ECS

EUROPEAN CYBER SECURITY ORGANISATION

HEALTH: CHALLENGES AND NEEDS (European Cyber Security Organisation)

24 January 2019

SWG3.6 Healthcare

OBJECTIVES

1. Understanding of health stakeholders' needs and suppliers' available (innovative) solutions / services / technologies
2. Provide inputs to other ECSO WGs to guide their activities based on cybersecurity needs and challenges.
3. Identify key cybersecurity challenges
4. Identify key issues for market uptake of innovation
5. Improvement of trust and facilitation of information exchange

MAIN ACTIVITIES

1. Fostering a trusted community of healthcare stakeholders through:
    1. Encouraging ECSO membership
    2. Liasion with other health organizations
    3. Dissemination of the SWG activities and creating contacts
2. Identifying trends in the health market as well as cybersecurity needs and challenges in different fields: technical solutions, architectures, frameworks, standards, education and awareness, etc.
3. Proposing innovation areas for the next years

Health Cybersecurity: Context

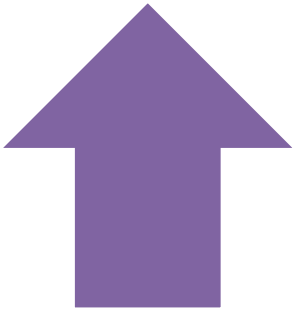
Aging society which increases healthcare costs. 70% spent in chronic diseases.

eHealth is a good solution to contain these costs while offering a better service.

eHealth is expected to have a substantial growth in the upcoming years.

Privacy, integrity and resilience are probably the key aspects to generate the required Trust in eHealth services.

Increase in cyber attacks. Impact estimated in six billion per year.



Health Cybersecurity: Market

eHealth market is expected to reach over 280.000 million Euro by 2022 (http://www.grandviewresearch.com/industry-analysis/e-health-market)

Fields:

- Health Analytics and BigData in Health
- mHealth
- TeleHealth
- Integrated Electronic Health Records
- eLearning in eHealth
- Social Media in Health

Health Cybersecurity: Challenges

1. Increase in cyberattacks
2. Aging society favours eHealth services
3. Patient ecosystem: delocalized network of care services
4. Medical devices cybersecurity
5. Trust in eHealth shall be obtained through: privacy, integrity and resilience of services.
6. Trends towards exploitation of health BigData <-> privacy
7. An EU integrated Electronic Health Record <-> heterogeneous legislation within Europe

Health Cybersecurity: Needs

Key levers for the following years:

1. **My data, my decisions.** Patients and institutions share their data with flexible consent mechanisms.
2. **Liberate the data**. Health outcomes and performance data will be freely published with full transparency.
3. **Revolutionise health**. Technology and information management drives the pace of change.
4. **Connect up everything**. This will link the lifestyle data with health data by means of lots of new apps and tools.
5. **Include everyone**. In other words, the contribution and benefits from eHealth for all.

CONTACT US

European Cyber Security Organisation 10, Rue Montoyer
1000 – Brussels – BELGIUM

www.ecs-org.eu

Phone:
+32 (0) 27770256

E-mail:
Dr. Julio Vivero
Healthcare SWG3.6 Chair
jvivero@gmv.com

Follow us
Twitter: @ecso_eu