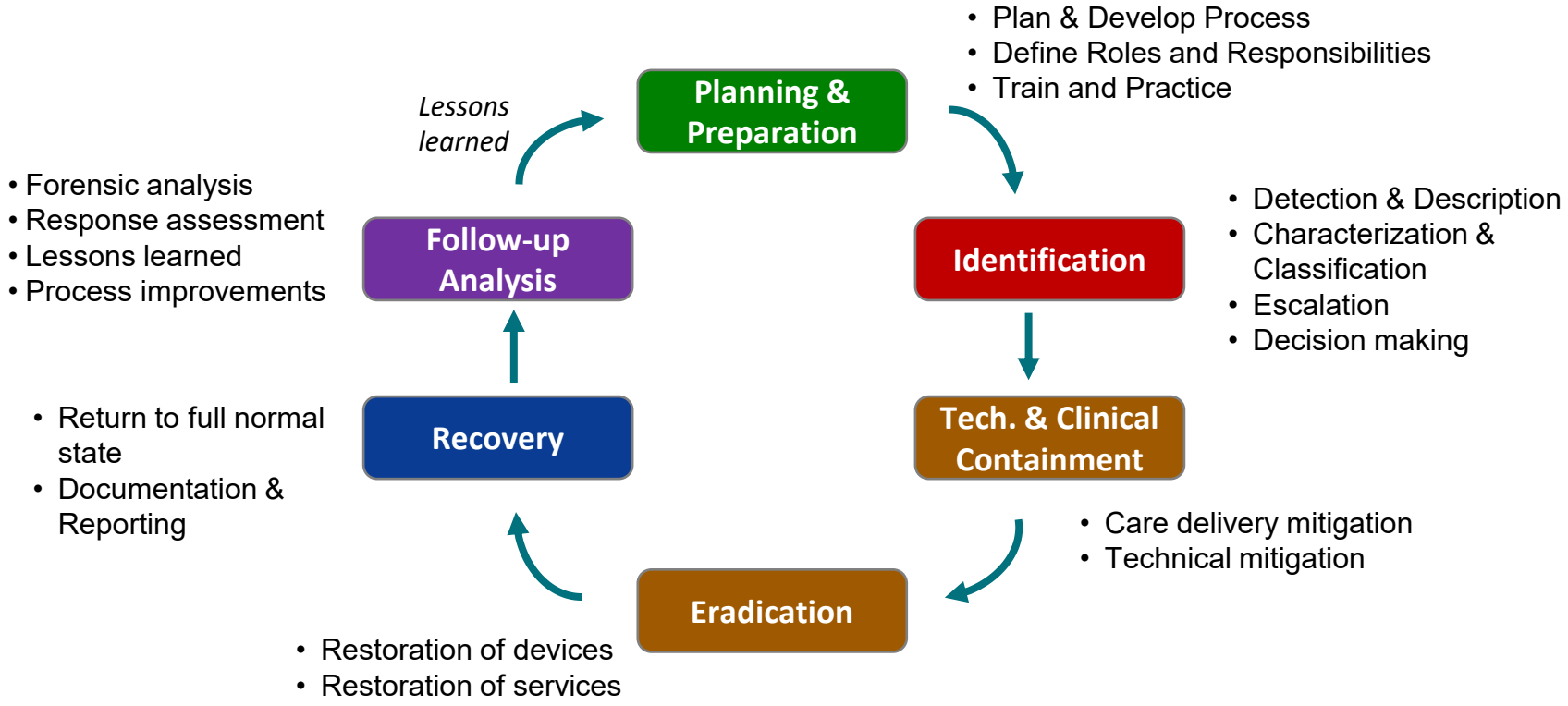
- Coordinated disclosure of vulnerabilities and exploits identified by external entities (including third-party software suppliers and researchers);
- Disclosure of vulnerabilities and exploits identified by the manufacturer of cyber devices; and
- Manufacturer procedures to carry out disclosures of the vulnerabilities and exploits, as identified above.[62]

Medical Device Cybersecurity
Manufacturer vs Operator Perspective

- Recap – Secure Lifecycle Concept
- Postmarket Activities
- Coordinated Vulnerability Disclosure
- Incident Response Deep Dive

Incident Response – General Approach

Example Incident Response Flow and Tasks



Where Incidents can Occur

Examples for Type of Compromise:

Production	Sales & Distribution	Installation & Integration	Operation (incl. XaaS)	Service & Maintenance	Decommission
• SW corruption • Lack of signing • Manufacturing environment compromised	• Logistics breakdown • Environmental compromise • Miscommunication	• Corrupted device • Misconfiguration • Insecure integration	• Malware • Hack • Insider • Beachhead	• Corrupted update • Infected media • Remote hack	• Loss or Theft • Improper disposal

