Cybersecurity and medical devices

Webinar of the IBA Healthcare and Life Sciences Committee

Tuesday 24 February 2022

14.00 – 15.30 GMT

the global voice of the legal profession®

Cybersecurity and Medical devices

Presentation of the IBA Healthcare and Life Sciences Law Committee

The webinar is part of a series of webinars organised by the HCLFL Committee.

Cybersecurity has become a key legal issue for the healthcare sector. The number of cyberattacks has increased in recent years, particularly during the Covid-19 pandemic. Medical device manufacturers need to deploy effective prevention and management crisis programmes in order to prevent cyber attacks or minimize their effects.

Topics to be discussed will include:

- The context and categories of cyberattacks in the healthcare sector, including facts and figures
- Regulation regarding cybersecurity and its application on medical devices
- The recent evolution of regulations (including cyber and data protection, medical device regulation, connected medical devices, use of artificial intelligence and compliance officers)
- Legal and technical challenges (including liability), as well as recommended actions in this respect

IBA Cybersecurity Guidelines for law firms, October 2018

THALES

Systematic
Paris Region Deep Tech Ecosystem

LANTER

DREW & NAPIER

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Speakers

Emmanuel Dotaro – ICT Director at Thalès- France and Head of the Cyber & Security Hub of Systematic Paris Region, Paris - France

Stefan Juon – Head of Department ICT/CISO
Cantonal Hospital Graubuenden, Chur - Switzerland

Sean Letz – Asia Cyber Leader, FINPRO, Marsh - Singapore

THALES

Systematic
Paris Region Deep Tech Ecosystem

LANTER

DREW & NAPIER

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Introduction and Moderator

Cécile Théard-Jallu – Partner, De Gaulle Fleurance & Associés – France
Vice Chair, IBA Healthcare and Life Sciences Law Committee

Moderators

Benjamin Gaw – Partner, Drew & Napier – Singapore
Asia Pacific Regional Forum Liaison Officer, IBA Healthcare and Life Sciences Law Committee

Monika Gattiker – Partner, Lanter – Switzerland
Vice Chair, IBA Healthcare and Life Sciences Law Committee

THALES

Systematic
Paris Region Deep Tech Ecosystem

LANTER

DREW & NAPIER

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Introduction: Some facts & figures

Digital health boom:

- **Numerous digital tools for major challenges**: Fighting against medical vacancies, decompartmentalizing care paths, relieving hospital overcrowding, facilitating prevention, proposing a new service offer or accelerating personalized medicine ...

MDs in the front line

- **2.3 billion gigabytes of health data worldwide / 80 billion connected health objects / 50,000 m-apps** (SNITEM projection for 2020)
- Almost all health and medico-social professions concerned:

MDs at the heart

- Medical records on the black market: **20 to 30 dollars** => i.e for an hospital hosting for example 100 000 records, a windfall of **2 to 3 million dollars** for hackers

Facing a rise in cyber risk:

- **Multiple categories**: malware, phishing, identity theft, DDoS, customer database corruption, HR, R&D ....
- In 2020, + 47% of attacks in the healthcare system (source: ENISA) / ex: in **French hospitals**, an **average of 1 cyberattack per week** since the beginning of 2021 (growing with Covid-19)
- **40% in 2020 (57% in 2019) is the share of incidents of accidental origin** (main reasons: software bugs, malfunctions or failures of network, applications or phones)
- **Attacks on MDs also outside of healthcare facilities** (e.g. pacemakers, connected defibrillators, insulin pumps.. in patients' homes: a 2017 report detected nearly 1,400 **vulnerabilities in a single connected implant in the United States**)

⇒ MD manufacturers with **a still very heterogeneous cybersecurity culture** according to ANSM (French Health Products Safety Agency), for multiple reasons, including:

- no specific risk analysis
- lack of awareness of cybersecurity requirements
- failure to take cybersecurity into account in the MD design and development process

Sources: MSS / ANS Report May 2021, CERT Santé Public Report for 2020, Le Figaro February 2021, Irdeto Survey, 2019, Oodrive August 2019

Examples:

- Hacking the IS of an Hospital's radiotherapy department giving access to patient data contained in medical devices
- A University Hospital "in degraded mode" for 10 days / 100% of the IS to be restarted or IS compromised, including interaction with the MDs

