enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

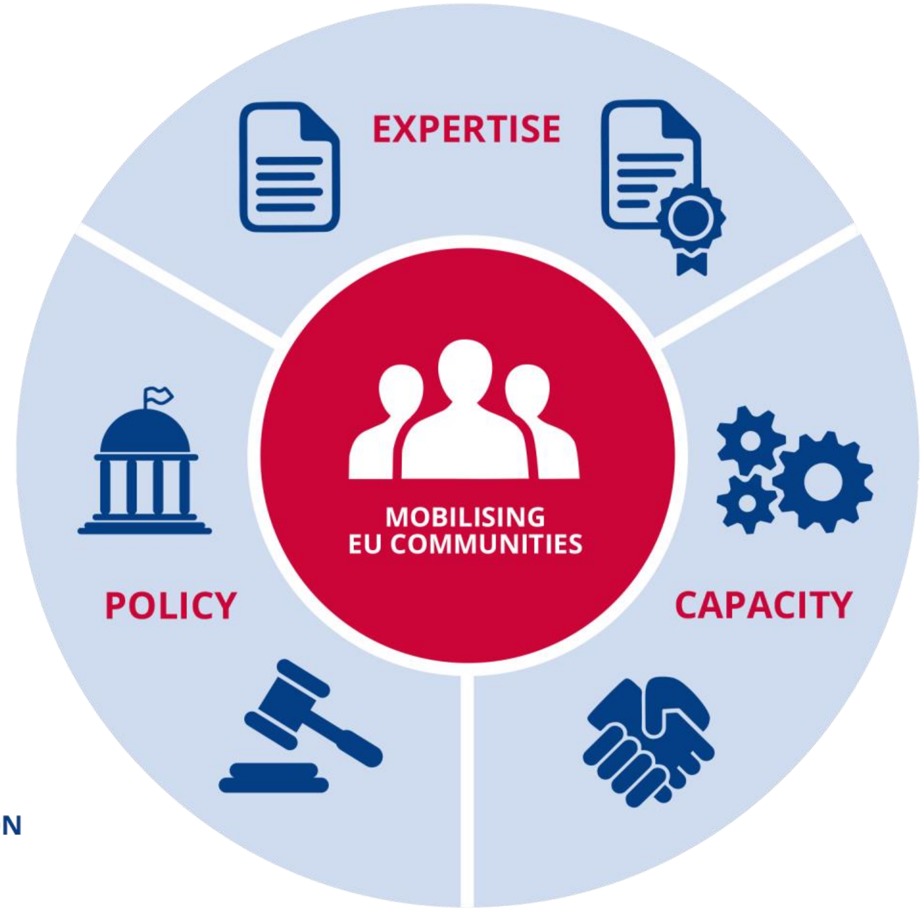
PROCUREMENT GUIDELINES FOR CYBERSECURITY IN HOSPITALS

D. Athanasios Drougkas
NIS Expert

5th eHealth Security Conference

30 | 10 | 2019

POSITIONING ENISA'S ACTIVITIES



1

RECOMMENDATIONS
ON CYBER SECURITY
AND INDEPENDENT
ADVICE

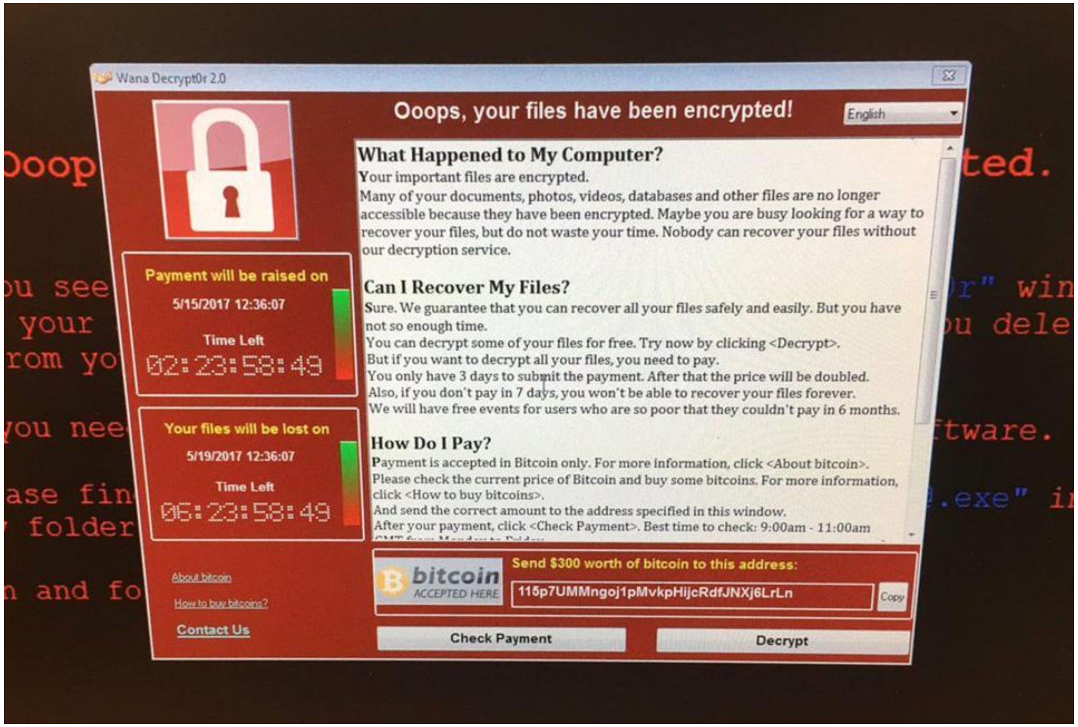
2

SUPPORT
MS & EC IN POLICY
IMPLEMENTATION
AND HARMONISATION
ACROSS EU

3

'HANDS-ON' WORK,
COLLABORATING WITH
OPERATIONAL TEAMS
THROUGHOUT EUROPE

HEALTHCARE UNDER ATTACK



Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 12:36:07
Time Left
02:23:58:49

Your files will be lost on
5/19/2017 12:36:07
Time Left
06:23:58:49

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

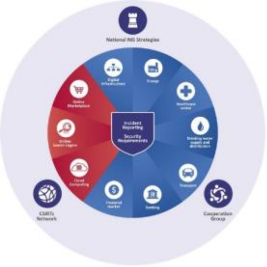
How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

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

