EU eHealth Cybersecurity Policy Context and Incident Reporting under the NIS Directive

5th eHealth Security Conference

ENISA

30 October 2019
Barcelona, Spain

Marco Marsella, Head of Unit “eHealth, well-being and ageing”
European Commission
DG CONNECT – Communications Networks, Content and Technology Directorate H – Digital Society, Trust and Cybersecurity
The cyberspace is a backbone of digital society & economic growth but cybersecurity incidents are increasing at an alarming pace.

Cybersecurity incidents may:

- Disrupt the supply of essential services such as water, healthcare, electricity or mobile services
- Undermine trust in digital services & products
  - Only 22% of Europeans have full trust in companies such as search engines, social networking sites & e-mail services
  - Only 38% of Europeans feel confident about online purchasing from another EU Member State

...as well as financial theft, loss of intellectual property, data breaches, etc.
Evolution of the Cyber Threat Landscape

- Ransomware/Malware as a Service – Cybercrime 'industry'
- Cloud Apps – New Attack Vector
- Hybrid Attacks - Cyber as a strategic weapon
- Increase in Data Breaches/Compromised Credentials
- Internet of Things – from smart devices to zombie bots
Ineffective cybersecurity is a danger to patient safety worldwide

- Attacking Obsolete Operating Systems
- Hijacking Access to National Healthcare Databases
- Rootkit Malware Attack in a Cancer Treatment Institute
- Healthcare Data Theft
- Tampering with Medical Devices
- Ransomware Attack to Healthcare Data
- Distributed Denial-of-Service Attack in Regional Hospital

**WannaCry** (devasted NHS in 2017)

230,000 computers in 150 countries wide-ranging attack

**SingHealth** (Singapore, 2018)

stole information about 1.5 million patients targeted attack

**Anthem Insurance** (US, 2015)

79 million records breach 100 M$ in settlements
Healthcare Incidents

Extract from CERT-EU’s media monitor - 23 October 2019

Hospital leaks 129K patient records in sophisticated phishing scam

A healthcare provider in Kalispell, Montana has suffered an embarrassing data breach resulting in 129K health records getting leaked, exposing patients to identity theft and fraud. Kalispell Regional Healthcare initially learned of the breach in June, but an investigation into the incident suggests.......  

Montana hospital leaks 129,000 patient records in sophisticated phishing scam

A healthcare provider in Kalispell, Montana has suffered an embarrassing data breach resulting in the leak of 129,000 health records, exposing patients to identity theft and fraud. Kalispell Regional Healthcare learned of the breach in June, but an investigation suggests the phishers started collecting patient records as early as May 24....

Cyber scare shuts down hospital IT systems in rural north-east Australia

A number of rural health services in the state’s north-east were forced to shut down their IT systems due to a malware virus. The Department of Health and Human Services confirmed on Wednesday a virus was detected in handful of desktop computers at two health services in the Hume region and staff.......
What makes the health sector particularly vulnerable?

**Summary Points**

- Investments to cyber security are not given priority
- Outdated and unsupported IT infrastructures and medical devices increase NHS vulnerabilities
- Untrained staff constitute (unintentional) internal threats
- Inefficient incident response capabilities due to lack of cyber security specialists
- Complex structures hinder fast and efficient responsiveness in the face of a cyber attack
Digital Transformation of Health and Care
Artificial Intelligence for Europe

- Increase investment
- Strengthen R&I
- Make data available
- Empower people
- Nurture talent
- Work together
- Boost competitiveness
- Maximise use

AI for Europe how?

#DigitalSingleMarket #AI
Cybersecurity

A strategic priority for the EU

Continuous policy response to the evolving threat landscape:
- 2013 EU Cybersecurity Strategy: 'An Open, Safe and Secure Cyberspace'
- 2016 Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry
- 2017 Cybersecurity package
- 2018 Proposal for the European competence centre and network
- 2019 Cybersecurity Act entered into force

Building EU Resilience to cyber attacks

Capacity Building
- Enhanced national capabilities & Risk management requirements
- Financial Support from the EU
- Industrial capabilities

Prevention & Response Coordination
- ENISA operational support & Cooperation between national CSIRTs
- Coordinated response to large-scale cybersecurity incidents and crises & exercises
- Single Market for certified ICT products and services