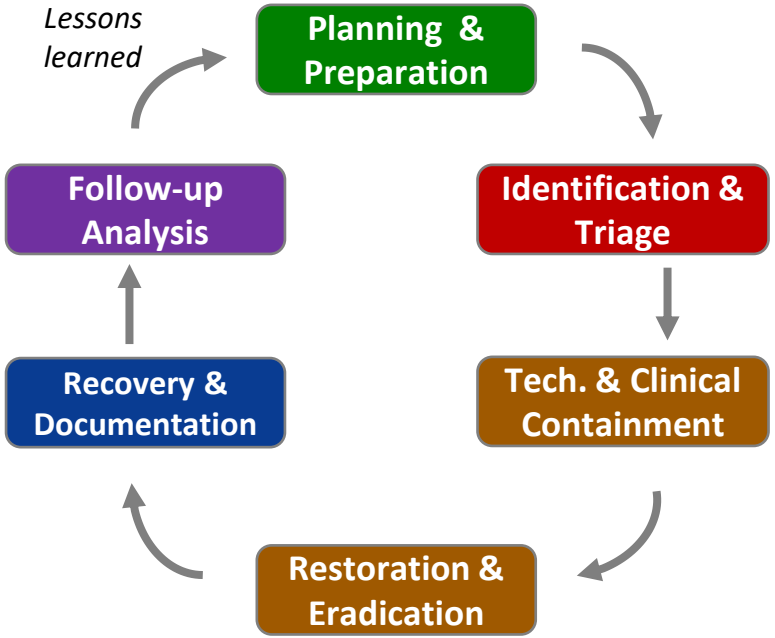
Main Consequences:

Production	Sales & Distribution	Installation & Integration	Operation (incl. XaaS)	Service & Maintenance	Decommission
• Adulterated device • Cryptographic secret compromise	• Adulterated device	• Security weakness	• Breach • Harm • Infection • Corruption	• Infection • Corruption	• Breach

This is where a lot of the attention is focused – too narrowly.

IR Example – Fielded Device Scenario

But specifics vary based on type of incident



Hospital (HDO):

- Patient Safety
- Care delivery
- Legally responsible
- May contract out
- May require 3rd party assistance

Manufacturer (incident at HDO):

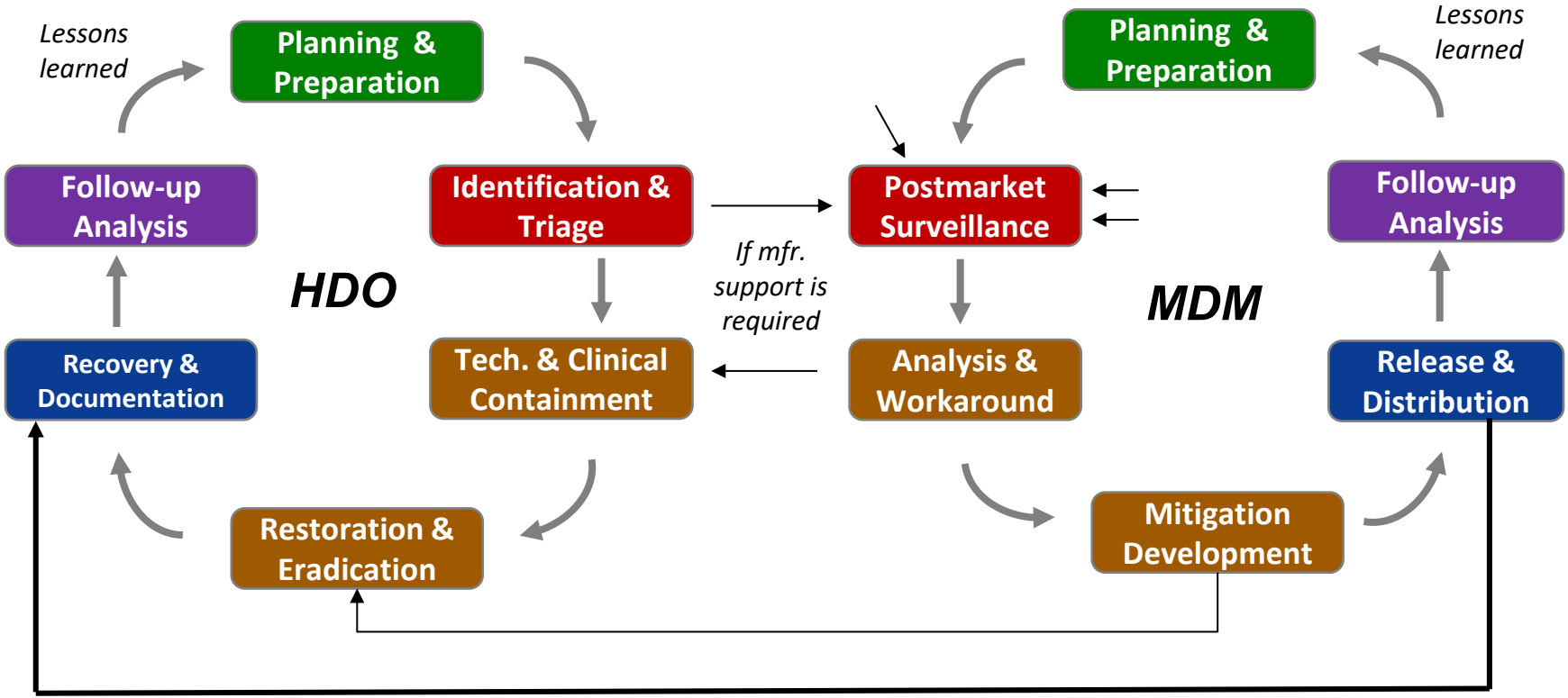
- May be asked for support
- May have contractual obligation
- May lead to vulnerability response or corrective action

