EUROPEAN UNION AGENCY
FOR CYBERSECURITY

PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS

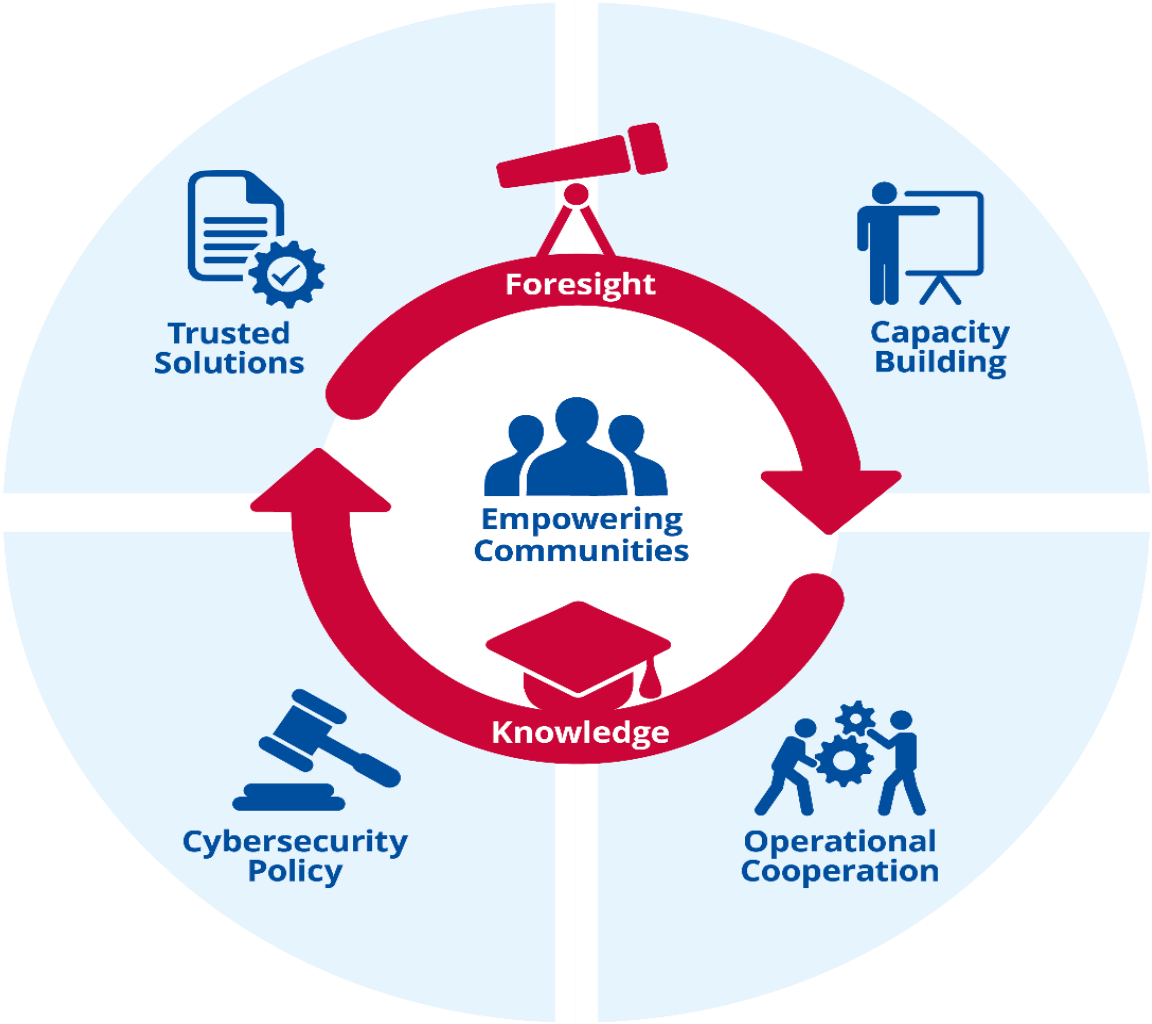
Dimitra Liveri
NIS Expert

16 | 12 | 2020

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

A TRUSTED AND CYBER SECURE EUROPE

Our mission is to achieve **a high common level of cybersecurity** across the Union in cooperation with the wider community



HEALTHCARE UNDER ATTACK

- 150+ countries
- 230K+ computers
- Significant impact on NHS!
  - Computers
  - MRI scanners
  - Blood storage refrigerators
  - Etc…

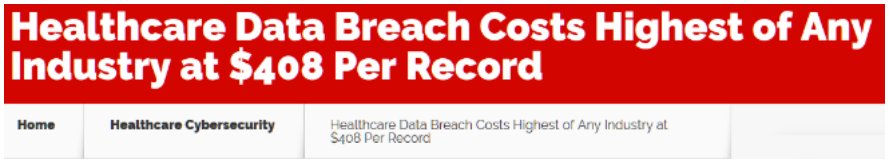
EHEALTH CYBERSECURITY – SITUATIONAL ANALYSIS

