Sustainable Competence
in Advancing Healthcare

Developments on Cybersecurity in Europe and at Global level, and How Industry is Contributing

Jessica Yuan
COCIR China Representative

9th CIMDR 2018 – Medical Device Internet Security Forum – 15 Sept. 2018
Fuzhou (China)

Table of contents

1. Introduction
2. Developments in Europe
3. Developments at International Level
4. Cybersecurity and Data Protection - Updates in China
5. Industry Contribution
6. Industry Recommendations

1. Introduction

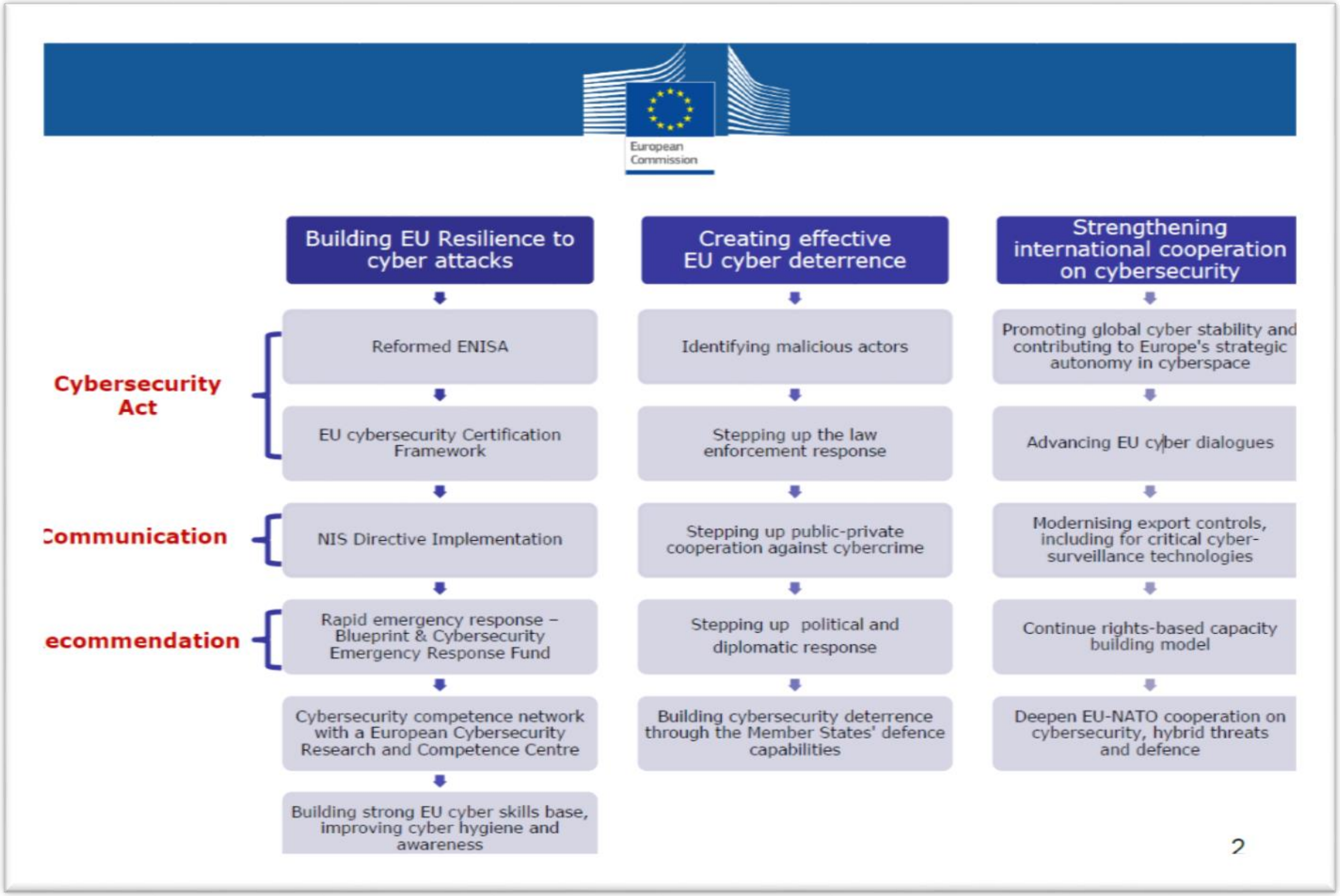
Why Cybersecurity is critical in healthcare