=> ***Consequence: interruption of the HCO's activities***

- In 2016: WIFI-enabled infusion pump was withdrawn from the market by J&J due to vulnerability to hacking / In 2019: Medtronic recalled an insulin pump model due to risk that unauthorized persons could record transmitted data

EU Member States and EU laws interplay framework

- ***NIS Directive 2016/1148 6 July 2016 => MS laws***
- *What is an Essential Service Operator (ESO)?*
  - Public or private actor providing an essential service whose interruption would have a significant impact on the functioning of a society or its economy
  - An essential service corresponds to 3 criteria:
    1. service essential to maintain critical societal or economic activities
    2. Its provision is dependent on NIS
    3. an incident on these NIS would have a significant disruptive effect on the provision of said service

Recast of the NIS Directive

Report on the new EU cybersecurity strategy in December 2020: wants revision of NIS Directive

« Cybersecurity Act » (European Regulation 2019/881 of 17 april 2019)

- Sets out the objectives, tasks and organisational issues concerning ENISA - the European Union Agency for Cyber Security => permanent mandate

Among others, ENISA is actively involved in **healthcare** (recital 15)

- **New European cybersecurity certification framework** to harmonize assessment methods and certification assurance levels across Europe => 3 levels (elementary: ex IoT - substantial: ex Cloud - **high: ex connected MD)**

Ex : HCOs, services providers, wholesalers

- Nearly 600 (?) ESOs / OVIs- list is kept confidential for national security reasons /
- Massive wave of ESOs designated in September 2021 in FR (approx. 100) among HCOs + 13 existing OVIs

MD manufacturers: cybersecurity players

OVIs and ESOs: anticipation and specific obligations

	Operator of Vital importance (OVI / Code of Defense)	Essential Service Operator (ESO) and Digital Service Provider (DSP)	Data controller and processor Personal data
Main applicable texts	**LPM** Fr Act no. 2013-1168 of December 18, 2013	**NIS Directive 2016** Transposed by FR Act no. 2018-133 of February 26, 2018	**GDPR** EU Regulation 2016/679 of April 27, 2016 – Fr Act no.78-17 of January 6. 1978 as modified
Main obligations	▪ Identification and **reporting of VIIS** ▪ Security **incident reporting** ▪ Security checks ▪ Implementation of sectoral security rules ▪ **12 sectors of vital activity** / 18 sectoral decrees ▪ 1 coordinating minister for each sector	▪ Appointment of a **representative** to the ANSSI ▪ **Declaration of networks and IS necessary for the** provision of essential services ▪ **Notification of incidents** affecting the networks and IS necessary for the provision of essential services ▪ Security **checks**	▪ **Notification of** data breaches to the CNIL (unless there is no risk to the rights and freedoms of individuals) ▪ **Notification of** data breaches to data subjects if there is a high risk to their rights and freedoms
Main sanctions	▪ **Administrative fines** ▪ No protection plan: €150.000 ▪ Non-compliance with IS security provisions: €150,000 ▪ **Criminal sanctions**	▪ **Administrative fines** ▪ Lack of incident reporting: ○ €75.000 (EOS) ○ €50.000 (EO supplier) ▪ Preventing ANSSI control actions: ○ €125.000 (EOS) ○ €100.000 (EO Supplier)	▪ **Administrative fine** ▪ Up to €20 million or 4% of annual world wide turnover ▪ **Criminal sanctions** ▪ E.g. failure to comply with the obligation to notify the CNIL : 5 years, €300.000.

GDPR and Personal Data Cybersecurity

Security by design / Procedure in case of a data breach

Privacy by design: the protection of users' privacy is taken into account even before the design of a system involving the processing of personal data => MDs

❖ **Data Security** (art. 32 GDPR)

Same criteria as for privacy by design

List of possible security measures: pseudonymisation, encryption, means to ensure ongoing confidentiality, integrity, availability and resilience of systems and services, timely restoration of availability and access to personal data in the event of an incident, regular testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring processing security

❖ **Sanctions**

- Order to bring processing operations into compliance
- Impose a temporary or definitive limitation on processing
- Suspend data flows
- Order to comply with the data subject's requests
- Impose an administrative fine

What to do in case of a data breach

- ❑ **No risk to the rights & freedoms of individuals**: entry in the internal processing register
- ❑ **Risk**: entry in the internal register **and** notify the DPA within 72 hours
- ❑ **If high risk**: also **warning the inviduals concerned / with exceptions**

