ENISA 5 e-Health Security Conference

Martha De Cunha Maluf-Burgman
QA Reg. Affairs Program Manager for RF & Cybersecurity

30 October, 2019
Medtronic

Medtronic
Further, Together

CYBERSECURITY AND PROCUREMENT FOR HEALTHCARE ORGANISATIONS

VENDOR PERSPECTIVE

AGENDA

- Definition of procurement and vendor perspective
- Necessary gear to ensure MD security and challenges
- Cybersecurity during entire lifecycle of devices
- Guidances, regulations and standards harmonised and coordinated by HCAs and Manufacturers

CYBERSECURITY AND PROCUREMENT FOR HEALTHCARE ORGANISATIONS
VENDOR PERSPECTIVE

What is procurement?

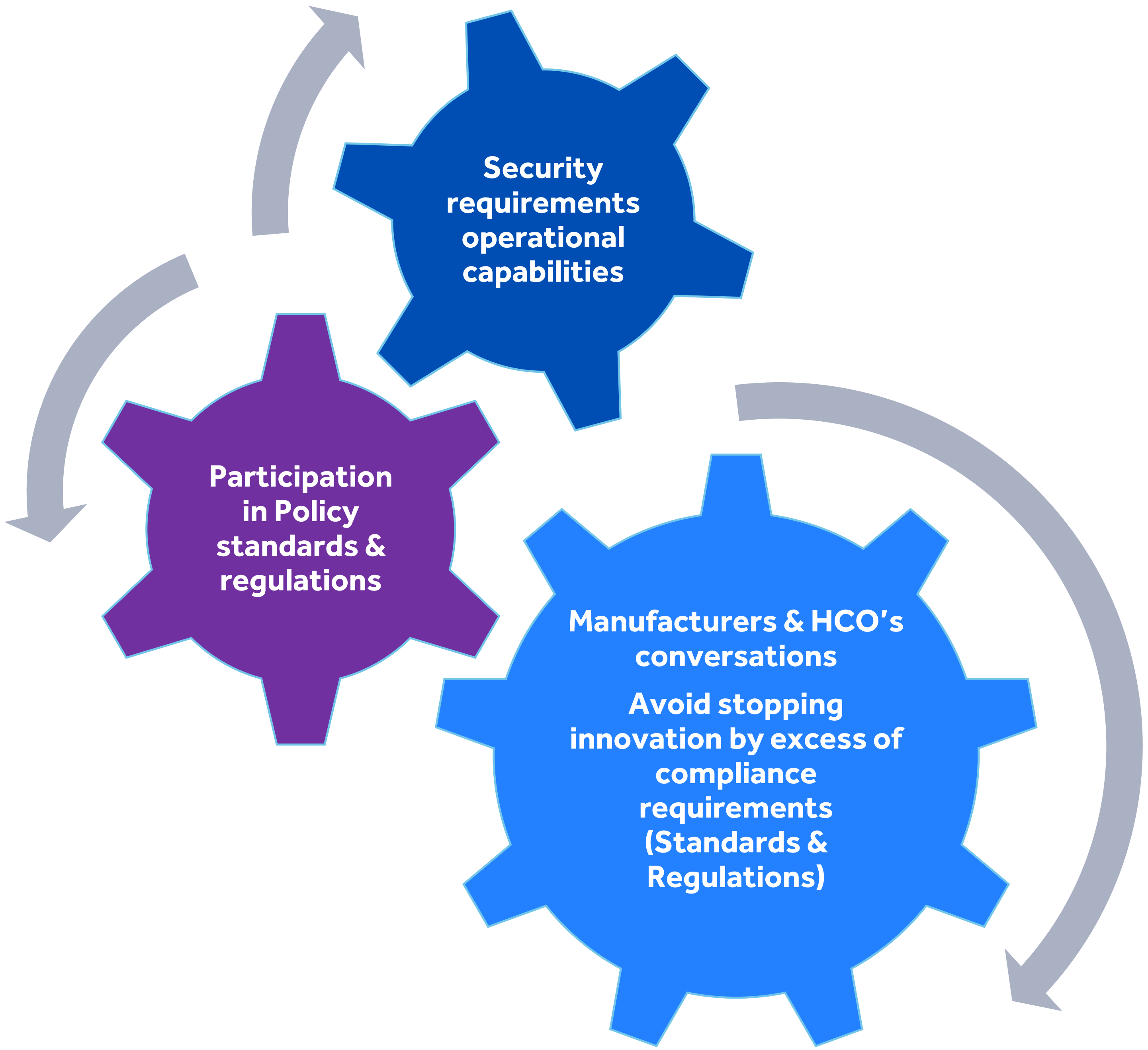
- ❖ Procurement is the process of selecting vendors, strategic vetting, establishing payment terms, selection, contracts negotiation, and final purchasing of goods. Procurement deals with acquiring all the goods, services, and work that is important to an organization.
- ❖ Effective procurement needs effective commissioning guidelines as well as a transparent and open process in which to apply to provide services and goods.