- Healthcare systems are becoming complex
- Massive Innovations in medical technologies and increase of digital health solutions contributing to healthcare system efficiency
- Eco-system is changing towards more patient outcome focused

2. Developments in Europe

- Cybersecurity Package
- GDPR
- MDR

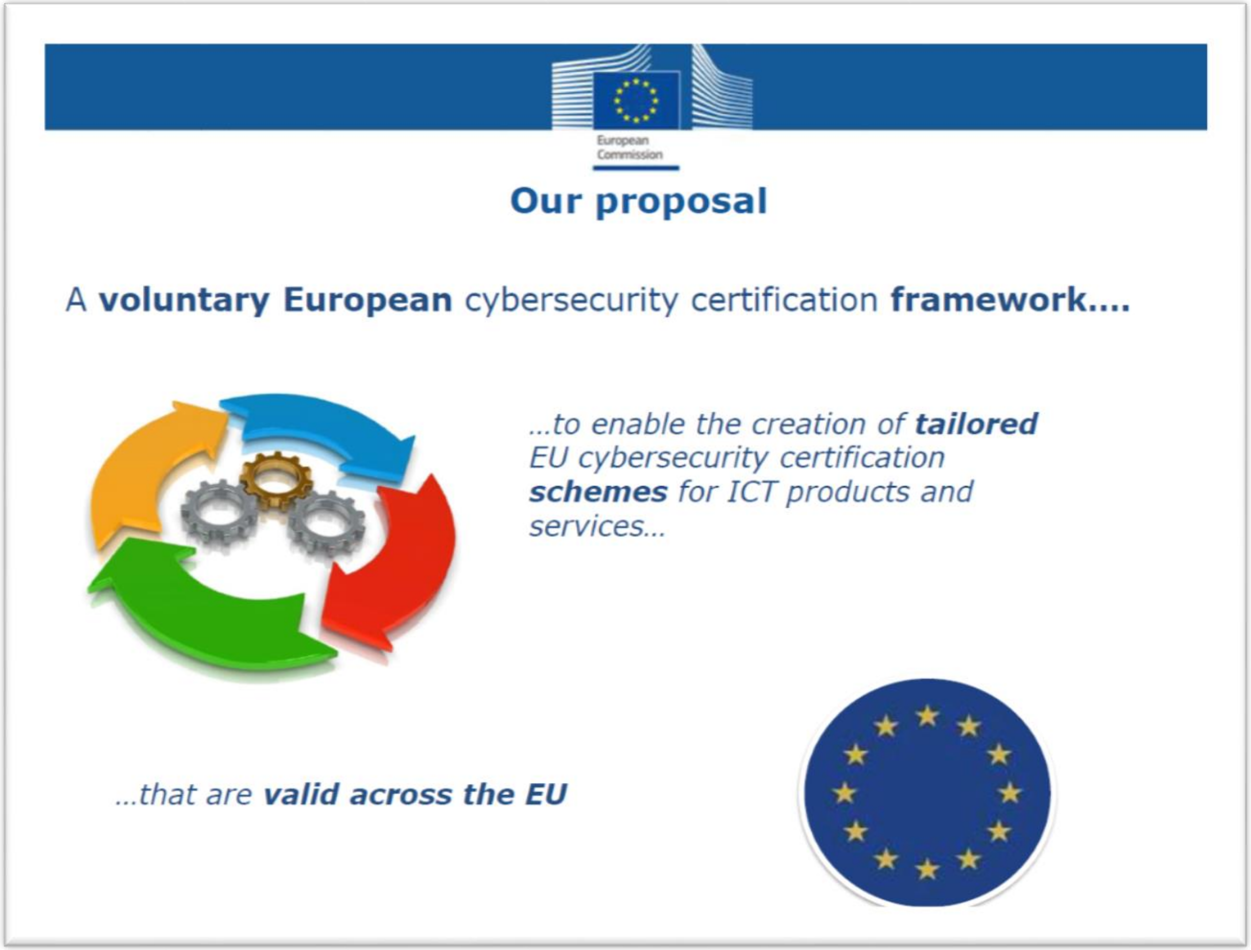
Cybersecurity Package



European Commission

	Building EU Resilience to cyber attacks	Creating effective EU cyber deterrence	Strengthening international cooperation on cybersecurity
Cybersecurity Act	Reformed ENISA	Identifying malicious actors	Promoting global cyber stability and contributing to Europe's strategic autonomy in cyberspace
	EU cybersecurity Certification Framework	Stepping up the law enforcement response	Advancing EU cyber dialogues
ommunication	NIS Directive Implementation	Stepping up public-private cooperation against cybercrime	Modernising export controls, including for critical cyber-surveillance technologies
ecommendation	Rapid emergency response – Blueprint & Cybersecurity Emergency Response Fund	Stepping up political and diplomatic response	Continue rights-based capacity building model
	Cybersecurity competence network with a European Cybersecurity Research and Competence Centre	Building cybersecurity deterrence through the Member States' defence capabilities	Deepen EU-NATO cooperation on cybersecurity, hybrid threats and defence
	Building strong EU cyber skills base, improving cyber hygiene and awareness		

EU Cybersecurity Act (1)



European Commission

Our proposal

A **voluntary European** cybersecurity certification **framework….**

*…to enable the creation of **tailored** EU cybersecurity certification **schemes** for ICT products and services…*

*…that are **valid across the EU***

EU Cybersecurity Act (2)

- **European Commission**

  13 September 2017: Publication of proposal for a Regulation on ENISA