Manufacturer (own infrastructure):

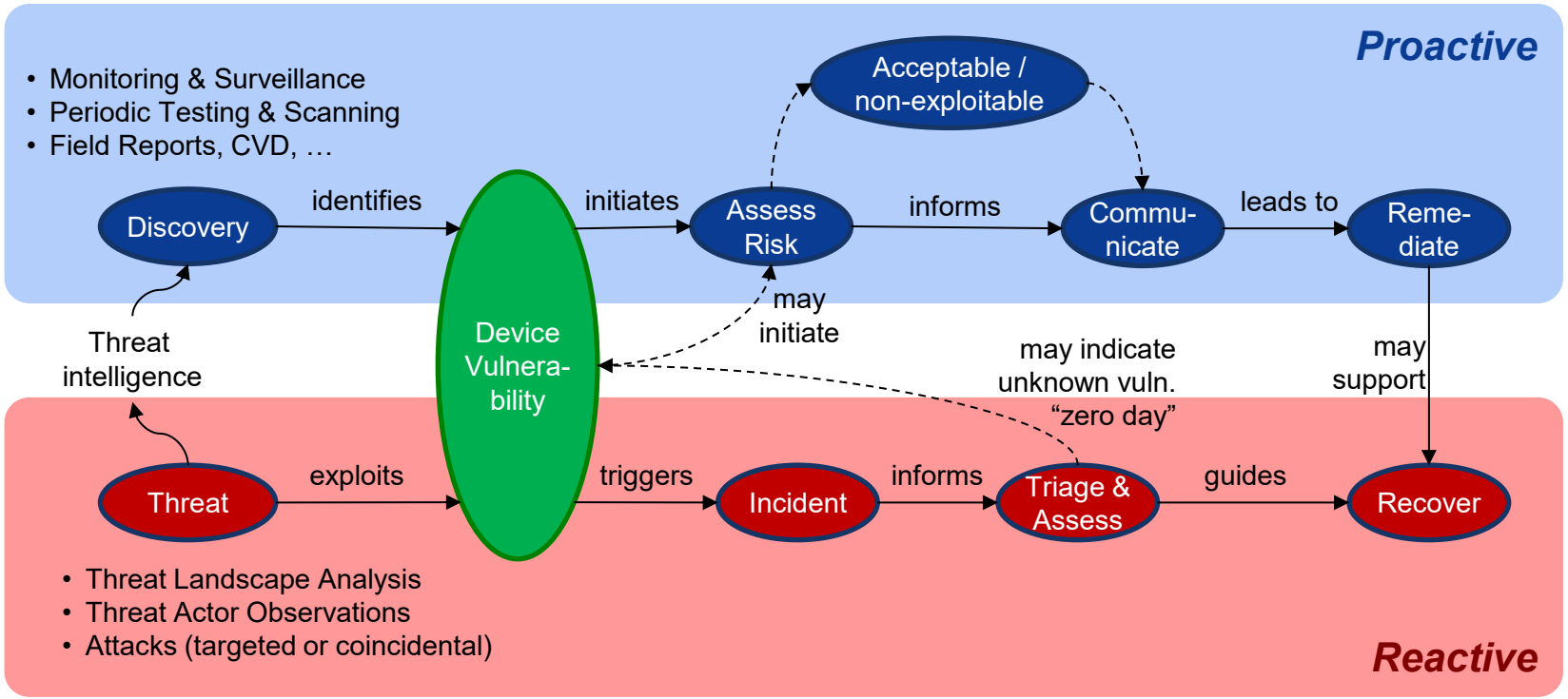
- Production (may lead to recall or product shortage notifications)
- Remote support infrastructure (may require customer notification)
- May impact customer or patient data (e.g. cloud hosting) and require HIPAA action