Cybersecurity Act:
Building strong cybersecurity for the EU: Resilience, Deterrence and Defence

| From reactive to pro-active and cross-policy approach bringing various work streams together to build EU’s strategic cybersecurity autonomy |
| Improving resilience and response by boosting capabilities (technology/skills), ensuring the right structures are in place and EU cybersecurity single market functions well |
| Stepping up work to detect, trace and hold accountable those responsible for cyber attacks |
| Strengthening international cooperation as a platform for EU leadership on cybersecurity |
| Involving all key actors - the EU, Member States, industry and individuals to give cybersecurity priority it deserves |
Policy/legislative framework

Awareness

- Network and Information Security Directive (NIS)
- Radio Equipment Directive
- eIDAS Regulation
- Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy)

Education

- General Data Protection Regulation (GDPR)
- Cybersecurity Act
- Medical Device Regulation

Research and Innovation

Infrastructures
**NIS Directive: Main Features**

**GREATER CAPABILITIES**
Member States have to improve their cybersecurity capabilities.

**COOPERATION**
Increased EU-level cooperation

**RISK MANAGEMENT**
Operators of essential services and Digital Service Providers have to adopt risk management practices and notify significant incidents to their national authorities.
Cooperation Group - Tasks

Information & Best practices on
- Risks
- Incidents
- Awareness raising
- Training
- R&D

Work of the Group
- Establish a work programme by 18 months after entry into force
- Prepare WP every 2 years thereafter

Policy coordination
- guidance for CSIRTs Network
- assist MSs in NIS capacity building
- support MSs in the identification of operators of essential services
- discuss incident notification practices
- Discuss standards
- Engage with relevant EU institutions
- Evaluate NIS national strategies and CSIRTs (voluntary)

On progress
- Every 1,5 yrs provide a report as input to EC's review of the Directive
Exchange info on CSIRTs' services, operations & capabilities

Discuss lessons learnt from NIS exercises

Discuss individual CSIRT issues (on request)

Guidelines on operational cooperation

Inform Cooperation Group & seek guidance

Report as input to EC review every 1½ years

Exchange info on individual incidents (on request & voluntary)

Identify coordinated response to incidents (on request & voluntary)

Support cross-border incident handling (voluntary)

Explore further forms of operational cooperation
Security and notification requirements

Operators of essential services

- Energy: electricity, gas and oil
- Transport: air, rail, water and road
- Banking: credit institutions
- Financial market infrastructure
- Health: healthcare providers
- Water: drinking water supply and distribution
- Digital infrastructure: internet exchange points, domain name system service providers, top level domain name registers
Security and notification requirements

Digital Services Providers (DSPs)

- Online market places
- Cloud computing services
- Search engines
Member States shall ensure that Operators of Essential Services and Digital Service Providers adopt security requirements to:

- **Prevent Risks**: Technical and organisational measures that are appropriate & proportionate to the risk.
- **Ensure NIS**: The measures should ensure a level of NIS security appropriate to the risks.
- **Handle Incidents**: The measures should prevent and minimize the impact of incidents on the IT systems used to provide the services.
Notification requirements

MSs shall ensure notifications without undue delay to the competent authority or to the CSIRT.

Operators of Essential services

"incidents having a significant impact on the continuity of the essential services they provide. [...]"

Digital Service Providers

"any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union"
NIS implementation one year later

**Transposition**
- All MS Notified Full Transposition
- EC assessment of completeness & conformity underway

**Cooperation Group**
- 10 Work Streams (15 Work Programme tasks)
- 12 Plenary meetings
- 10 Reference documents delivered (on the implementation of the Directive as well as wider cybersecurity issues)
- 2 table-top exercise. One already performed (on EU elections) and one which took place in July (blueprint operational layer).
- Commission- secretariat of the NIS CG

**CSIRTs Network**
- 7 meetings (continuous exchange through common facilities)
- 2 exercises testing Standard Operating Procedures.
- ENISA- secretariat of the CSIRT Network
The NIS Cooperation Group work