Challenges in Healthcare procurement

Healthcare procurement involves many hidden costs	The core of HC procurement spending is the cost of the product, but HCOs should be aware of invisible costs associated with the procurement, such as inventory holding, distribution expenses, cybersecurity requirements. Understanding the costs behind utilization, internal distribution, inventory holding, and special deliveries will not only yield savings but will also enhance clinician and patient satisfaction.
Medical equipment procurement	Generally, medical equipment is produced in high volumes with standard specifications. However, customization in specifications to meet the specific needs increases the medical equipment procurement cost. The manufacture of such specific products may result in errors as the companies struggle to meet the demands of the end users within the stipulated time frame.

MAIN CONSIDERATIONS ON PROCUREMENT

GEAR THAT WORKS


Security requirements operational capabilities
Participation in Policy standards & regulations
Manufacturers & HCO's conversations
Avoid stopping innovation by excess of compliance requirements (Standards & Regulations)

- ENSURE good practices on cybersecurity in procurement. Beneficial for the industry

- HCO are starting to send security questionnaires on a variety of topics, including, patches, bill of materials, IT Requirements, etc. Many manufacturers respond proactively to these inquiries

- CHALLENGE: Different formats used by the hospitals and by the countries CAs. Harmonisation of format questionnaires across borders is necessary.

- CONVERSATION with HCOs and manufacturers are needed to determine the best way to support this need for information. The end of support for a product have risks associated, representing a liability from the cybersecurity standpoint. E.g. Microsoft's management of products for a period of time, and when they drop support, they give a standard support plan for extended time, if needed.

- Manufacturers are being transparent to cyber staff and answering questionnaires from the HCO.
  - E.g. Diabetes pumps are never in a hospital network for example, so the questionnaires are not applicable to these kind of products.
  - Patching plan or patching schedule will be provided to HCO's . Manufacturers get approval from the CA, and proactive post market security requirements that we need to follow and comply.

MAIN CONSIDERATIONS ON PROCUREMENT

- HCOs and medical device manufacturers can benefit from working towards a common set of security expectations.
- This can be facilitated by the use of a common procurement language and guidelines to ensure security is integrated into medical devices and systems.
    - E.g. The US Department of Homeland Security (DHS) developed the cybersecurity procurement language for control systems. The document provides an introduction to control systems and outlines escalating risk to control systems and security objectives with a control systems perspective. A similar approach for medical devices could provide specification language for use in procurement specifications, covering all aspects of cybersecurity, including acceptance testing, verification, integration, maintenance guidance and any supporting references (guidelines, regulation or standards).

Source: .Department of Homeland Security (DHS), "Cyber Security Procurement Language for Control Systems," 09 September 2016. https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_ Language_Rev4_100809_S508C.pdf

- HCOs have the opportunity to stipulate baseline practices and for vendors to demonstrate adoption of secure development processes, device or system hardening and lifecycle management. E.g. Cybersecurity standards developed for industrial control systems vendors and their products (IEC 62443-4-1 and IEC 62443-4-2) can be used to set expectations for supplier secure product development processes and embedded device security assurance.