IR Example – Fielded Device Scenario

HDO Incident Response Process ↔ Mfr. Postmarket Management Process

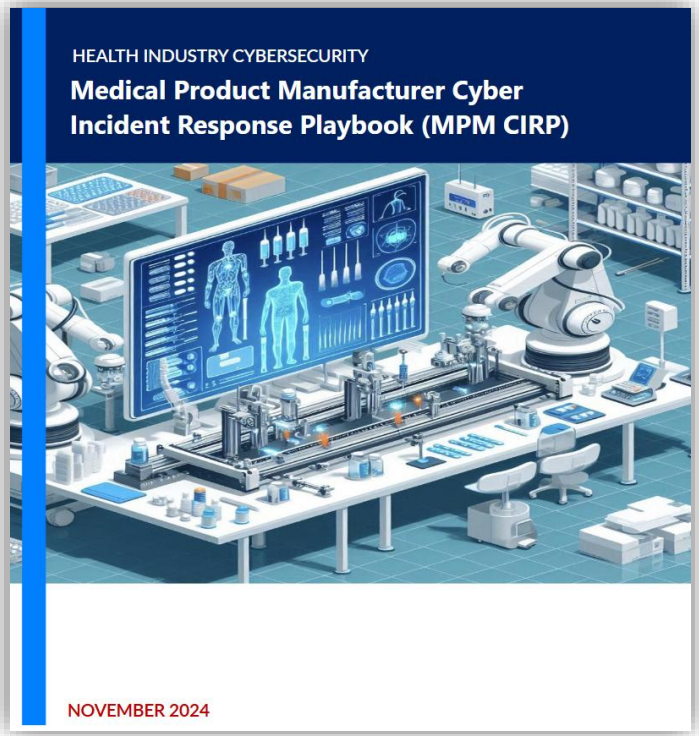


Postmarket Vulnerability Management Scenarios



Note – although they may be related, vulnerability management and incident response are different

IR Example – Production (OT) Scenario



Timely incident reporting to comply with statutory, regulatory, and contractual obligations.

General Federal:

- Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022 - report a “covered cyber incident” to CISA within 72 hours and report ransomware payment within 24 hours after payment.
- Securities and Exchange Commission (SEC) - report certain cyber incidents within 4 business days after determination.

Medical Product Regulatory Reporting:

- FDA Medical Device Reporting (MDR) 21 CFR part 803 - reporting of adverse events and product problems.
- FDA medical device corrections or removals (“voluntary recalls”) under 21 CFR part 806 - submit within 10 working days.
- Section 506J of the Federal Food, Drug, and Cosmetics Act - notify FDA of interruption, discontinuation for certain device types.

