The NIS Directive and Cybersecurity in eHealth

Dr. Athanasios Drougkas | Officer in NIS
Belgian Hospitals Meeting on Security | Brussels | 13th October
<table>
<thead>
<tr>
<th></th>
<th>Agenda</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The NIS Directive and cybersecurity in eHealth &amp; ENISA work in eHealth security</td>
</tr>
<tr>
<td>2</td>
<td>ENISA supporting the implementation of the NIS Directive for eHealth</td>
</tr>
</tbody>
</table>
The NIS Directive and cybersecurity in eHealth & ENISA work in eHealth security
Securing Europe’s Information society
Positioning ENISA activities

**CAPACITY**
- Hands on activities

**POLICY**
- Support MS & COM in Policy implementation
- Harmonisation across EU

**COMMUNITY**
Mobilizing EU communities

**EXPERTISE**
- Recommendations
- Independent Advice
Predicting the future: Hospitals under attack

At least 19 hospitals were infected with ransomware in Q1 and Q2.

A related group of Q1 attacks on hospitals generated $100,000 in ransom payments.

Major Cyberattacks On Healthcare Grew 63% In 2016

Number of hacks reported to HHS-OCR

Malware Shuts Down Operations at Hospitals

Sources: U.S. Department of Health and Human Services; Office for Civil Rights
The Network and Information Security Directive
Obligations for MSs on OESs

- Identification of operators of essential services
- Minimum security measures to ensure a level of security appropriate to the risks
- Incident notification to prevent and minimize the impact of incidents on the IT systems that provide services
- Make sure authorities have the powers and means to assess security and check evidence of compliance for OES
Working groups under the NISD

NIS Directive Groups

- Cooperation Group
  - Identification Criteria Subgroup
  - Security Measures Subgroup
  - Incident Reporting Subgroup

- CSIRT

ENISA
## NIS directive - TIMELINE

<table>
<thead>
<tr>
<th>Date</th>
<th>Period</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2016</td>
<td>-</td>
<td>Entry into force</td>
</tr>
<tr>
<td>February 2017</td>
<td>6 months</td>
<td>Cooperation Group starts its tasks</td>
</tr>
<tr>
<td>August 2017</td>
<td>12 months</td>
<td>Adoption of implementing on security and notification requirements for DSPs</td>
</tr>
<tr>
<td>February 2018</td>
<td>18 months</td>
<td>Cooperation Group establishes work programme</td>
</tr>
<tr>
<td>9 May 2018</td>
<td>21 months</td>
<td>Transposition into national law</td>
</tr>
<tr>
<td>November 2018</td>
<td>27 months</td>
<td>Member States to identify operators of essential services</td>
</tr>
<tr>
<td>May 2019</td>
<td>33 months</td>
<td>Commission report - consistency of Member States' identification of OES</td>
</tr>
<tr>
<td>May 2021</td>
<td>57 months</td>
<td>Commission review</td>
</tr>
</tbody>
</table>
And this is not the only legislation targeting healthcare

- **General Data Protection Regulation**
  - Implementation of security measures
  - Reporting data breaches to DPA
  - Perform Privacy impact assessment

- **Medical Devices Regulation**
  - Compliance to safety and performance requirements for medical devices manufacturers
  - Notification obligation in the case of an incident in a vigilant system
  - Use of harmonized standards
ENISA collaborates with HCO to setup pilots across the EU
Cyber Security in the Healthcare Sector – ENISA activities

- Security and Resilience for eHealth Infrastructures and Services (2015)
- Cyber Security for Smart hospitals (IoT in Healthcare) (2016)
- NISD implementation in Healthcare in the MS (on-going)
- Cloud security in eHealth (on-going) [OES-DSP dependency]
ENISA work to secure Smart Hospitals

Objectives

• Improve security and resilience of hospitals information systems
• Identify common cyber security threats and challenges and,
• Present mitigation measures to address them
• Support pilots in hospitals across the EU

Secure devices and systems to improve patients’ safety
Recommendations – For Hospitals

ENISA recommendations:

- Establish effective **enterprise governance** for cyber security
- Implement **state-of-the-art security measures**
- Provide specific IT security requirements for IoT components in the hospital
- **Invest** on NIS products over IoT components
- Establish an **information security sharing mechanism**
- Conduct **risk assessment and vulnerability assessment**
- Perform **pen testing and auditing**
- Support **multi-stakeholder communication platforms (ISACs)** and information sharing alternatives