EHEALTH CYBERSECURITY – SITUATIONAL ANALYSIS

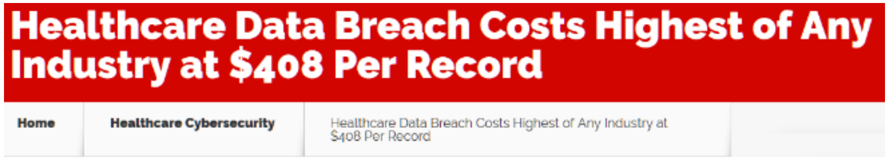


- **200%** increase in software supply chain attacks
- **600%** increase of attacks on IoT devices, 29% on ICS
- **46%** increase in ransomware variants
- Surge in crypto-mining malware hijacking processing power

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**

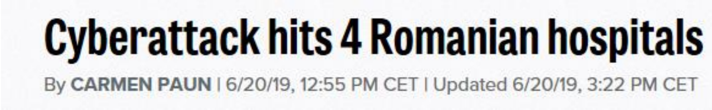
Source: Infoblox - Cybersecurity in Healthcare, 2019



Healthcare Data Breach Costs Highest of Any Industry at $408 Per Record

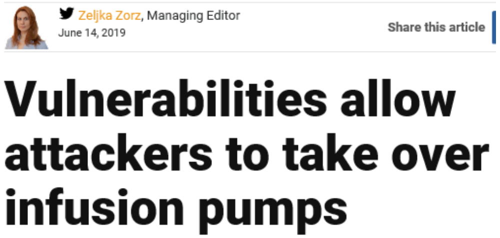
Home | Healthcare Cybersecurity | Healthcare Data Breach Costs Highest of Any Industry at $408 Per Record

Source: IBM, Cost of a Data Breach, 2018



Cyberattack hits 4 Romanian hospitals

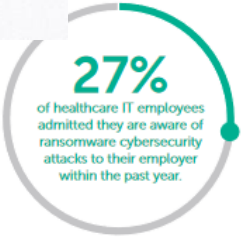
By CARMEN PAUN | 6/20/19, 12:55 PM CET | Updated 6/20/19, 3:22 PM CET