- **European Parliament**

  30 July 2018: Adoption of the draft report

  Sept. 2018: Planned vote in plenary

- **Member States**

  8 June 2018: Adoption of Council General Approach

Next steps:

- **Until end 2018:** Workshops organized by ENISA to collect stakeholders opinions
- **End 2018:** Targeted adoption of Cybersecurity Act

EU Cybersecurity Act (3)

- Policy makers have decided that whenever a specific regulated framework applies then security will be managed through that framework

- Currently European Commission, ENISA and Member States agree that there will be no European cybersecurity certification scheme for medical devices

DIRECTIVE „NIS“ (EU) 2016/1148

- First-ever EU-wide law on cybersecurity!
- It is intended to increase the security of network and information systems within the EU.
- As directive, the Member States need to transpose it into national law.
- 9 May 2018 was the deadline for all EU Member States for national transposition:
  - **Transpositon finalised by 11 countries**: Cyprus, the Czech Republic, Estonia, Finland, Germany, Italy, Malta, Slovakia, Slovenia, Sweden and the UK
  - **Partially transposed by 2 countries**: France, Hungary
  - **Still on-going for remaining 15 countries**

DIRECTIVE „NIS“ (EU) 2016/1148

- The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:
  - Member States to establish a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority
  - Cooperation among all the Member States in order to support and facilitate strategic cooperation and the exchange of security information
  - A culture of security across sectors which are vital for our economy and society, relying heavily on ICT. These Operators of Essential Services (critical infrastructures) and Digital Service Providers need to adopt risk management practices and notify significant security incidents to the competent authorities.