*Invest on cyber security for IoT components*
Recommendations – For IoT devices manufacturers

ENISA recommendations:

- Incorporate security into existing quality assurance systems
- Involve third parties in testing activities
- Consider applying medical device regulation to critical infrastructure components
- Support the adaptation of information security standards to healthcare

Involve HCO throughout the whole device lifecycle
Recommendations – For Policy makers

ENISA recommendations:

- Promote collaboration on cyber security across Europe
- Develop **awareness raising** on IoT threats and risks
- Establish a **governance model** for cyber security
- Integrate (trade-off risk/investment) **security in business processes**
- Define security requirements to ensure “security for safety”

A public private partnership can lead to a better cooperation
ENISA supporting the implementation of the NIS Directive for eHealth
NISD Implementation in the Healthcare Sector in the MS - 2017

- Perform stocktaking of existing guidelines/schemes in the different Member States and international standards on cyber security in healthcare.
- Identify of baseline security measures for healthcare organisations.
- Identify incident notification approaches.
- Map interdependencies to other sectors and Digital Service Providers.

Survey on Incident Reporting open for dissemination!
https://ec.europa.eu/eusurvey/runner/IncidentReporting_OES
Identification of Baseline Security Measures for Healthcare Organisations

- Is there some NIS measure that you apply missing from this mind map?
# Identification of Baseline Security Measures for Healthcare Organisations

**NIS Measures**

- Please rate the NIS measures in terms of priority for your organisation

<table>
<thead>
<tr>
<th>DOMAIN</th>
<th>MEASURES</th>
<th>HIGH</th>
<th>MEDIUM</th>
<th>LOW</th>
<th>TOP 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance and management</td>
<td>Information security governance and management</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Information security policies and standards</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Risk management and assessment</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Compliance</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Human resource security</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td>Network and communications security</td>
<td>Secure network components</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Secure network architecture</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Remote connection security</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Communications security</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td>Asset management</td>
<td>Patch management</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Software control</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Configuration management</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Information classification and protection</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Media security</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td>Monitoring and auditing</td>
<td>Auditing and logging</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Monitoring</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Security accreditation</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td>Resilience</td>
<td>Business continuity management</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Disaster recovery management</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td>Logical and physical security</td>
<td>Identity and access management</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Physical access security</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Healthcare facilities security</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td>Incident management</td>
<td>Preparation and readiness</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Handling and response</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td>Supply chain security</td>
<td>Contractual and service agreements</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Supplier risk management</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Service delivery management</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td>Interoperability and portability</td>
<td>Mobile device security</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Application portability</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
<tr>
<td></td>
<td>Data portability</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>Select Rating</td>
</tr>
</tbody>
</table>
Identification of Baseline Security Measures for Healthcare Organisations

• Which NIS measures are implemented in your organisation and are more mature in your organisation?

• For each of the security measures of high and medium importance/maturity please provide concrete examples of physical, technical and administrative controls.
Identification of Operators of Essential Services (OES)

An Operator of Essential Services is defined as any public or private entity which:

- provides a service which is essential for the maintenance of critical societal and/or economic activities;
- the provision of that service depends on network and information systems;
- an incident would have significant disruptive effects on the provision of that service.

<table>
<thead>
<tr>
<th>Sector</th>
<th>Subsector</th>
<th>Types of entity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy</td>
<td>Electricity, Oil, Gas</td>
<td>N/A</td>
</tr>
<tr>
<td>Transport</td>
<td>Air transport, Rail transport, Water transport, Road transport</td>
<td>N/A</td>
</tr>
<tr>
<td>Banking</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Financial market infrastructures</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Drinking water supply and distribution</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Digital infrastructure</td>
<td>N/A</td>
<td>Internet Exchange Points (IXP), DNS service providers, TLD name registries</td>
</tr>
</tbody>
</table>
DSP means any legal person that provides a digital service as defined in the following:

<table>
<thead>
<tr>
<th>Types of digital services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Online marketplace</strong></td>
<td>An online marketplace allows consumers and traders to conclude online sales or service contracts with traders, and is the final destination for the conclusion of those contracts.</td>
</tr>
<tr>
<td><strong>Cloud computing service</strong></td>
<td>Cloud computing services covers services that allow access to a scalable and elastic pool of shareable computing resources. Those computing resources include resources such as networks, servers or other infrastructure, storage, applications and services</td>
</tr>
<tr>
<td><strong>Online search engine</strong></td>
<td>An online search engine allows the user to perform searches of, in principle, all websites on the basis of a query on any subject. It may alternatively be focused on websites in a particular language</td>
</tr>
</tbody>
</table>
Interdependencies of Healthcare Organisations Information Systems (1/3)

What dependencies on services provided by OES and DSP are in place with regards to:

- Business processes (e.g. finance process provided by the banking sector).

- Essential services provided (e.g. electricity provided by the energy sector).

- Information systems (e.g. provision of DNS services by providers).
Interdependencies of Healthcare Organisations Information Systems (2/3)

What are the specific services that are provided by the OES and DSP and may affect the essentials service provided by healthcare providers?

Please provide detailed information about:

• The dependencies of other sectors on the provided service (detailed description).

• The impact of dependency disruption/essential service provision and the criticality level of each one for the healthcare providers.
Interdependencies of Healthcare Organisations Information Systems (3/3)

• What practices have you adopted and what measures have you implemented in order to adequately protect the aforementioned dependencies?

• In which ways can the interdependencies be further secured from the healthcare organisations perspective? What do you consider as the most critical success factor?
Incident Reporting for OES in the context of the NIS Directive

Current incident reporting mechanisms/frameworks

Are you overseeing any type network and information security (cyber security) incident notification mechanism used within the sector/subsector selected above?

- Yes, national law
- Yes, EU regulation/directive
- Yes, international regulation
- Yes, standard (non-mandatory)
- Yes, industry standard (mandatory)
- Yes, guideline (non-mandatory)
- Yes, other mandatory initiative
- Yes, other non-mandatory initiative
- Yes, internal policy only
- No
Measuring the impact of cyber incidents

When measuring the significance of the impact of cyber incidents affecting systems used in the provision of services, which of the following parameters do you take into account?

- the number of users affected that are relying on the service provided by the operator
- the duration of the incident
- the geographical spread with regard to the area affected by the incident
- the dependency of other sectors on the service provided by the affected entity
- the impact the incident could have on economic and societal activities or public safety
- the importance of the affected entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service
- the market share of the affected entity (answer suitable only for authorities)
- none of the above
Incident Reporting for OES in the context of the NIS Directive

Measuring the impact of cyber incidents

• Please provide units of measure and thresholds used for the parameters above when determining significance of incidents:

<table>
<thead>
<tr>
<th>Unit of measure</th>
<th>Threshold for becoming critical</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>the number of users affected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the duration of the incident</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the geographical spread with regard to the area affected by the incident</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the dependency of other sectors on the service provided by the affected entity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>impact the incident could have on economic and societal activities or public safety</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the importance of the affected entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the market share of the affected entity (answer suitable only for authorities)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Incident Reporting for OES in the context of the NIS Directive

Measuring the impact of cyber incidents

• What are the most common threats causing cyber incidents in your organisation?

• What do you think are the primary root causes that determine incidents having a significant impact on the services provided (disruption of confidentiality, integrity or availability);
  - Human Errors
  - Malicious actions
  - Natural phenomena
  - System failures
  - Third party failures
  - Other types of root causes
  - Do not know
Next steps for eHealth Security in ENISA

• Support in the criteria for the identification of Healthcare organisations in the scope of the NISD

• Raise awareness in the MS through organizing workshops and dedicated meetings

• Build on the baseline security measures for healthcare organisations as required by the NISD

• Identify incident reporting mechanisms for healthcare sector

• Signify security measures for IoT devices/components supporting core healthcare services

• Establish procurement guidelines for obtaining secure systems and devices in the healthcare organisations

• Find synergies with stakeholders under the implementation of the upcoming Medical Devices Regulation
Join us at the eHealth Security Conference!

3rd eHealth Security Conference
Protecting the Hospital of tomorrow

15th November
Lisbon
Faculty of Dental Medicine
University of Lisbon
Join us!!

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
eHealthSecurity@enisa.europa.eu