Work Stream 1
Identification of OES

Work Stream 2
Security Requirements

Work Stream 3
Incident notification requirements

Work Stream 4
Cross-Border dependencies

Work Stream 5
Digital Service Providers

Work Stream 8
Energy

Work Stream 10
Digital infrastructures

NIS Implementation

The NIS Cooperation Group work

**Work Stream 6**
Cybersecurity of Elections

**Work Stream 7**
Large scale cyber incidents and crisis

**Work Stream 8**
Sectors aspects influencing the implementation of the Directive (i.e. energy sector, 5G)

**Work Stream 9**
Capacity building

**Synergies between incident reporting mechanisms** (i.e. GDPR, eIDAS, Telecom)

**Cybersecurity of 5G**
EC Recommendation

Wider cybersecurity cooperation issues

NIS Cooperation Group output

**Key outputs:** non-binding guidelines to the EU Members States to allow effective and coherent implementation of the NIS Directive across the EU and to address wider cybersecurity policy issues

**Examples:**

- CG Publication 01/2018 - Reference document on security measures for Operators of Essential Services
- CG Publication 02/2018 - Reference document on incident notification for Operators of Essential Services (circumstances of notification)
- CG Publication 03/2018 - Compendium on cyber security of election technology
- CG Publication 04/2018 - Cybersecurity incident taxonomy
- CG Publication 05/2018 - Guidelines on notification of Operators of Essential Services incidents (formats and procedures)
- CG Publication 06/2018 - Guidelines on notification of Digital Service Providers incidents (formats and procedures)
- CG Publication 07/2018 - Reference document on the identification of Operators of Essential Services (modalities of the consultation process in cases with cross-border impact)
- CG Publication 01/2019 - Guidelines for the Member States on voluntary information exchange on cross-border dependencies
In order to scale up the EU’s response to cyber-attacks, improve cyber resilience and increase trust in the Digital Single Market, the EU Cybersecurity Act:

- Strengthens ENISA, the European Union Agency for Cybersecurity to improve the coordination and cooperation in cybersecurity across EU Member States and EU institutions, agencies and bodies;

- Establishes an EU cybersecurity certification framework that will allow the emergence of tailored certification schemes for specific categories of ICT products, processes and services. Companies will be able to certify their products, processes and services only once and obtain certificates that are valid across the EU.
The EU CYBERSECURITY ACT – ENISA

Centre of expertise on cybersecurity

Assisting the Union institutions, bodies, offices and agencies, as well as Member States, in developing and implementing Union policies related to cybersecurity

Supporting capacity-building and preparedness across the Union

Promoting cooperation, including information sharing and coordination at Union level

Contributing to increasing cybersecurity capabilities at Union level

Promoting the use of European cybersecurity certification, and a high level of cybersecurity awareness
The EU Cybersecurity Certification Framework

The Framework enables the creation of tailored, voluntary European Cybersecurity Certification Schemes for ICT products, services and processes.

The compliance of ICT products, services and processes with specific security requirements will be assessed against relevant “certification schemes”.

3 different assurance levels: basic, substantial or high.

The conformity assessment for the basic level assurance may be performed by manufacturers or service providers themselves.
How: Establishment of an EU Cybersecurity Certification Scheme

**Certification Group**
Advises Commission on strategic priorities and Union Rolling Work Programme on Cybersecurity Certification

**Annual Union Rolling Work Programme on Cybersecurity Certification**

**European Commission**
Requests ENISA to prepare Candidate Scheme

**ENISA**
Prepares candidate scheme

**ENISA**
Consults Industry, Standardisation Bodies, other stakeholders

**European Commission**
Adopts Candidate Scheme

**European Cybersecurity Certification Group (MSs)**
Advises ENISA and may propose the preparation of a candidate scheme to **ENISA**
Cybersecurity Act - Expert Groups

- the European Cybersecurity Certification Group (ECCG), comprised of representatives from Member States appointed representatives from their competent authorities and started its work

- the Stakeholder Cybersecurity Certification Group (SCCG) which will be responsible to advise ENISA and the Commission, [call for applications](#) ended on 17 September 2019
European Cybersecurity Technology & Innovation Ecosystem

**European Competence Centre:**
- manage the funds foreseen for cybersecurity under Digital Europe and Horizon Europe 2021-2027
- facilitate and help coordinate the Network and Community to drive the cybersecurity technology agenda
- support joint investment by the EU, Member States and industry and support deployment of products and solutions.