- **200%** increase in software supply chain attacks
- **600%** increase of attacks on IoT devices, 29% on ICS
- **46%** increase in ransomware variants
- Surge in crypto-mining malware hijacking processing power

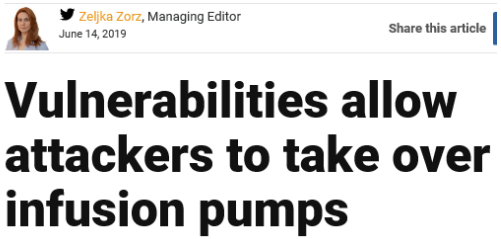
Source: Infoblox - Cybersecurity in Healthcare, 2019

- **Confidence** in response: **92%** up from **82%** two years ago
- **Patching**: **87%** claim to frequently patch systems
- **Investment**: More healthcare organizations (28%) are spending **11-20% more** on cybersecurity than in 2017
- **Outdated systems**: Number of devices running on Windows XP has fallen from **1 in 5** to **1 in 10**

Source: Infoblox - Cybersecurity in Healthcare, 2019



Source: IBM, Cost of a Data Breach, 2018



Source: Kaspersky, 2018

EHEALTH – ENISA ACTIVITIES

December 2015

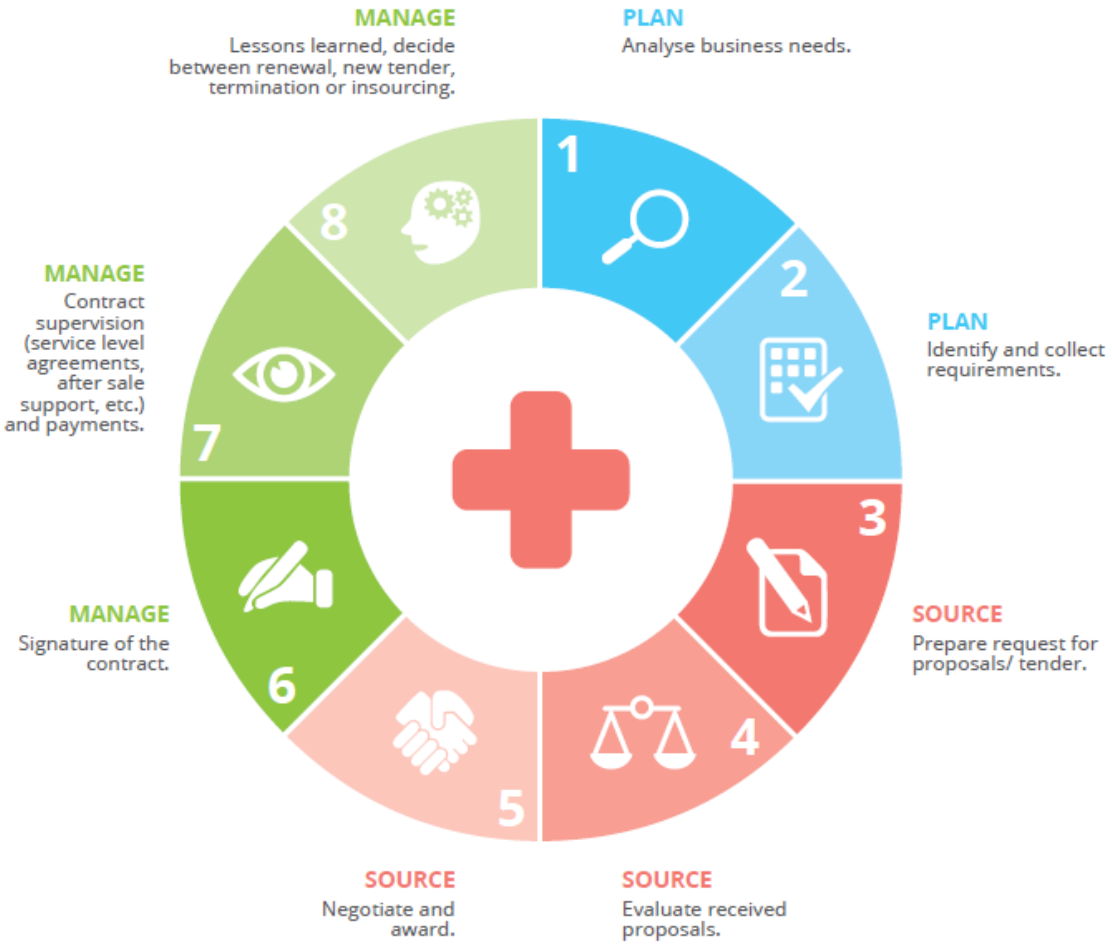
November 2016

February 2020

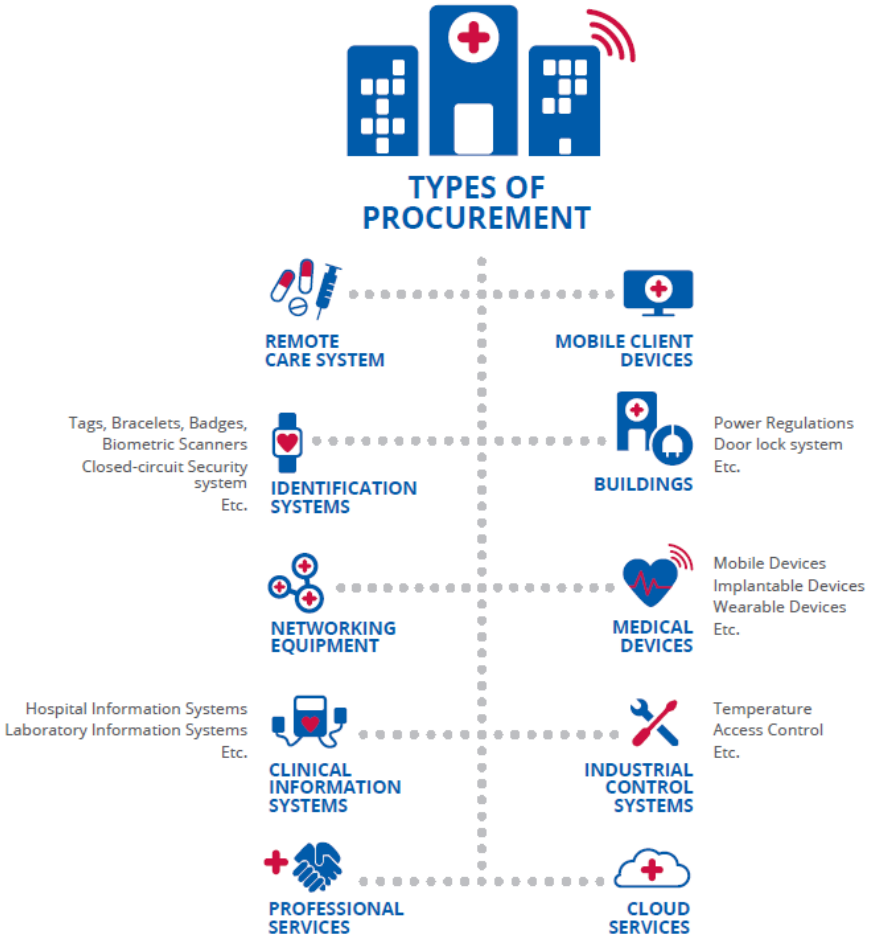
PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS

- Target audience: healthcare organisations/hospitals
- Entire applicable procurement scope of a healthcare organisation (products, services, infrastructure etc.)
- Interviews with healthcare organisations and other stakeholders
- Stock-taking of existing guidelines/regulations

CYCLE OF PROCUREMENT



TYPES OF PROCUREMENT



POLICY CONTEXT, STANDARDS AND GUIDELINES

CYBERSECURITY CHALLENGES IN PROCUREMENT

Clinical Information Systems

- Component vulnerability
- Increasing interoperability
- Full continuous operation

Medical Devices

- Manufacturing processes
- Rented equipment
- Legacy devices
- Hidden functionalities
- Update / lifecycle management

Buildings / ICS

- IoT / hybrid solutions

Networking

- Unprotected protocols

Professional Services

- Human factors
- Patient safety

THREAT TAXONOMY

GOOD PRACTICES FOR CYBERSECURITY IN PROCUREMENT