Art. 4.12 GDPR

Art. 32, 33 and 34 GDPR

MD manufacturers: cybersecurity players

Cybersecurity in the EU MD Regulations

- **Directive 93/42/EEC** of 14 June 1993 did not explicitly refer to cyber security
- **Directive 98/79/EC** on in vitro diagnostic medical devices did not refer to cybersecurity either

→ **MD Regulation 2017/745 & MD DIV Regulation 2017/746** of April 5, 2017 **do contain specific cybersecurity provisions**

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

MD manufacturers: cybersecurity players

Cybersecurity in the EU MD Regulations

Numerous MDR provisions relating to MDs cybersecurity, including :

- Article 83 on the post-market surveillance system set up by the manufacturer
- Article 84 on the post-market surveillance plan
- Article 85 on the post-market surveillance report
- Article 86 on the periodic safety update report
- Article 87 on the notification of serious incidents and corrective actions
- Article 88 on trend reporting
- Article 89 on the analysis of serious incidents and corrective safety measures
- Annex I on general safety and performance requirements
- Annex II on technical documentation
- Annex III on technical documentation for post-market surveillance
- Appendix XVI B on post-market clinical follow-up

+ Importance of recognizing the **responsibility of all actors in the protection of MD**

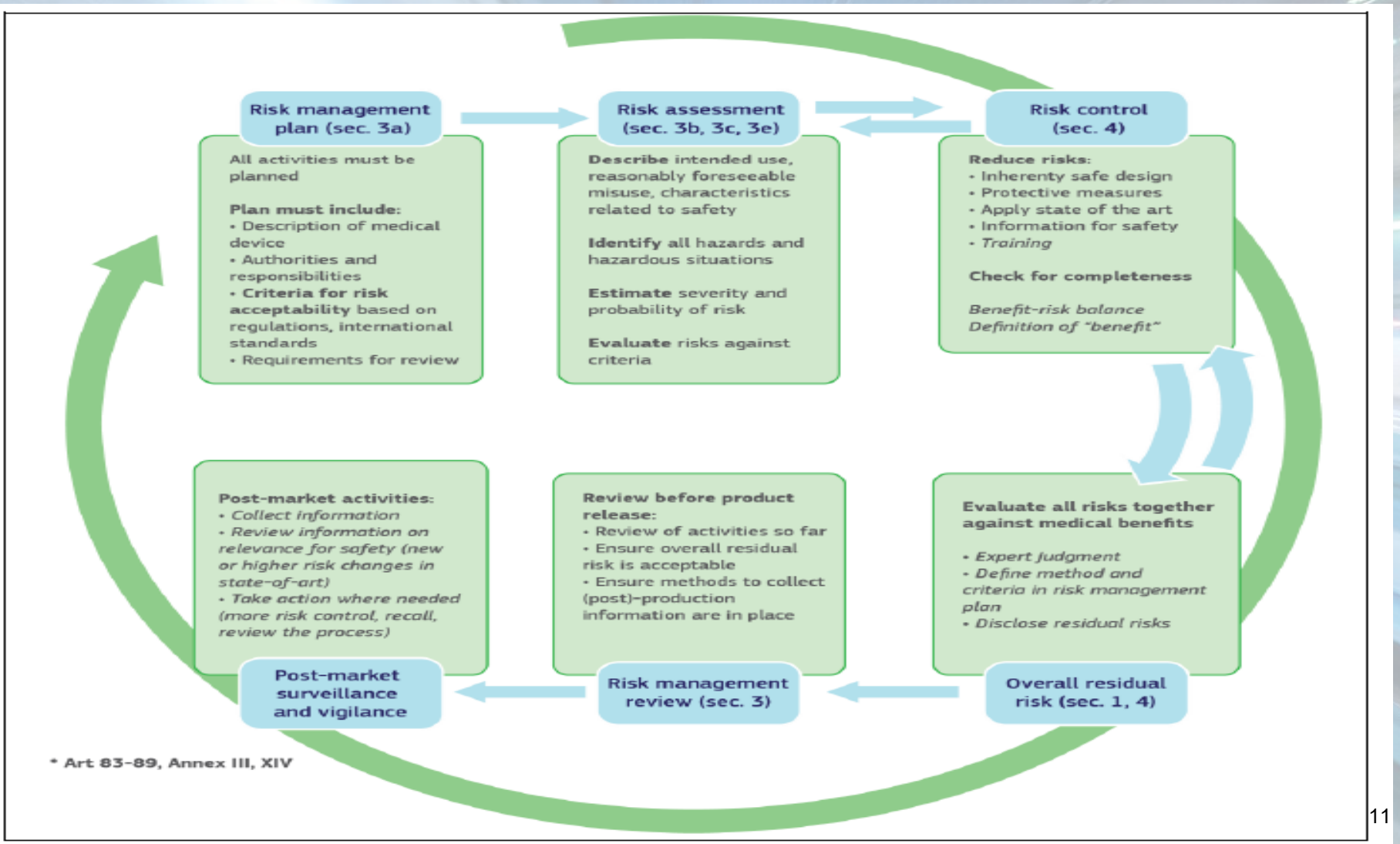
+ **Responsibility/liability can also have a contractual origin**