Zeljka Zorz, Managing Editor
June 14, 2019

Share this article

Vulnerabilities allow attackers to take over infusion pumps



Source: Kaspersky, 2018

EHEALTH – ENISA ACTIVITIES

December 2015

enisa

Security and Resilience in eHealth

Security Challenges and Risks

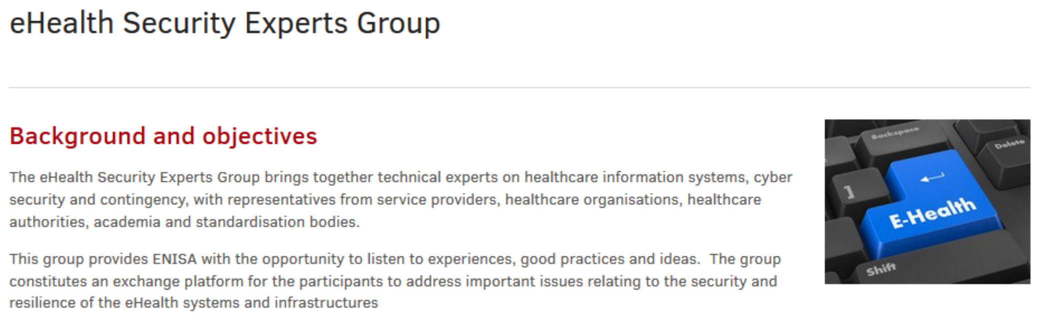
November 2016

enisa

Smart Hospitals

Security and Resilience for Smart Health Service and Infrastructures

NOVEMBER 2016



eHealth Security Experts Group

Background and objectives

The eHealth Security Experts Group brings together technical experts on healthcare information systems, cyber security and contingency, with representatives from service providers, healthcare organisations, healthcare authorities, academia and standardisation bodies.

This group provides ENISA with the opportunity to listen to experiences, good practices and ideas. The group constitutes an exchange platform for the participants to address important issues relating to the security and resilience of the eHealth systems and infrastructures

EHEALTH EXPERTS GROUP

SPMS EPE

УСБАЛО

Estonian Health Insurance Fund

Kela

SIEMENS

PHILIPS

IBM

kav wiener krankenanstalten verbund
Vienna Hospital Association

E-HEALTH
Estonian e-Health Foundation

Roche

Croatian Health Insurance Fund

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

NHS Digital

eHälso myndigheten

ppshp POHJOIS-POHJANMAAN SAIRAANHOITOPIIRI

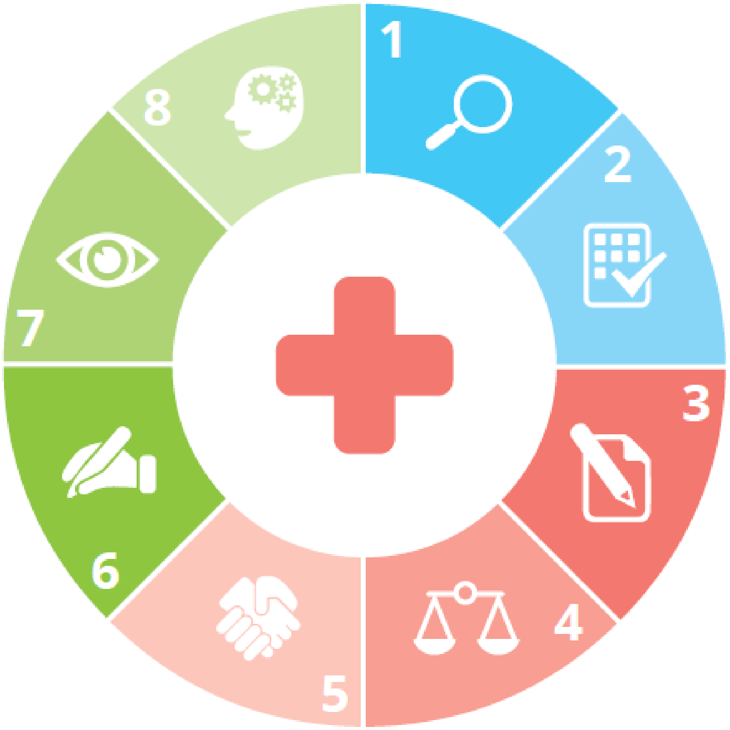
SaludMadrid Hospital Clínico San Carlos

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

ENISA 2019 REPORT

- **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



PLAN
Analyse business needs.

