


# Security and resilience for eHealth Infrastructures and Service

Dimitra Liveri

Network and Information Security Expert, ENISA

European Union Agency For Network And Information 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

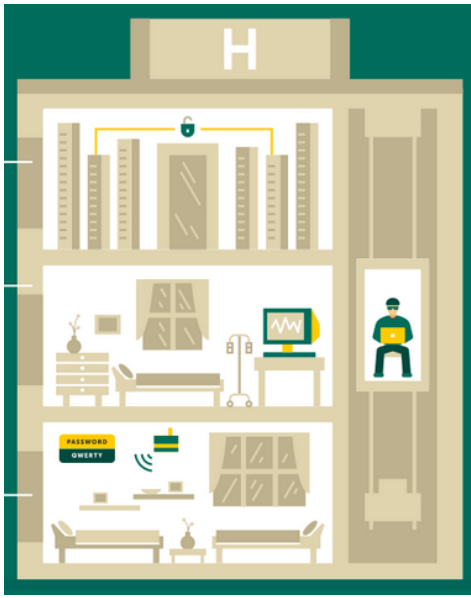
# Predicting the future: Hospitals under attack

intel Security

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

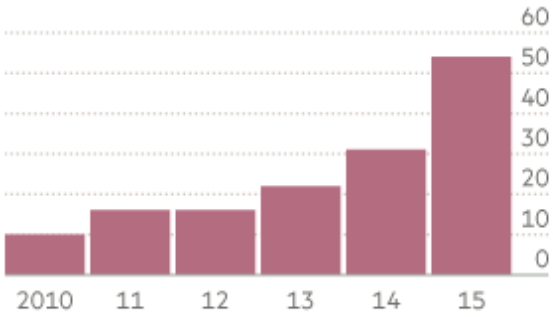
intel Security

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




Sources: U.S. Department of Health and Human Services; Office for Civil Rights

FT

# Indicative list of Incidents

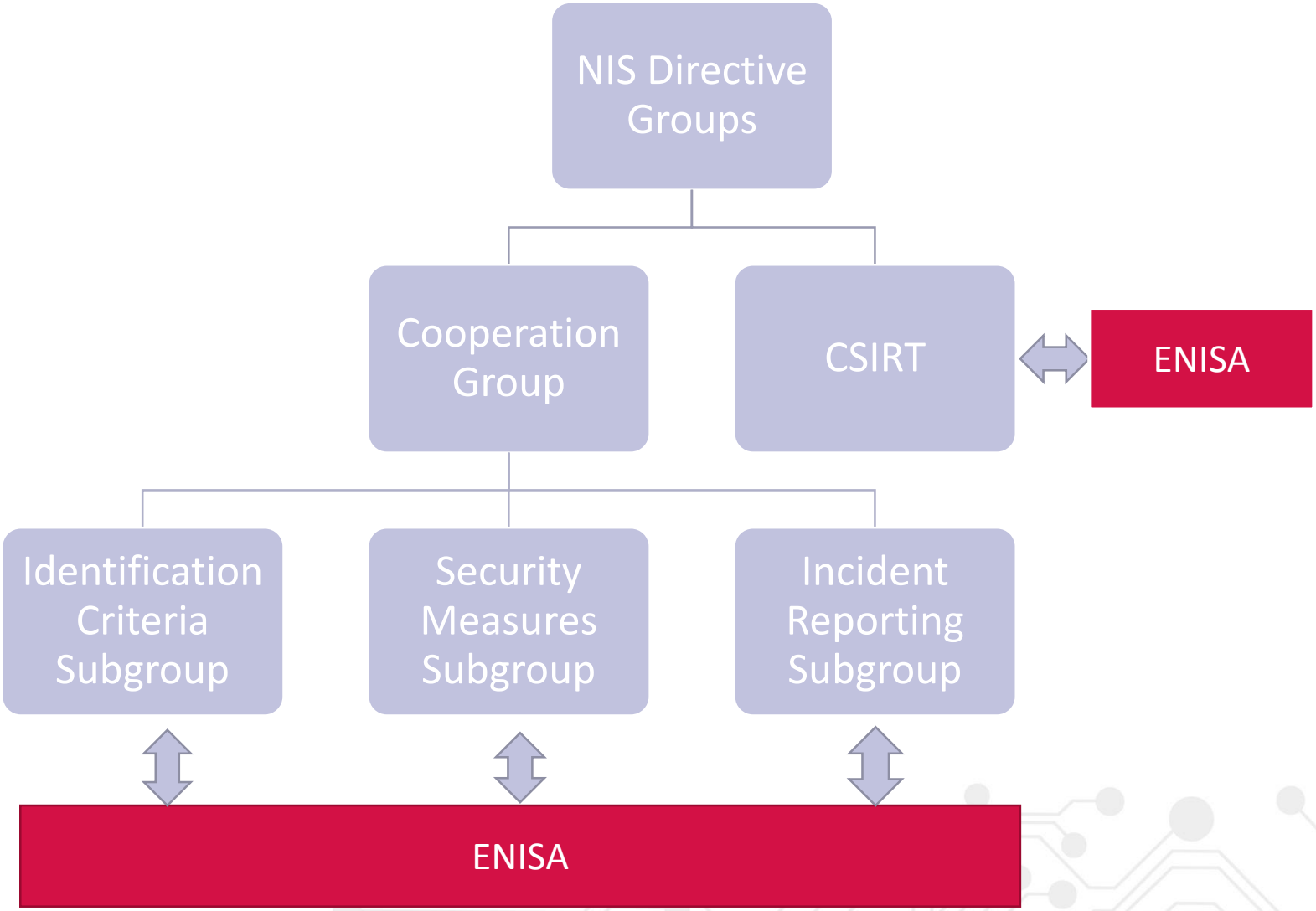
- DDoS in central Health Information System in **Finland** (KELA), causing disruption for two days.
- Two hospitals in Germany were victims of ransomware campaigns in February. Neuss-based **Lukas Hospital** did not have email access and was conducting business using pencils, paper and fax machines. **Klinikum Arnsberg hospital** was also affected by a ransomware attack.
- Hundreds of planned operations, outpatient appointments, and diagnostic procedures have been canceled at multiple hospitals in Lincolnshire, **England**, after a "major" computer virus compromised the National Health Service (NHS) .
- Theft of healthcare data in hospital in **Greece**, causing loss of data of patients.
- And many more…