Same provisions as in the MD DIV Regulation in Articles 78 to 84, and Annexes I and III

MD manufacturers: cybersecurity players

Cybersecurity in EU MD Regulations - Diagram 1

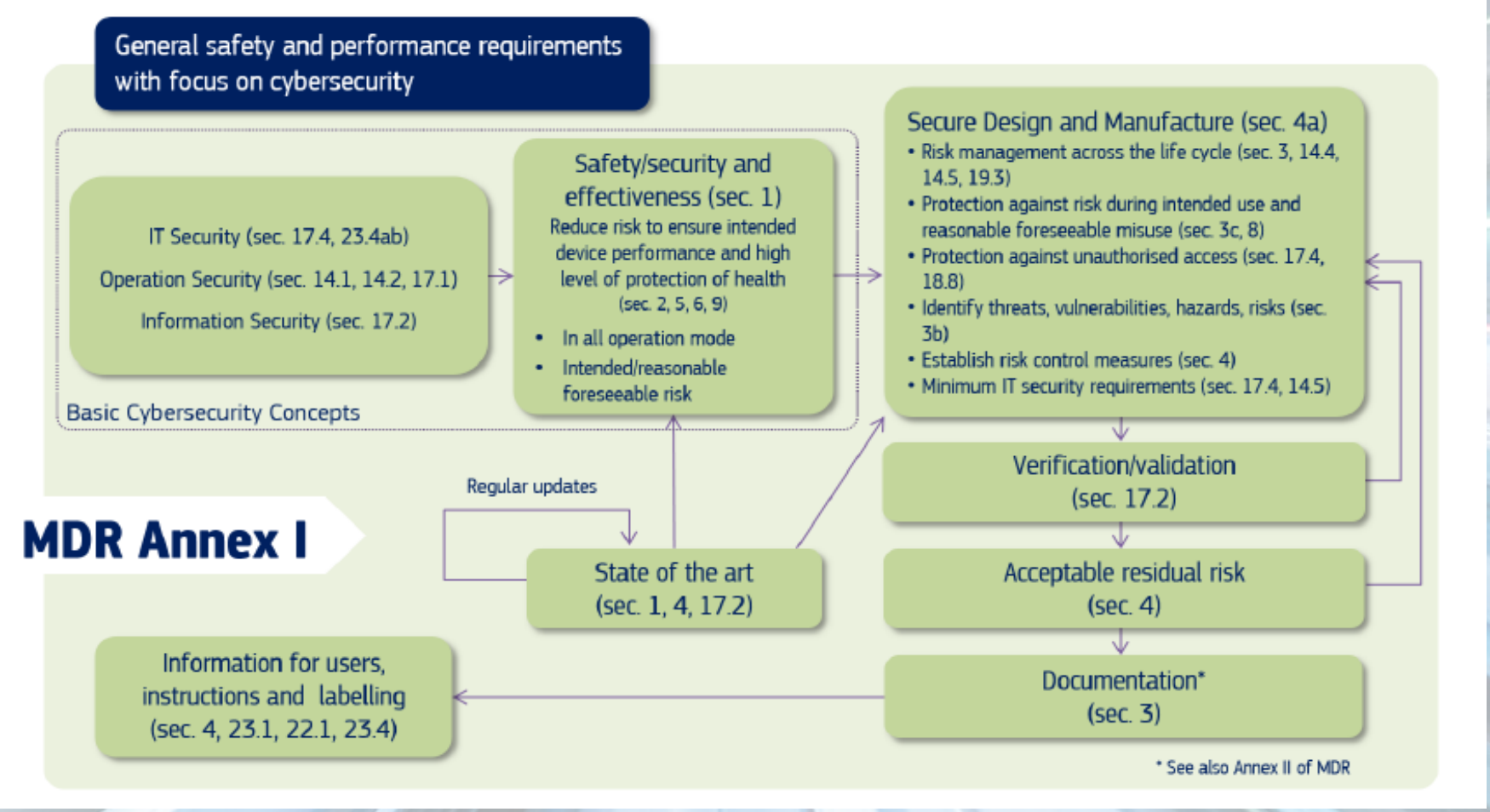
Main obligations in cybersecurity



Source: MDCG, Guidance on Cybersecurity for medical devices, 2019

MD manufacturers: cybersecurity players

Cybersecurity in EU MD Regulations - Diagram 2



Source: MDCG, Guidance on Cybersecurity for medical devices, 2019

MD manufacturers: cybersecurity players

Cybersecurity in draft AI Regulation applying to MDs

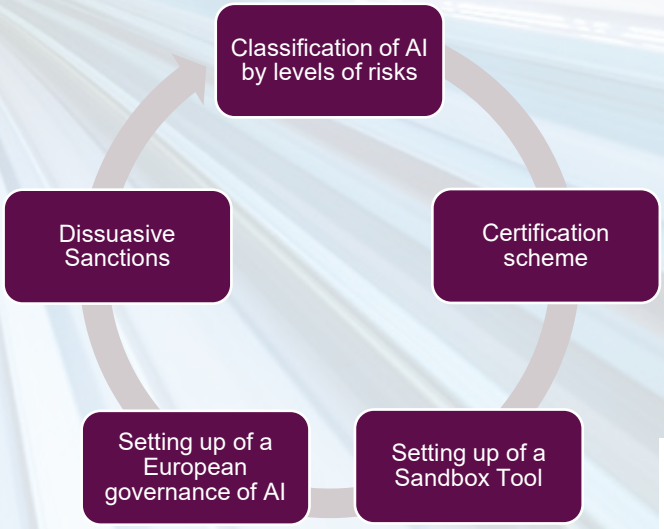
European Regulation project on AI (21 April 2021)

- **AI classified by level of risk (inacceptable, high risk, limited => MDs can be considered high risk)**
- **Recital 43: Health and cyber**
  - *requirements apply to high-risk **AI systems including cybersecurity***
  - *requirements are **necessary to effectively mitigate health risks***
- **Article 14 on human control of high-risk AI**
  - ***effective control by natural persons** during the period of use of the AI system*
  - *human control aims to **prevent or reduce health and safety risks***
- **Article 42 on the presumption of conformity**

with certain requirements

Presumption of conformity if :

- *High risk AI systems **trained and tested with geographic, behavioral and functional context data***
- *High-risk AI systems that have been **certified/declared compliant** under a cybersecurity scheme **in accordance with Regulation (EU) 2019/881** (Cybersecurity Act 17 April 2019)*



DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Speaker

Emmanuel Dotaro

ICT Director at Thalès
Head of the Cyber & Security Hub of Systematic Paris Region,
Paris, France

THALES

Systematic
Paris Region Deep Tech Ecosystem

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Cybersecurity and Medical devices

Interview with Emmanuel Dotaro

Question 1: From your cybersecurity industry point of view, what are your visions on the risks and vulnerabilities in the healthcare sector?

➔ **Which types of attacks?**

- **unauthorized access**: interception of the wireless data flow between the MD and a sensor by a malicious individual who can store, modify, encrypt ...
- **malware**: *malware* designed to disrupt the functionality of an MD
- **denial of service attacks**: overload of requests made to the MD leading to a service interruption
- **Others?**

➔ **Data centric**

➔ **Systems and services**

THALES

Systematic
Paris Region Deep Tech Ecosystem

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Cybersecurity and Medical devices

Interview with Emmanuel Dotaro

Question 2: What are the good practices that healthcare players must adopt to protect their critical environment?

