MEDICAL DEVICE CYBERSECURITY

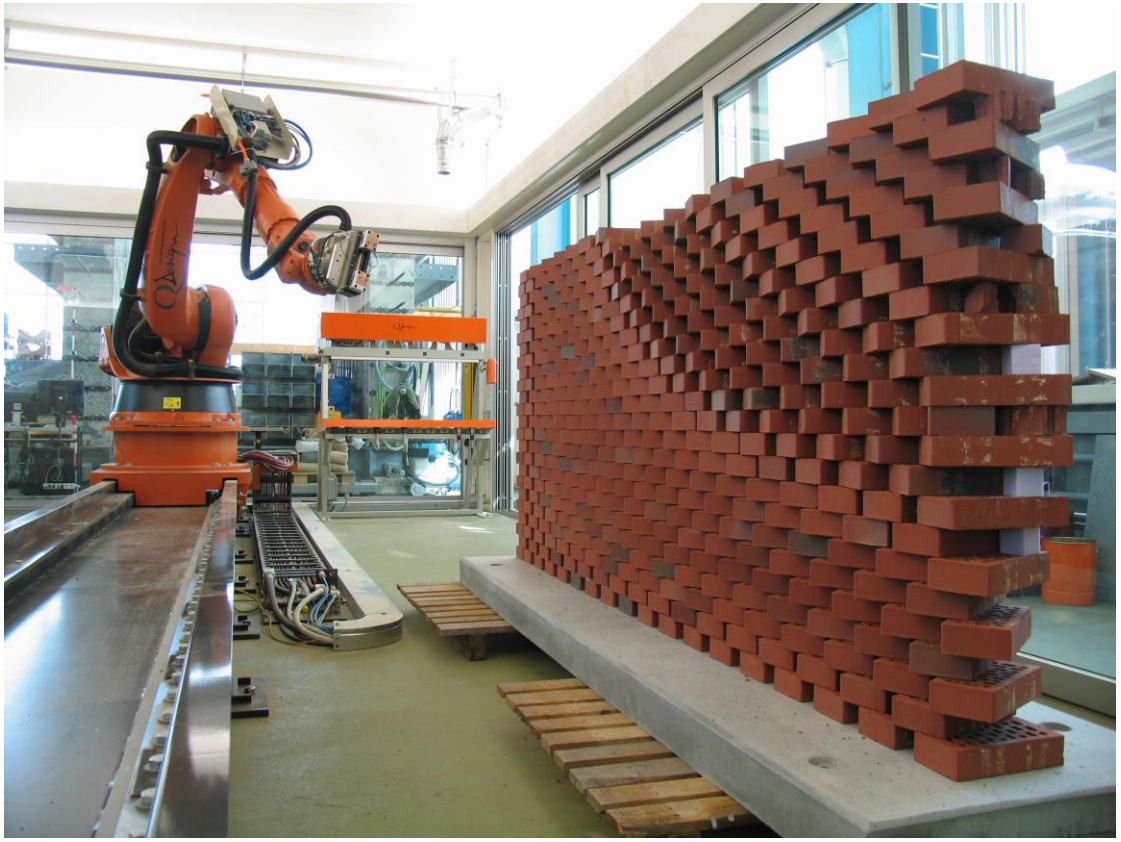
SETH D. CARMODY, PHD

APRIL 16, 2018

AMDM 2018 IVD SUBMISSIONS WORKSHOP

Intended Use + Misuse

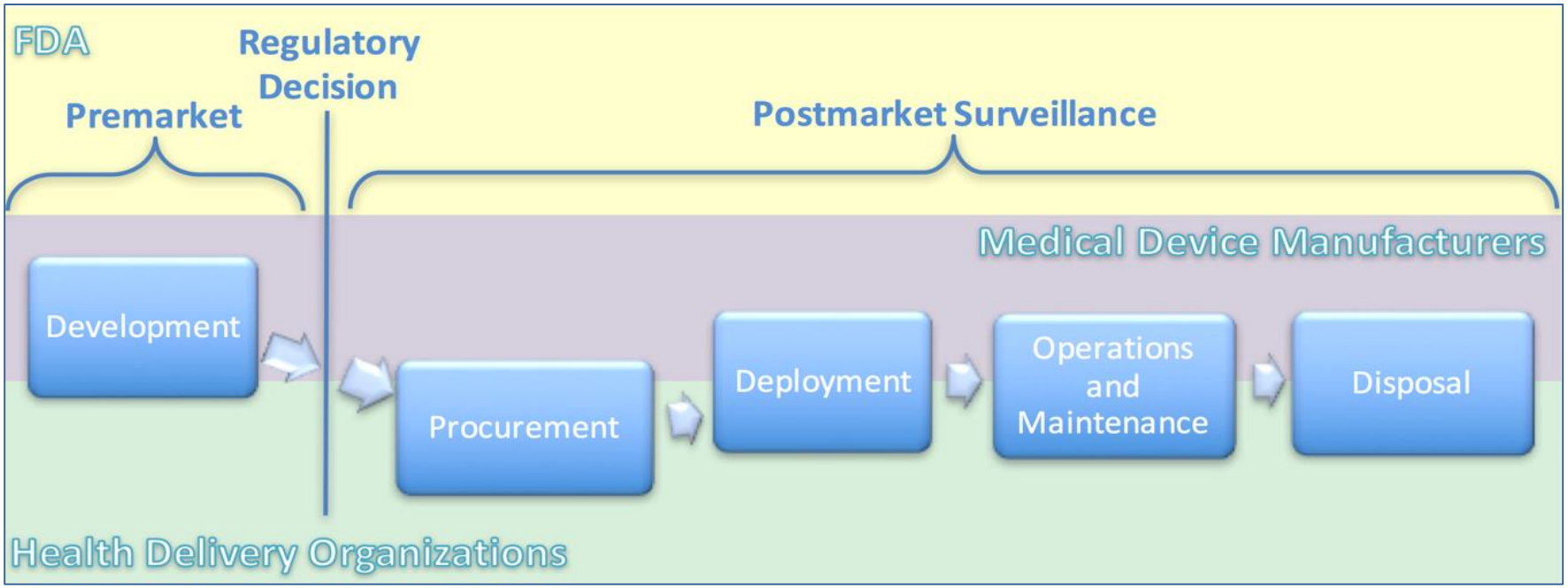
http://hackaday.com/2015/09/07/brick-laying-robot-does-it-better/



http://www.technologyvista.in/pin/here-comes-the-brick-laying-robot-to-make-buildings/