# 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 - TIMELINE

| | | |
|---|---|---|
| August 2016 | - | Entry into force |
| February 2017 | 6 months | Cooperation Group starts its tasks |
| August 2017 | 12 months | Adoption of implementing on security and notification requirements for DSPs |
| February 2018 | 18 months | Cooperation Group establishes work programme |
| 9 May 2018 | 21 months | Transposition into national law |
| November 2018 | 27 months | Member States to identify operators of essential services |
| May 2019 | 33 months (i.e. 1 year after transposition) | Commission report - consistency of Member States' identification of OES |
| May 2021 | 57 months (i.e. 3 years after transposition) | Commission review |

# 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

# Cyber Security in the Healthcare Sector – situational analysis

- Healthcare organisations are considered **Operators of Essential Services** thus is scope of the NISD
- **Low maturity on cyber security** in the healthcare sector i.e. hospitals don't have a CISO
- Hospitals are **easy targets for malicious attackers** i.e. cases of ransomware attacks in hospitals across the EU, DDoS attack in Finnish ehealth system
- **Lack of security awareness** in the involved stakeholders and use of walk arounds i.e. physicians, administrative parsonel, patients etc
- **Life span of the medical devices** in use i.e. CAT scanners or MRI machines can be outdated and patch management process usually is a third party task to perform

# 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 (details…)
- Cloud security in eHealth (on going) [OES-DSP dependency]
  - Security self assessment questionnaire

# 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

# eHealth experts group

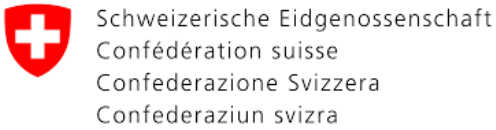
















**ENISA collaborates with HCO to setup pilots across the EU**

# Dissemination Activities

- 1st eHealth Security workshop 2015 – Brussels, together with DG CNCT H3
- 2nd eHealth Security workshop 2016 – Vienna, together with the Hospitals Association of Vienna
- Session moderation during eHealth Week 2017, speaking slot at eHealth Network meeting 2017
- Mini workshops with stakeholders around the EU MS
- 3rd eHealth Security workshop 2017 – location tbc

# 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!!

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

eHealthSecurity@enisa.europa.eu