➔ **Work together w/ Cyber professionals, balance in house vs. managed services etc…**

➔ **Prevention, protection, detection, remediation**

Example of EU project:
PANACEA: Protection and priVacy of hospital and health iNfrastructures with smart Cyber sEcurity and cyber threat toolkit for dAta and people

THALES

28 février 2022

Systematic
Paris Region Deep Tech Ecosystem

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

Cyber attacks and medical devices: *How to react towards the cyber risk? A management involving a large panel of actors*

In relation with competent authorities and agencies

- Data Protection Authorities
- Cybersecurity Agencies
- Criminal judicial authorities
- Civil judicial remedies

DE GAULLE FLEURANCE & ASSOCIÉS
SOCIÉTÉ D'AVOCATS

MD manufacturers: cybersecurity players

Question 3: How healthcare players and users can trust the digital infrastructure and services

➔**Standards, certification, regulation**

➔**Interplay of the three!**

Example: GDPR certification , Art. 42, first EU-wide scheme

➔**Confidentiality/privacy and liabilities**

MD manufacturers: cybersecurity players

International comparison

Countries, International Authorities, Standards and Guidelines

❖ **National guidelines** related to cybersecurity & MDs, for example in: Australia, Canada, Germany…

❖ **Examples of international organizations using cybersecurity standards**

- International Medical Device Regulators Forum (**IMDRF**)
- European Network and Information Security Agency (**ENISA**)
- In France, Agence nationale de la sécurité des systèmes d'information (**ANSSI**)

❖ **Standards and reports issued on cybersecurity**

- Ex. : Standards ISO 27005 and 14971
- « *Guidance on Cybersecurity for medical devices* » (MDCG, 2019)
- Procurement guidelines for hospital cybersecurity (ENISA, 2020)
- Practical Guide to the Rules for Connected Devices in a Health Information System (General Security Policy for Health Information Systems - PGSSI-S) (2013 and following)
- Guide IMDRF for cybersecurity in 2019

MD Manufacturers: Cybersecurity players

Interview with Emmanuel Dotaro

Questions 4:

How the current digital transformation is changing the picture for the health sector?

➔New attack surface, device, data, system etc…

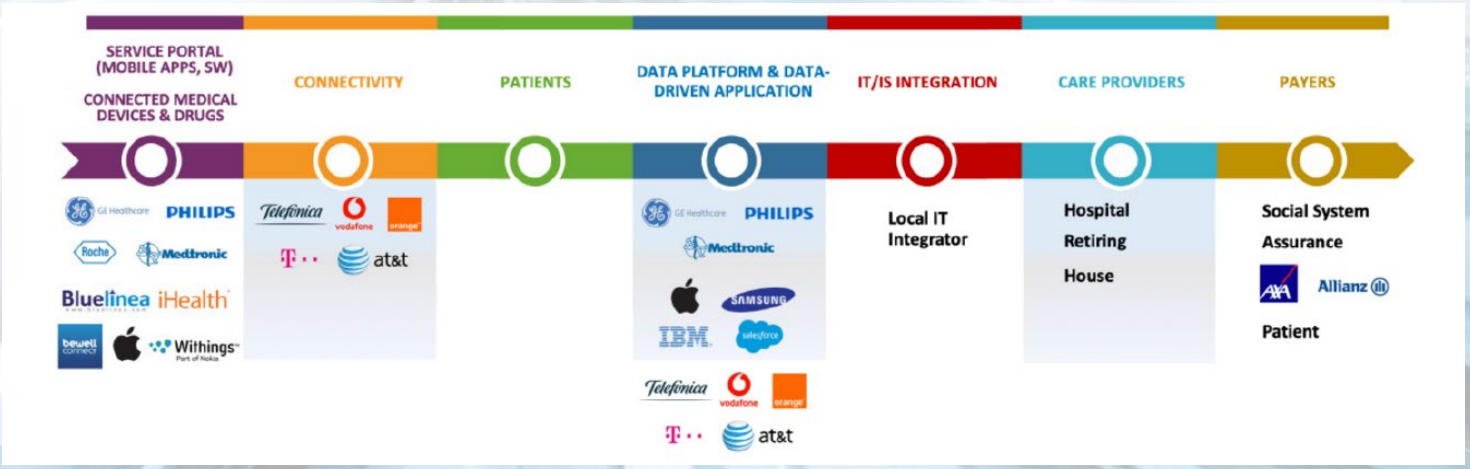
➔Current challenges of data centric and SecOps

What are the next challenges, technical disruptions and potential impact on the health sector ?