SUMMARY OF CHALLENGES

1. Lack of harmonised procurement requirements –> One single format and unified procurement language

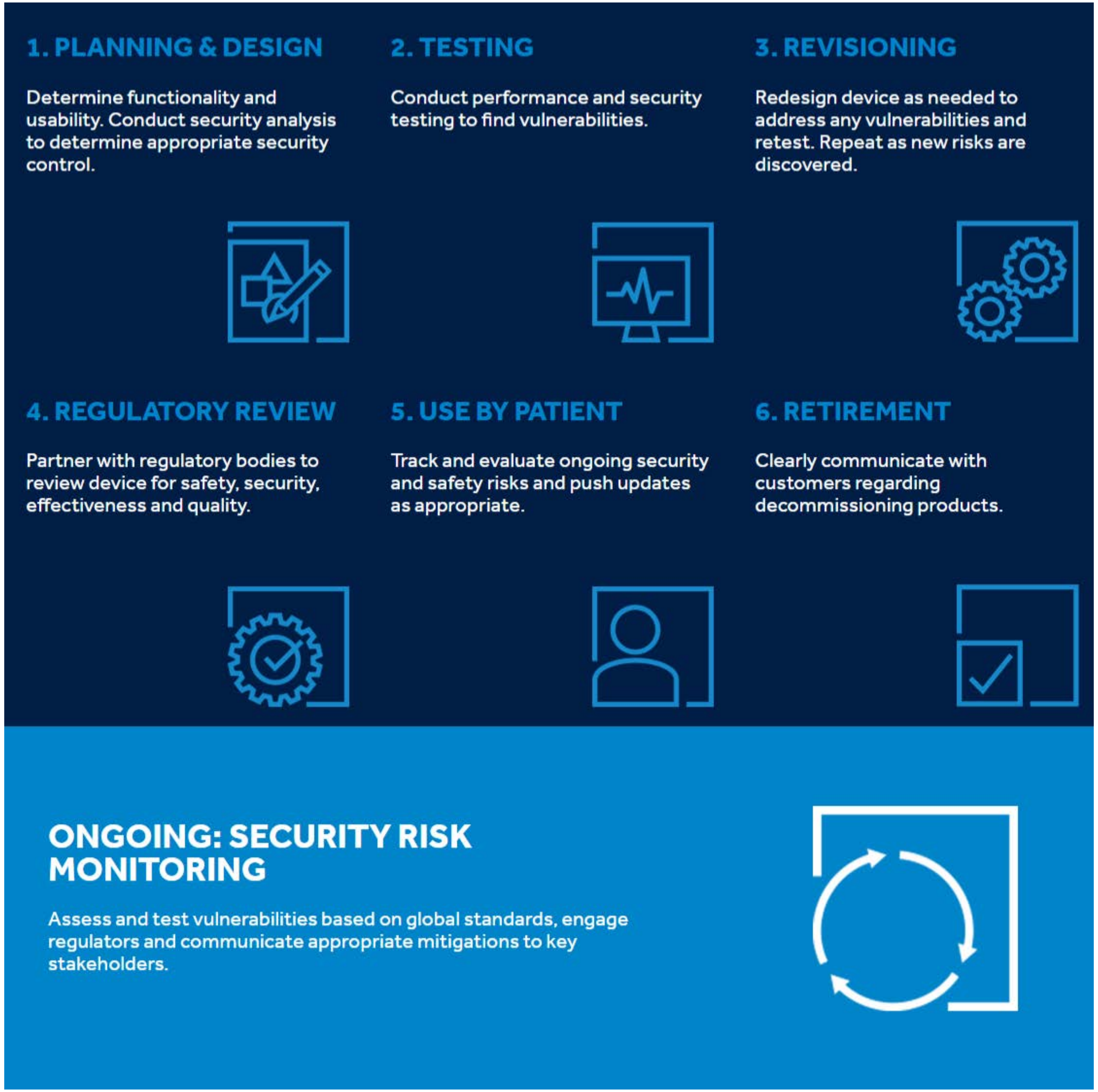
2. End of support of product. Represents **Liability Risk**

3. Customization in security specifications to meet the specific needs **increases the Medical equipment procurement costs**

SECURITY FOR LIFE

MANAGING SECURITY THROUGHOUT PRODUCT LIFECYCLE

Security is maintained from development to decommissioning with ongoing security risk monitoring



1. PLANNING & DESIGN

Determine functionality and usability. Conduct security analysis to determine appropriate security control.

2. TESTING

Conduct performance and security testing to find vulnerabilities.

3. REVISIONING

Redesign device as needed to address any vulnerabilities and retest. Repeat as new risks are discovered.

4. REGULATORY REVIEW

Partner with regulatory bodies to review device for safety, security, effectiveness and quality.

5. USE BY PATIENT

Track and evaluate ongoing security and safety risks and push updates as appropriate.

6. RETIREMENT

Clearly communicate with customers regarding decommissioning products.

ONGOING: SECURITY RISK MONITORING

Assess and test vulnerabilities based on global standards, engage regulators and communicate appropriate mitigations to key stakeholders.