General Data Protection Regulation (GDPR)

- 25 May 2018: Application in all EU Member States

- The most important change in data privacy regulation in 20 years

- Includes requirements related to security:

For example, a personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data

- Still unclear enforcement in EU countries regarding health data

Medical Device Regulation (MDR)

- The MDR introduces new requirements related to security
- For manufacturers addressing security is not only mandatory but also the emphasis beyond good security design such as security monitoring and to include an extensive foreseeable misuse
- There is a need to clarify that all involved parties have a common understanding that “**security is a shared responsibility**”.... Not only for manufacturers but also hospitals and public authorities
- DG Grow has created a task force to develop security requirements in the coming 18 months. COCIR is a member of this task force. The final deliverable will likely be a **guidance document**

3. Developments at International Level

- IMDRF
- Standardisation

International Medical Device Regulators Forum (IMDRF) – 10 Jurisdictions and Observers

IMDRF International Medical Device Regulators Forum

- IMDRF Management Committee will discuss cybersecurity at the next meeting in September in Beijing

- A proposal for a New Work Item on cybersecurity of medical devices has been proposed by China

General overview of cybersecurity standards relevant for medical devices

HEALTHCARE

HDO-centric
ISO 13606-4, 14441, 21547 EHR
IEC 80001 series-1, -2-1 through -2-9
ISO 17799, ISO 27799:2016
HIMSS/NEMA HN 1-2013 (MDS^{2})

Horizontal med. device standards
ISO 14708-1 Manuf. info
ISO 11633-1:2009
EN 45502-1:2015
IEC 60601-1 (Ed. 3.1)
(each includes some security requirements)

Supports ISO 14971
AAMI TIR57:2016
AAMI TIR97*
AAMI SW96*
* Under development

Software life cycle
IEC 80001-5-1 Security: Activities
NIST IR 8151 Reducing SW Vuln.
ISO 15443 Security Assurance

In vitro diagnostics
CLSI AUTO11-A2 (2014)

GENERAL

NIST
SP 800-30 rev. 1
SP 800-53 rev. 4

NIST FIPS
140-2
180-4
186-4
197
198-1
199
200
201-2
202

General IT security
ISO/IEC 27000 series, e.g.,
- ISO/IEC 27001:2013
- ISO/IEC 27002:2013

ISO/IEC 15408-1:2009
ISO/IEC 15408-2:2008
ISO/IEC 15408-3:2008

Vulnerability disclosure
ISO/IEC 29147:2014
ISO/IEC 30111:2013

Industrial control systems
IEC 62443 series

UL
UL 2900-1 (Ed. 1)
UL 2900-2-1

Cybersecurity standardisation

- Recognizing multiple security frameworks is paramount, there is not a one fits all solution!

- New developments should focus on how to apply base security standards within the healthcare domain, e.g.:
- **IEC 60601-4-5** New Work Item Proposal for a Technical Report on cybersecurity functionality of Medical Devices
- **IEC 80001-5-1** New Work Item Proposal for a standard on lifecycle activities towards information security of medical devices

4. Cybersecurity and Data Protection - Updates in China

Cybersecurity and data protection

- TC10/SC1 is now drafting a standard covering cybersecurity requirements. The drafting phase is coming to an end.
  - Formerly, this standard is intended solely for DICOM. The direction changed during the drafting phase and cybersecurity requirement was included in the upcoming standard.
- Some cybersecurity product requirements are under developing by NMPA Jiangsu test lab.
- ZMDS(Zhongguancun Medical Device Society) is collaborating with Beijing test lab on drafting a cybersecurity guidance.

Cybersecurity and data protection

- Spectrum of standards from TC260
  - More than 20 standards are lately drafted under the title *Information security technology*. And the comments are collected.
  - Among the whole spectrum, it worth mention the GB/T 35273—2017
    - Information security technology — Personal information security specification
    - similar concept of GDPR

5. Industry Contribution

Global industry activities on cybersecurity

DITTA
GLOBAL DIAGNOSTIC IMAGING,
HEALTHCARE IT &
RADIATION THERAPY
TRADE ASSOCIATION

1. DITTA White Paper on Cybersecurity of Medical Imaging Equipment (LINK)

- a common understanding of security concepts can help to make stakeholders aware of cybersecurity risks.
- it is important for manufacturers and healthcare providers to adopt best practices and standards and to share those with other stakeholders.