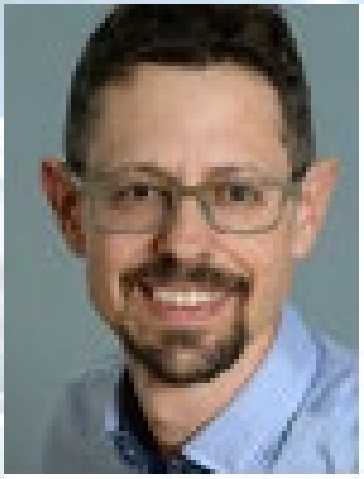
➔5G➔6G➔cloud/edge/IoT/AI

➔may address up to Surveillance Capitalism debate

IoT research, Innovation and deployment priorities in the EU White Paper, Report 2018/2021 – part of European Union's Horizon 2020 research and innovation program)



Cybersecurity
Perspective of Healthcare Service Providers



Stefan Juon

Head of Department CT/CISO,
Cantonal Hospital Grisons,
Switzerland

28 February 2022

LANTER

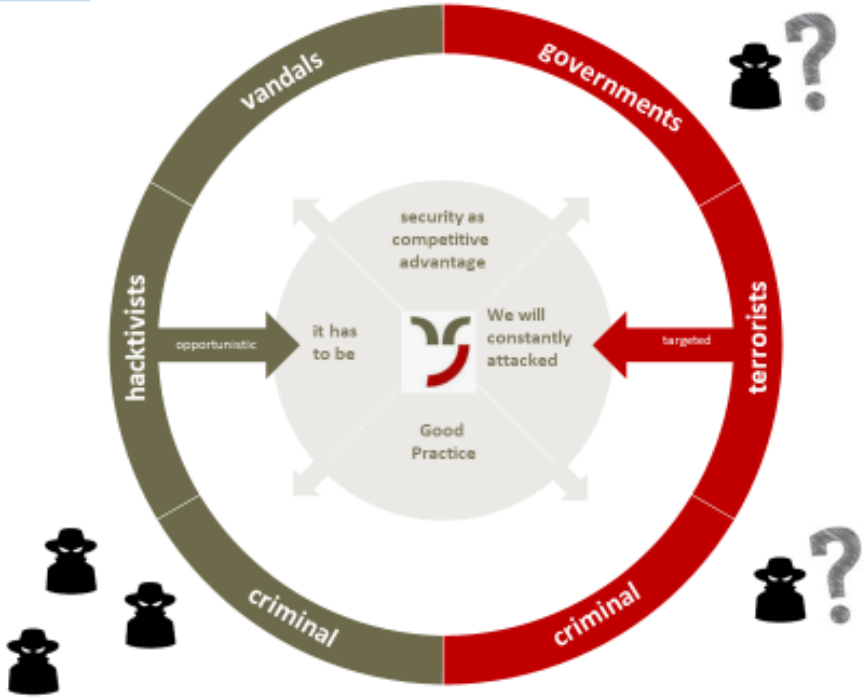
Kantonsspital Graubünden

Regulatory Requirements for Healthcare Providers?

- MD Regulation 2017/745 & MD DIV Regulation 2017/746 of April 5, 2017 contain rules on post-market surveillance, vigilance and market surveillance (article 83 – 89 MDR and articles 78 – 84 MD DIV), which also apply to cybersecurity.
- MDR and MD DIV: no specific obligation for healthcare providers to report suspected serious incidents.
- Swiss legislation on medical devices:
  specific obligation for healthcare providers to report suspected serious incidents to the supplier and the Swiss federal authority (Swissmedic).
- Supply agreements state obligation of healthcare providers to report incidents

Cyber Risks in a Hopitals?

Who threatens our protection goals?



Cyber Risks and Risk Manangement

- Cyber risks = business risks => financial losses
- Reputational damage / business interruption / liability risks

Minimize / avoid risks

- IT-Specialists
- QM, compliance with technical standards

risk occurred

Shifting / limiting risks

- Liability of suppliers / manufacturers?
- Insurance?

LANTER

Kantonsspital Graubünden

Summary

- Cybersecurity and cyber attacks are increasing challenges also for healthcare providers.
- Regulatory and liability risks of healthcare providers related to cybersecurity are currently rather low (may change in future)
- Shifting damages related to cyber attacks onto the supplier/manufacturer can be challenging and guaranteed

➢ The main focus must lie on the minizing the risks based on IT security measures, ideally in close cooperation with the industry

➢ Other option: Insurance for cybersecurity risks

Speaker

Sean Letz

Asia Cyber Leader, FINPRO, Marsh - Singapore

Cybersecurity and Medical devices

Interview with Sean Letz

Understand the impact and consequence of a cyber event

Cyber Event

Malicious attacks or accidental events to your digital system (including IT and OT*), data (in house or outsourced), or technology.