Organisational Practices

- Involve the IT department in procurement
- Asset inventory / configuration management
- Vulnerability identification and management
- Develop incident response plans
- Risk assessment as part of procurement
- Establish testing policies
- Threat identification for products/services
- Establish Business Continuity plans
- DPIA for new products/services
- Establish eligibility criteria for suppliers
- Raise cybersecurity awareness among staff
- Policy for hardware and software updates
- Provide training to staff / external consultants
- Plan network, HW and license requirements

GOOD PRACTICES FOR CYBERSECURITY IN PROCUREMENT

Technical Practices

Require cybersecurity certification	Allow auditing and logging
Determine network requirements	Schedule / monitor maintenance operations
Segregate your network	Involve supplier in incident management
Keep legacy systems/machines connected	Penetration testing frequently or after change
Take into account interoperability issues	Dedicated RFP for procuring Cloud Services
Access control for medical device facilities	Minimise / control remote access
Security controls for wireless communication	Encrypt sensitive data at rest / in transit
Enable testing of all components	Require patching for all components

CONCLUSIONS

- New regulations, policies and standards are setting the framework
- Procurement goes beyond the RfP when it comes to cybersecurity
- Staff awareness/training is key
- Cybersecurity is a consideration for the entire lifecycle
- Suppliers should be involved in post-procurement stages (e.g. incident response, patching, vulnerability disclosure)
- Next for ENISA: Cloud security for Healthcare services

THANK YOU FOR YOUR ATTENTION

European Union Agency for Cybersecurity
Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europa.eu