PLAN
Identify and collect requirements.

SOURCE
Prepare request for proposals/ tender.

SOURCE
Evaluate received proposals.

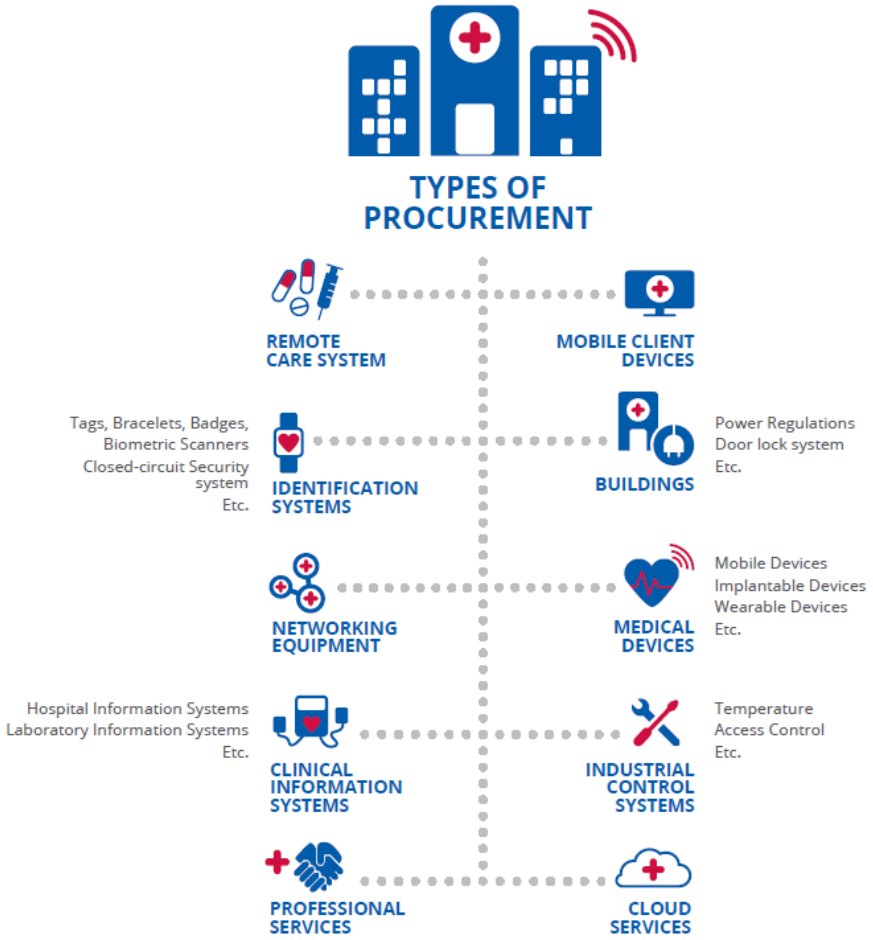
SOURCE
Negotiate and award.

MANAGE
Signature of the contract.

MANAGE
Contract supervision (service level agreements, after sale support, etc.) and payments.

MANAGE
Lessons learned, decide between renewal, new tender, termination or insourcing.

TYPES OF PROCUREMENT



TYPES OF PROCUREMENT

REMOTE CARE SYSTEM

MOBILE CLIENT DEVICES

Tags, Bracelets, Badges,
Biometric Scanners
Closed-circuit Security system
Etc.

IDENTIFICATION SYSTEMS

BUILDINGS

Power Regulations
Door lock system
Etc.

NETWORKING EQUIPMENT

MEDICAL DEVICES

Mobile Devices
Implantable Devices
Wearable Devices
Etc.

Hospital Information Systems
Laboratory Information Systems
Etc.