Resulting in:

Impact

Non-physical

- Confidentiality Issues
- Integrity Issues
- Availability Issues

Physical

- Property Damage
- Bodily Injury

Leading to losses/claims:

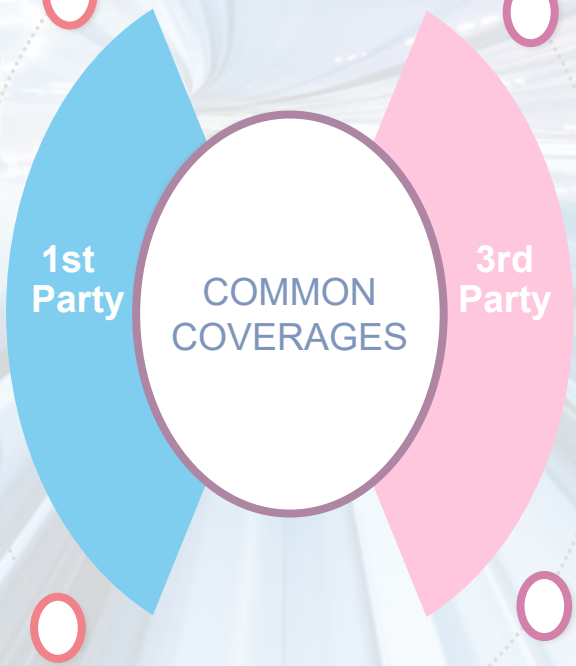
Consequence

- Loss of Income
- First Party Costs
- Third Party Liability
- Fines and Penalties
- Extortion Demands
- Negligence in Services
- Shareholder Litigation

*Operational technology

Cyber Insurance Overview

Covers perils and the non physical risks arising from malicious acts or accidental events impacting data, computer networks, or technology and costs associated with their impact



Event management / breach response

Forensics, public relations, call center, notification and credit monitoring services

Business / network interruption

Extra expense and loss of business income

Cyber extortion / ransomware

Forensics, investigation and ransom payments

Data restoration

Costs to replace, restore, recreate damaged or lost data

Privacy Liability

Failure to prevent unauthorized access / disclosure of entrusted personally identifiable or confidential information (Liability and defense costs, PCI fines and penalties)

Network Security Liability

Failure of system security to prevent or mitigate a computer attack (Liability and defense costs)

Privacy Regulatory Defense Costs

Privacy breach and related fines or penalties assessed by Regulators

Interview with Sean Letz

Cyber market influenced by increased exposure

Ransomware sophistication:

- Average downtime up 16% YOY to **22 days**
- 66% YOY increase in data exfiltration to **83% of attacks**
- **Ransoms paid** less than ransoms demanded (tens of millions increasingly commons)
- Organisations of all sizes and industries are impacted

Regulations intensify:

- **GDPR:** Average fine has more than tripled (~1.55 million € vs. ~470 thousand €); not much correlation
- **CCPA:** statutory damages can range up to $750 per consumer; CPRA & similar regulations emerging
- **BIPA:** Litigation is expensive and on the rise; large USA class actions

Systemic Risk concerns:

- **Common vulnerabilities** (in hardware or software) and **common dependencies** (vendors and software)
- Sample events driving aggregation concerns: SolarWinds, Accellion, Microsoft Exchange, Kaseya & Log4J
- **43% of leaders** report no confidence in their ability to prevent third-party cyber threats

Marsh

Ransomware: Coveware Q3 Blog; **GDPR:** November 2019 vs. November 2021, enforcementtracker.com; **Systemic Risk:** Marsh Microsoft Cyber Risk Perception Survey

Q&A session

Any questions?

IBA HCLSL Committee, what's next?

YOUR CONTACTS

Emmanuel Dotaro

email: emmanuel.dotaro@thalesgroup.com

Cécile Théard-Jallu

Tel.: +33 (0)6 61 92 05 29

Email: ctheardjallu@dgfla.com

Stefan Juon

email: stefan.juon@ksgr.ch

Monika Gattiker

Tel.: +41 76 321 21 25

email: gattiker@lanter.biz

Sean Letz

email: sean.letz@marsh.com

Benjamin Gaw

Tel.: +65 9452 2114

email: benjamin.gaw@drewnapier.com

THANK YOU!