DITTA

DITTA White Paper on Cybersecurity of Medical Imaging Equipment[1]

[1] The DITTA White Paper on Cybersecurity of Medical Imaging Equipment is derived from NEMA/MITA CSP 1-2016 Cybersecurity for Medical Imaging... Reprinted by permission of the National Electrical Manufacturers Association, Medical Imaging & Technology Alliance.

1 OF 9

30 NOVEMBER 2016

2. 19 March 2018 DITTA Workshop on Cybersecurity at IMDRF meetings in Shanghai

=> Find all presentations from the workshop here!

3. DITTA proposal for a New Work Item on cybersecurity at IMDRF

22 October 2018

DITTA Workshop on digital health and cybersecurity at next meeting of Asian Harmonisation Working Party (AHWP) in Kuala Lumpur, Malaysia

Join the discussion!

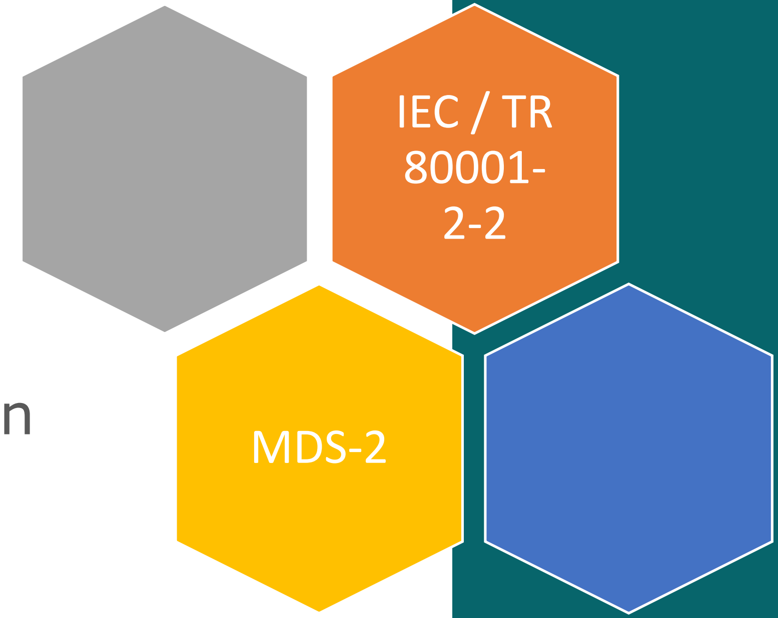
AHWP

Asian Harmonization Working Party

WORKING TOWARDS MEDICAL DEVICE HARMONIZATION IN ASIA

MDS2 in global perspective

- MDS2 originated as an industry standard to provide information for HIPAA compliance checks
- In final stages of its 3rd revision
- Chinese new proposal is to design a cybersecurity information declaration form based on MDS2 form
- Another proposal in Germany is to create a German version of the document



Industry Recommendations

- Only the combination of technical AND organizational measures can achieve cybersecurity.
  ➔ Security is a shared responsibility of manufacturers, integrators and users.

- A medical device‘s Intended Use defines the balance of Safety, Security and Performance
  ➔ The use of a device determines useful and appropriate security measures.

- Different to Safety, Security decays over time.
  ➔ State-of-the-art keeps moving rapidly, … a “secure device” will be hacked tomorrow.

- A product security certificate would be a too easy target
  ➔ Rather audit an organization’s capability to detect, respond and recover from new vulnerabilities and risks through well established lifecycle processes!

Thank you for your attention!

www.cocir.org