CLINICAL INFORMATION SYSTEMS

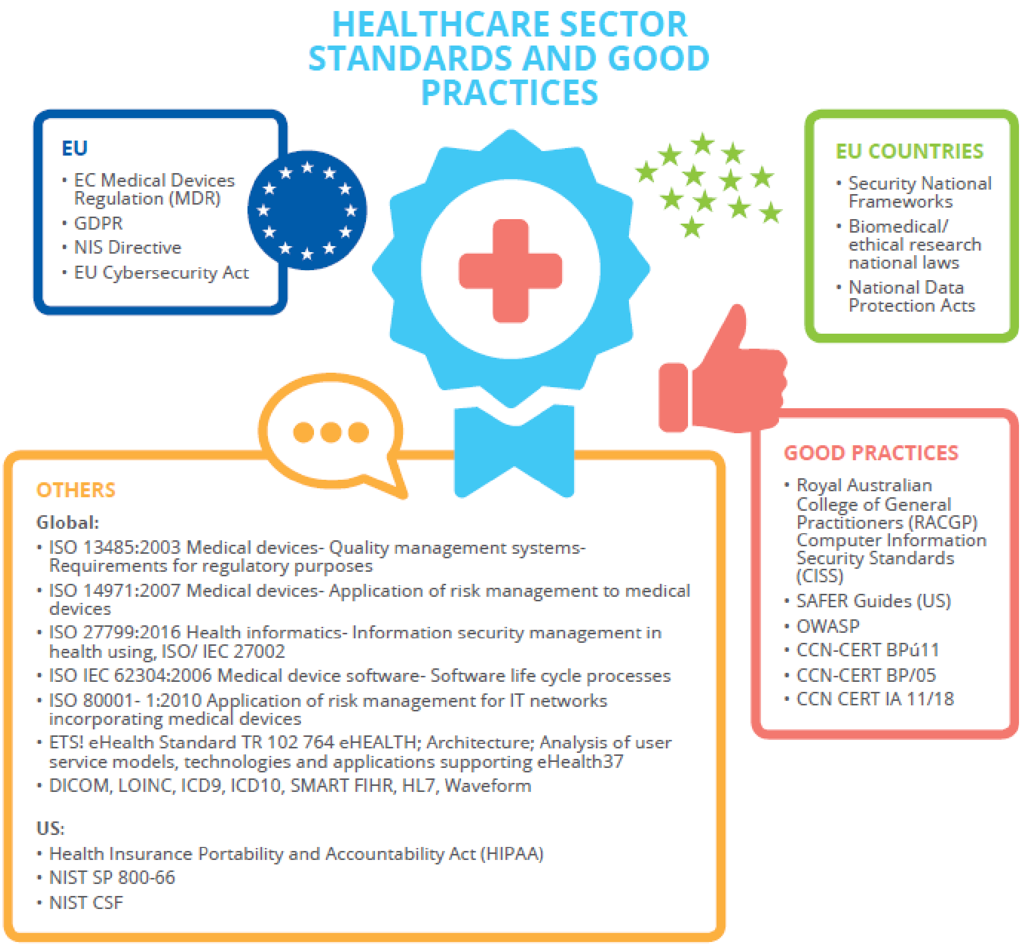
INDUSTRIAL CONTROL SYSTEMS

Temperature
Access Control
Etc.

PROFESSIONAL SERVICES

CLOUD SERVICES

POLICY CONTEXT, STANDARDS AND GUIDELINES



HEALTHCARE SECTOR STANDARDS AND GOOD PRACTICES

EU

- EC Medical Devices Regulation (MDR)
- GDPR
- NIS Directive
- EU Cybersecurity Act

EU COUNTRIES

- Security National Frameworks
- Biomedical/ ethical research national laws
- National Data Protection Acts

OTHERS

Global:

- ISO 13485:2003 Medical devices- Quality management systems- Requirements for regulatory purposes
- ISO 14971:2007 Medical devices- Application of risk management to medical devices
- ISO 27799:2016 Health informatics- Information security management in health using, ISO/ IEC 27002
- ISO IEC 62304:2006 Medical device software- Software life cycle processes
- ISO 80001- 1:2010 Application of risk management for IT networks incorporating medical devices
- ETS! eHealth Standard TR 102 764 eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth37
- DICOM, LOINC, ICD9, ICD10, SMART FIHR, HL7, Waveform

US:

- Health Insurance Portability and Accountability Act (HIPAA)
- NIST SP 800-66
- NIST CSF

GOOD PRACTICES

- Royal Australian College of General Practitioners (RACGP) Computer Information Security Standards (CISS)
- SAFER Guides (US)
- OWASP
- CCN-CERT BPú11
- CCN-CERT BP/05
- CCN CERT IA 11/18