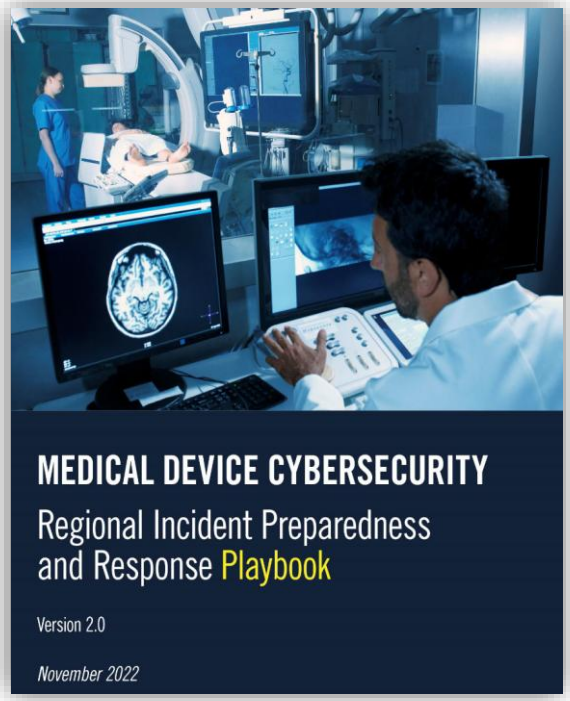
International Reporting Requirements

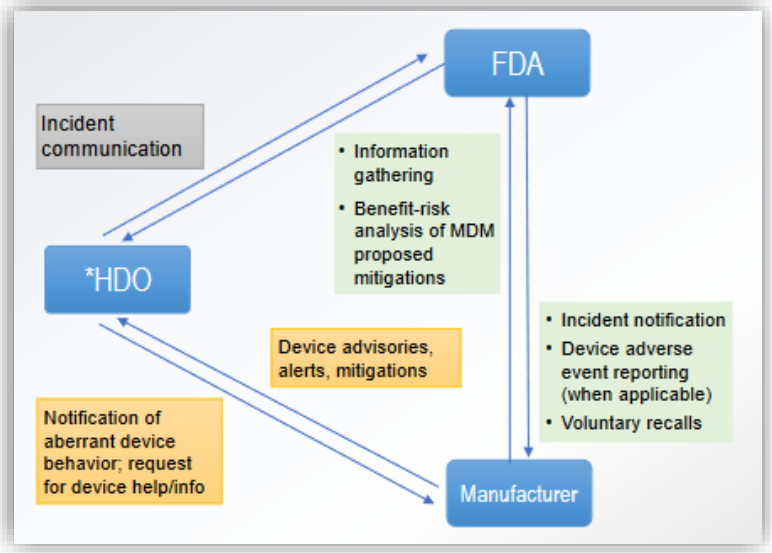
- E.g., a cyber incident causing interruption to the supply of a medical device within a European Union under Regulation (EU) 2024/1860

Cyber Insurance or Product Liability Insurance notification as applicable.

https://healthsectorcouncil.org/wp-content/uploads/2024/11/MEDICAL-PRODUCT-MANUFACTURING-CYBER-INCIDENT-RESPONSE-PLAYBOOK-2.pdf

Medical Device Incident Response (HDO-centric)





https://www.mitre.org/news-insights/publication/medical-device-cybersecurity-regional-incident-preparedness-and-response

IR & Notification Laws, Regulations, Guidances

- Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022
- FDA Medical Device Reporting (MDR) 21 CFR part 803
- FDA Medical Device Corrections or Removals (“voluntary recalls”) 21 CFR part 806
- Federal Food, Drug, and Cosmetics Act, Section 506J
- MedWatch Online Voluntary Reporting Form (for users)
- FDA Postmarket Cybersecurity Guidance
- CMS “Pub. 100-07 State Operations Provider Certification” (for operators)
- HIPAA Breach Notification Rule (45 CFR §§ 164.400-414)
- FTC Health Breach Notification Rule (16 CFR Part 318)
- European Union Regulation EU 2024/1860 – amendment of MDR/IVDR, establishes obligations to inform in case of interruption or discontinuation of supplies
- Other regional or industry-specific requirements may apply, e.g., critical infrastructure or personal data. Also, consider international requirements such as EU GDPR.

Thank you!

axel@medcrypt.com

Medical Device Cyber Incident Response

Additional References:

- MITRE: Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook
- ISO/IEC 27035: Information Security Incident Management ,
- NIST SP 800-61: Computer Security Incident Handling Guide
- NIST SP 800-83: Guide to Malware Incident Prevention and Handling
- NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-150: Guide to Cyber Threat Information Sharing
- NIST SP 800-184: Guide for Cybersecurity Event Recovery
- SANS: Creating and Managing an Incident Response Team
- CMSEI: Handbook for Computer Security Incident Response Teams (CSIRTs)
- ISACA: Incident Management and Response

Note – most IR frameworks and standards are for the typical IT environment and may need to be modified for the medical device case.

Further Incident Response Resources

- HHS: Healthcare System Cybersecurity - Readiness and Response Considerations
- HSCC: Medical Product Manufacturer Cyber Incident Response Playbook (MPM CIRP)
- HSCC: Health Industry Cybersecurity - Coordinated Healthcare Incident Response Plan
- HSCC: Health Industry Cybersecurity - Matrix of Information Sharing Organizations (HIC-MISO)
- HSCC: Operational Continuity - Cyber Incident (OCCI)
- HSCC: Medtech Vulnerability Communications Toolkit (MVCT)
- NIST: Cybersecurity Resources for Manufacturers
- FEMA: Planning Considerations for Cyber Incidents: Guidance for Emergency Managers
- CISA: Critical Manufacturing Sector
- World Economic Forum: Building a Culture of Cyber Resilience in Manufacturing
- World Economic Forum: Why using IT cybersecurity to protect OT puts industrial organizations at risk
- Centre for Cybersecurity (Belgium): Cyber Security Incident Management Guide