Negative Requirements are *Infinite*

Device Lifecycle: Ecosystem Challenges



Let's Play: Fact vs. Myth

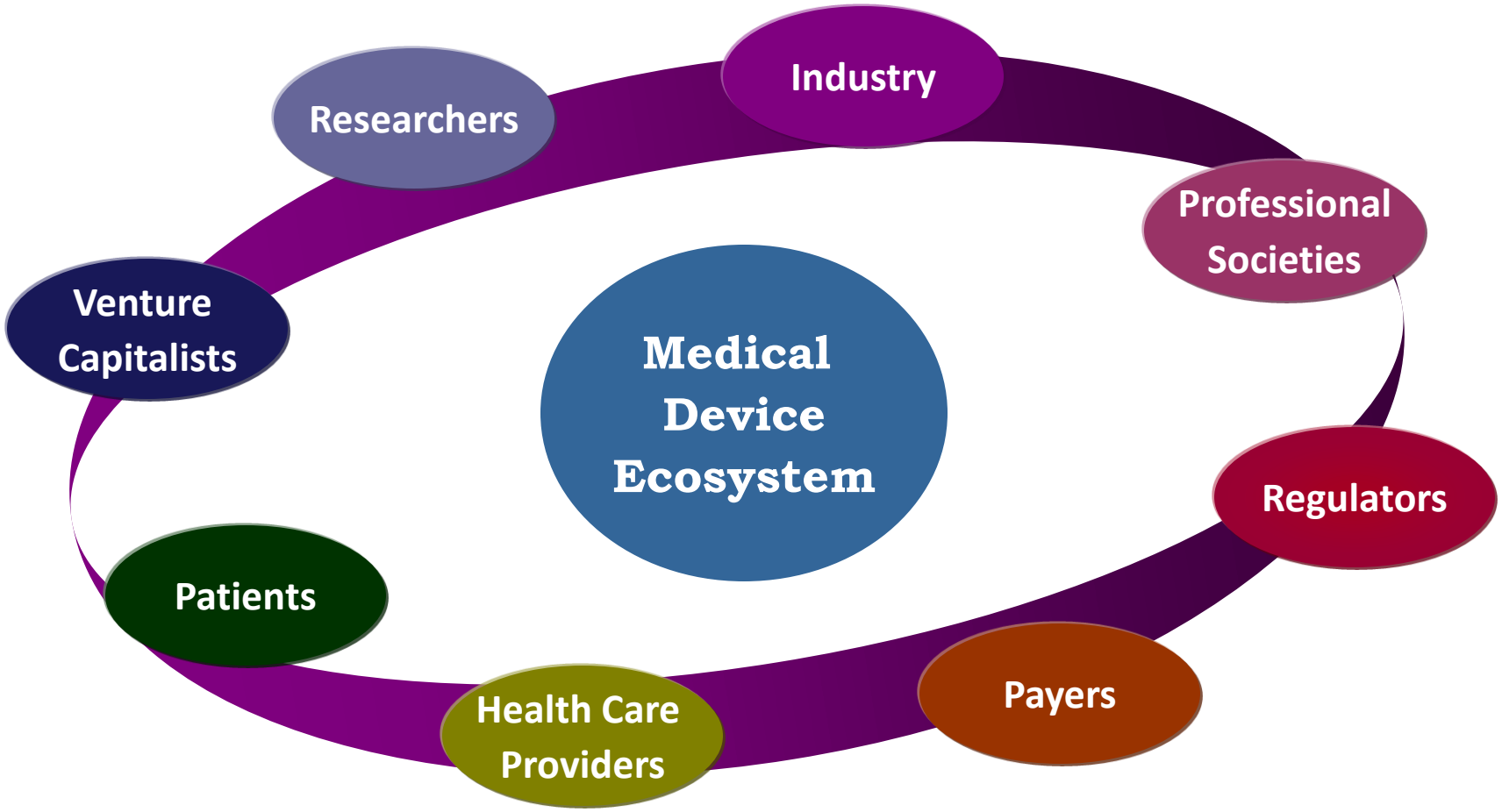
Fact vs. **Myth**

The FDA is the federal entity solely responsible for the cybersecurity of medical devices.

Myth

FACT: The FDA works closely with several federal government agencies including the U.S. Department of Homeland Security (DHS), members of the private sector, medical device manufacturers, healthcare delivery organizations, security researchers, and end users to increase the security of the U.S. critical cyber infrastructure.

A Complex Ecosystem



FDA Cybersecurity History

2013

Executive Orders
FDA Safety Communication
Draft Premarket Guidance
Begin Coordination with DHS
Recognize Standards
Establish Incident Response Team

2014

Final Premarket Guidance
MOU with NH-ISAC
Public Workshop

2015

Product-Specific Safety Comm
Build Ecosystem/Collaboration

2016

Draft and Final Postmarket Guidance
Public Workshop
MOU with NH-ISAC/MDISS

2017

Product-Specific Safety Comm

2018

1st Cybersecurity WL

2005: Issued guidance
2008: Halpern, et.al.

2009: Issued safety communication
2011: "Hacking" of implantable insulin pump (*Radcliffe*)
2012: First recall of vulnerable software (Roche - PC Anywhere)
2013: Recall of TNS-listener (Roche)

Premarket Cybersecurity Guidance

- Draft June 2013
- Final October 2014
- Key Principles:
  - #1 Shared responsibility between stakeholders, including health care facilities, patients, providers, and manufacturers of medical devices
  - #2 Address cybersecurity during the design and development of the medical device
  - #3 Establish design inputs for device related to cybersecurity, and establish a cybersecurity vulnerability and management approach as part of the software validation and risk analysis that is required by 21 CFR 820.30(g)

Let's Play: Fact vs. Myth

Fact vs. **Myth**