**Network of National Coordination Centres:**
- Nominated by Member States as the national contact point
- Objective: national capacity building and link with existing initiatives
- National Coordination Centres may receive funding
- National Coordination Centres may pass on financial support

**Competence Community:**
- A large, open, and diverse group of cybersecurity stakeholders from research and the private and public sectors, including both civilian and defence sectors
EU pilots helping to prepare the European Cybersecurity Competence Network

More than €63.5 million invested in 4 projects

**CONCORDIA**
- Partners: 46
- EU Member States involved: 14
- Key words:
  - SME & startup ecosystem
  - Ecosystem for education
  - Socio-economic aspects of security
  - Virtual labs and services
  - Threat Intelligence for Europe
  - DDoS Clearing House for Europe
  - AI for cybersecurity
  - Post-Quantum cryptography

**Cyber Security for Europe**
- Partners: 43
- EU Member States involved: 20
- Key words:
  - Cybersecurity for citizens
  - Application cases
  - Research Governance
  - Cyber Range
  - Cybersecurity certification
  - Training in security

**ECHO**
- Partners: 30
- EU Member States involved: 15
- Key words:
  - Network of Cybersecurity centres
  - Cyber Range
  - Cybersecurity demonstration cases
  - Cyber-skills Framework
  - Cybersecurity certification
  - Cybersecurity early warning

**SPARTA**
- Partners: 44
- EU Member States involved: 14
- Key words:
  - Research Governance
  - Cybersecurity skills
  - Cybersecurity certification
  - Community engagement
  - International cooperation
  - Strategic Autonomy
Horizon 2020 eHealth Cybersecurity R&I

Horizon 2020 Societal Challenge 1 Work Programme – Health, Demographic Change and Wellbeing

2018 Call for Proposals on TRUSTED DIGITAL SOLUTIONS AND CYBERSECURITY IN HEALTH AND CARE

8 proposals retained for funding, and projects started early 2019

The EC funding of the retained proposals is about 35M EUR

Expected impact:

- Reduced cybersecurity vulnerability of health and care services, data and infrastructures
- Less risk of data privacy breaches
- Increased patient trust and safety
- Less human errors causing cybersecurity threats
Some relevant H2020 R&I projects

Reducing cyber risks to healthcare infrastructure and enabling secure cross-border collaborative data mining by means of privacy-preserving data mining, integrated with blockchain technology.

Toolkit and guidelines to help health care systems users address cybersecurity risks by extensive use of AI, advanced encryption and access control techniques to protect data.

The toolkit will be integrated and validated in IoT and BYOD-based case studies at two hospitals.
Tailor-made training and awareness packages (CSA)
Cybersecurity forthcoming topics in H2020 - Overview

- SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems.
- SU-DS02-2020: Intelligent security and privacy management.

and

- H2020-SU-AI-2020: Artificial Intelligence and security: providing a balanced assessment of opportunities and challenges for Law Enforcement in Europe
SU-INFRA01-2018-2019-2020
Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe

- **Type of Action:** Innovation Action
- **Budget:** 20.7 MEUR
- **Indicative EU grant:** 7-8 MEUR
- **Duration:** maximum 24 months
- **Expected final Technology Readiness Level (TRL):** 7

- At least 2 operators in at least 2 EU or Associated Countries.
- Participation of industry able to provide security solutions is required.
- GA 30.3 option to object transfer to third countries

- **Opening:** 12/03/2020, **Deadline:** 27/08/2020

email to **cnect-h1@ec.europa.eu**  Follow us on Twitter: [@Cybersec_EU](https://twitter.com/Cybersec_EU)

Funding opportunities for eHealth 2021-27

- Digital Europe Programme and Connecting Europe Facility
- Horizon Europe
- European Social Fund + and European Globalisation Adjustment Fund
- European Regional Development Fund
- InvestEU Programme
Investing in the future: Digital Europe Programme

Digital transformation & Interoperability
1.3 € billion

Advanced digital skills
0.7 € billion

Cybersecurity & trust
2 € billion

High performance computing
2.7 € billion

Artificial intelligence
2.5 € billion

€ 9.2 billion in total

#EUBudget
#DigitalEurope
‘Cyber-attacks know no borders, but our response capacity differs very much from one country to the other, creating loopholes where vulnerabilities attract even more the attacks. The EU needs more robust and effective structures to ensure strong cyber resilience and respond to cyber-attacks. We do not want to be the weakest links in this global threat.’

Jean-Claude Juncker, Tallinn Digital Summit, 29 September 2017
THANK YOU!

Twitter: @eHealth_EU

Facebook: EU.ehealth

Subscribe to our newsletter 'eHealth, Wellbeing & Ageing' via bit.ly/eHealthinFocus