CYBERSECURITY PRACTICES - PROCUREMENT

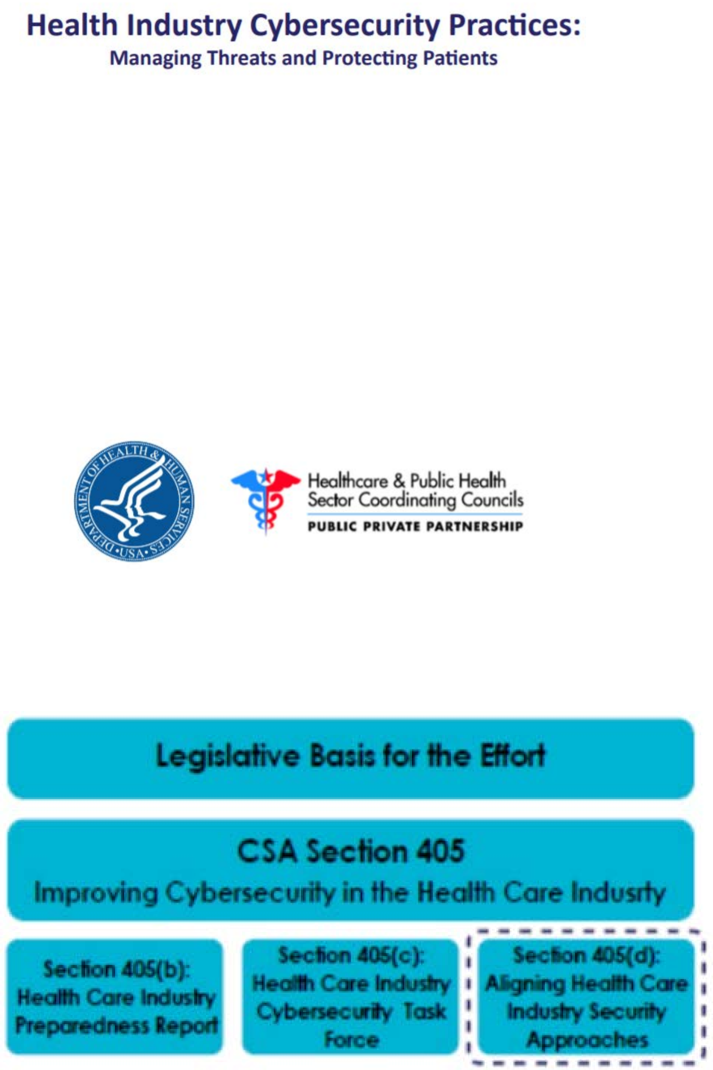
FACTS: increasingly sophisticated and widespread nature of cyber-attacks.

ACTIONS: the health care industry must make cybersecurity a priority and make the investments needed to protect its patients.

Cybersecurity requires mobilization, **cooperation and coordination** of resources across myriad public and private stakeholders, including hospitals, IT vendors, medical device manufacturers, and governments (state, local, tribal, territorial, and federal) to mitigate the risks and minimize the impacts of a cyber-attack.

E.g. The U.S. Department of Health and Human Services (HHS) and the Health Care and Public Health (HPH, Health Sector, Health Care Industry) sector are working together to address these challenges.

Other CA's are also taking actions.



Health Industry Cybersecurity Practices:
Managing Threats and Protecting Patients

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP
Legislative Basis for the Effort
CSA Section 405
Improving Cybersecurity in the Health Care Indusrty
Section 405(b): Health Care Industry Preparedness Report
Section 405(c): Health Care Industry Cybersecurity Task Force
Section 405(d): Aligning Health Care Industry Security Approaches

Figure 1. Section 405(d) is Part of CSA Section 405, Which Focuses on the U.S. Health Care Industry

Small Organisations	
Practice	**Sub-Practice**
5 – Asset Management	5.S.A Inventory
	5.S.B Procurement
	5.S.C. Decommissioning
Medium Organisations	
5- Assess Management	5.M.A. Inventory of Endpoints and Servers
	5.M.B. Procurement
	5.M.C. Secure Storage for Inactive Devices
	5.M.D. Decommissioning Assets.
Large Organizations	
9- Medical Device Security	9.L.A Vulnerability Management
	9.L.B Security Operations and Incident Response
	9.L.C Procurement and Security Evaluations
	9.L.D Contacting the FDA

Source: https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

TAKEAWAYS

- **Necessary to establish a MD procurement best practices**, by integrating MD procurement process, including cooperation between HCOs and manufacturers, who should provide documentation describing in detail their cybersecurity/penetration testing process as well as program details for patching, incident response and secure set up and configuration. Ensure security during the entire lifecycle of MDs.

- **HCO’s procurement team in open dialogue with vendor/manufacturers, via collaboration**. Ensure the right people are engaged and have ownership of the process.The relevant medical device subject matter experts from the vendor’s product teams need to be engaged to provide the requested information.

- **Leverage industry available resources** rather than developing and providing unique questionnaires to your device vendors, use publicly-available industry resources (e.g., Manufacturer Disclosure Statement for Medical Device Security –MDS2). Suppliers should provide documentation of processes and technology for external access, including security (authentication & authorization) and monitoring, as well as Bill of Materials (BoMs).

- **Standards:** Nowadays there are a lot of sources of standards/ regulations, and manufacturers are working to harmonize these standards and deploy across their organizations to ensure compliance and also availability of these devices to critical markets.