Cybersecurity for medical devices is optional.

Myth

FACT: Medical device manufacturers must comply with federal regulations. Part of those regulations, called quality system regulations (QSRs), requires that medical device manufacturers address all risks, including cybersecurity risk. The pre- and post- market cybersecurity guidances provide recommendations for meeting QSRs.

Let's Play: Fact vs. Myth

Fact vs. **Myth**

The FDA does not conduct premarket testing for any medical products.

FACT

Myth: The FDA tests for cybersecurity of medical devices.

Key Principles of FDA Postmarket Management of Cybersecurity in Medical Devices

- Use a risk-based framework to assure risks to public health are addressed in a continual and timely fashion
- Articulate manufacturer responsibilities by leveraging existing Quality System Regulation and postmarket authorities
- Foster a collaborative and coordinated approach to information sharing and risk assessment
- Align with Presidential EOs and NIST Framework
- Incentivize the “right” behavior

Let's Play: Fact vs. Myth

Fact vs. **Myth**

Medical device manufacturers can't update medical devices for cybersecurity.

Myth

FACT: Medical device manufacturers can always update a medical device for cybersecurity. In fact, the FDA does not typically need to review changes made to medical devices solely to strengthen cybersecurity

Let's Play: Fact vs. Myth

Fact vs. **Myth**

Health care Delivery Organizations (HDOs) can't update and patch medical devices for cybersecurity.

Myth

FACT: The FDA recognizes that HDOs are responsible for implementing devices on their networks and may need to patch or change devices and/or supporting infrastructure to reduce security risks. Recognizing that changes require risk assessment, the FDA recommends working closely with medical device manufacturers to communicate changes that are necessary.