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

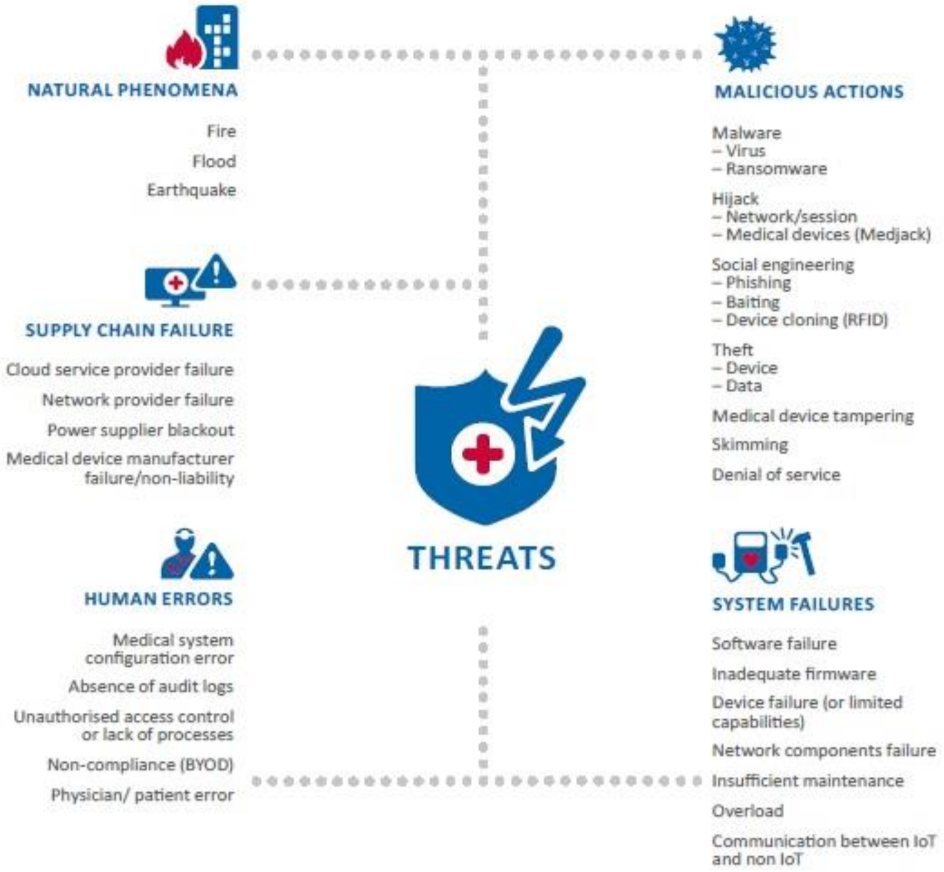
Networking

- Unprotected protocols

Professional Services

- Human factors
- Patient safety

THREAT TAXONOMY



THREATS

NATURAL PHENOMENA

- Fire
- Flood
- Earthquake

SUPPLY CHAIN FAILURE

- Cloud service provider failure
- Network provider failure
- Power supplier blackout
- Medical device manufacturer failure/non-liability

HUMAN ERRORS

- Medical system configuration error
- Absence of audit logs
- Unauthorised access control or lack of processes
- Non-compliance (BYOD)
- Physician/ patient error

MALICIOUS ACTIONS

Malware
– Virus
– Ransomware

Hijack
– Network/session
– Medical devices (Medjack)

Social engineering
– Phishing
– Baiting
– Device cloning (RFID)

Theft
– Device
– Data

Medical device tampering

Skimming

Denial of service

SYSTEM FAILURES

- Software failure
- Inadequate firmware
- Device failure (or limited capabilities)
- Network components failure
- Insufficient maintenance
- Overload
- Communication between IoT and non IoT

GOOD PRACTICES FOR CYBERSECURITY IN PROCUREMENT

Organisational Practices

- Involve the IT department in procurement
- Vulnerability identification and management
- Risk assessment as part of procurement
- Threat identification for products/services
- DPIA for new products/services
- Raise cybersecurity awareness among staff
- Provide training to staff / external consultants
- Plan network, HW and license requirements

- Asset inventory / configuration management
- Develop incident response plans
- Establish testing policies
- Establish Business Continuity plans
- Establish eligibility criteria for suppliers
- Policy for hardware and software updates

GOOD PRACTICES FOR CYBERSECURITY IN PROCUREMENT

Technical Practices

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

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