Postmarket Cybersecurity Risk Assessment

Assessing Exploitability with Common Vulnerability Scoring System (CVSS)

- **Establish a repeatable process by leveraging existing frameworks (e.g. CVSS)**

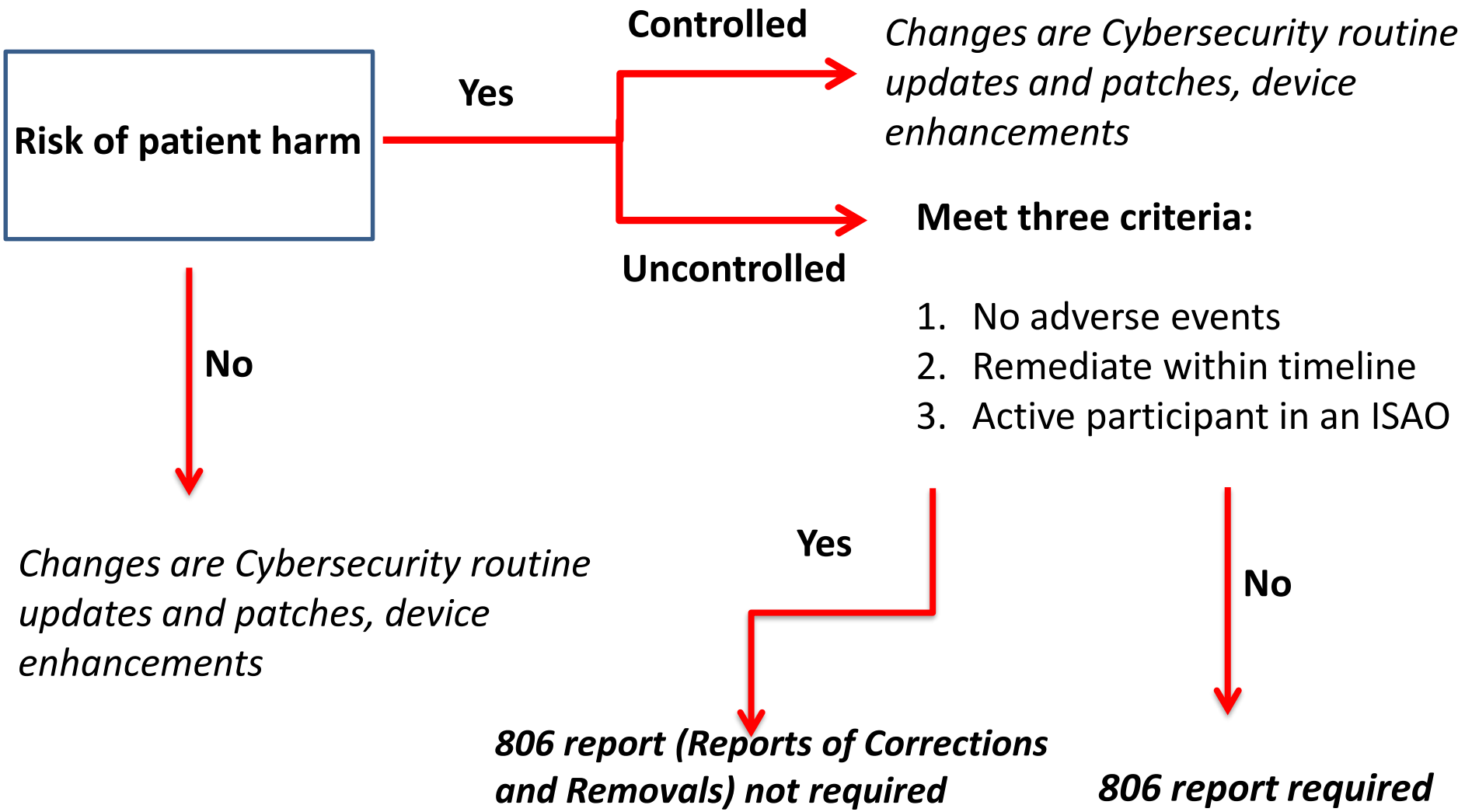
Base Scoring (risk factors of the vulnerability)
e.g. Attack Vector (physical, local, adjacent, network)

Temporal Scoring (risk factors that change over time)
e.g. Exploit Code Maturity (high, functional, proof-of-concept, unproven)

Environmental scoring (controls that reduce risk)
e.g. Physical, software, network, compensating controls.

CVSS – Common Vulnerability Scoring System https://www.first.org/cvss

Changes to a Device for Controlled vs. Uncontrolled Risk



Distinguishing Medical Device Recalls from Medical Device Enhancements

ISAO (Information Sharing and Analysis Organization)

Questions?

Contacts:

CDRH mailbox, CyberMed@fda.hhs.gov
Suzanne Schwartz, Suzanne.Schwartz@fda.hhs.gov
Aftin Ross, aftin.ross@fda.hhs.gov
Seth Carmody, seth.carmody@fda.hhs.gov