CYBERSEC4HEALTH

SPHINX
A Universal Cyber Security Toolkit for Health-Care Industry

WORKSHOP ON CYBER SECURITY SITUATION AWARENESS FOR HEALTH ORGANIZATIONS

Meeting place: Vrije Universiteit Brussel

Presenter name: Christos Ntanos

Presenter organisation: National Technical University of Athens, SPHINX Coordinator

Date: 10/07/2019

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

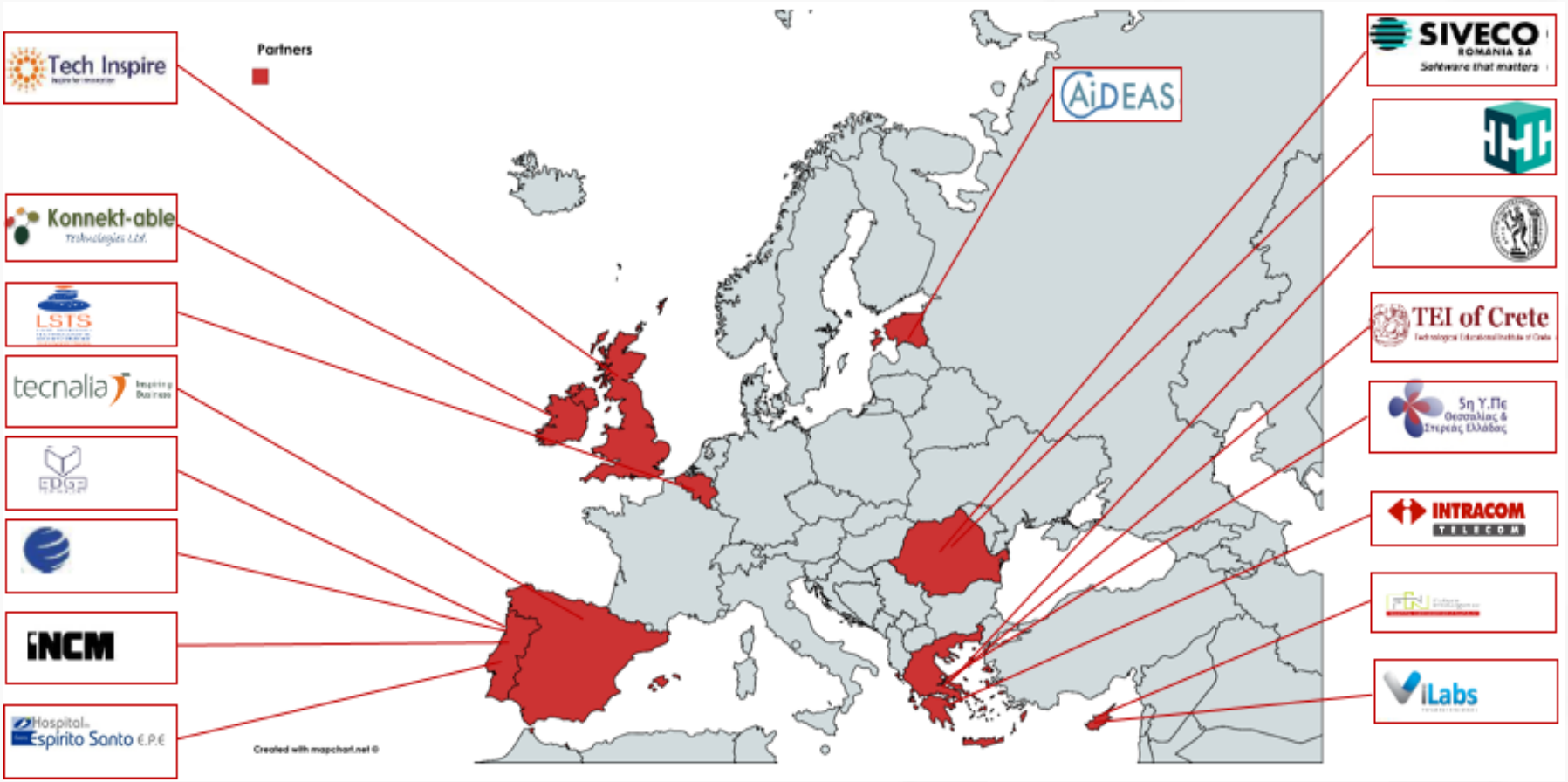
SPHINX at a glance

SPHINX aims to introduce a health tailored Universal Cyber Security Toolkit, thus enhancing the cyber protection of the Health and care IT Ecosystem and ensuring patient data privacy and integrity

- Provide an automated zero-touch device and service verification toolkit
- Adapt or embed on existing infrastructures
- Provide cyber-security services through the SPHINX cyber-security toolkit, in a secure and easy-to-use interface
- Address the threats to public critical infrastructure and cyber terrorism

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

SPHINX consortium



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

SPHINX POSITIONING

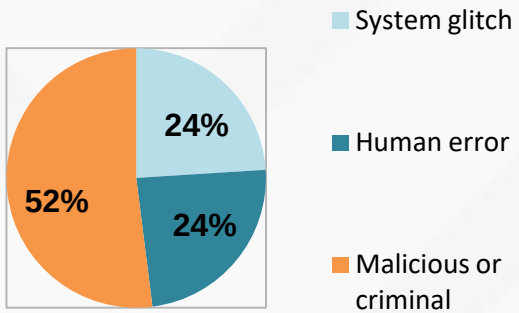
Breached Health Data

- Hospitals and care centres store and exchange large amounts of sensitive patient data, so they are prime targets for cyber criminals
- Medical devices and wearables collecting personal data, become more sophisticated and connected
- Vulnerability of the increasing healthcare ecosystem brought by smartphones

Threats
Advanced persistant threats
Ransomware
Human threat
DDoS
Lost info
Active attacks
etc.

FACTS

- Electronic medical records could be worth up to $USD 1000
- WannaCry caused the "biggest ransomware attack in history" with 57,000 infections in 99 countries, which included several hospitals
- Only in 2014, almost 1.6 million people in the U.S. had their medical information stolen from healthcare providers
- Predictions for more than 25 million people, will have their medical and/ or personal information stolen from their healthcare provider's digitized records between 2015 and 2019



Source: Ponemon

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing

WORKSHOP APPROACH

Agenda

Hospital Landscapes

- Improved security of Health and Care services, data and infrastructures

Technological Solutions

- Less risk of data privacy breaches caused by cyberattacks

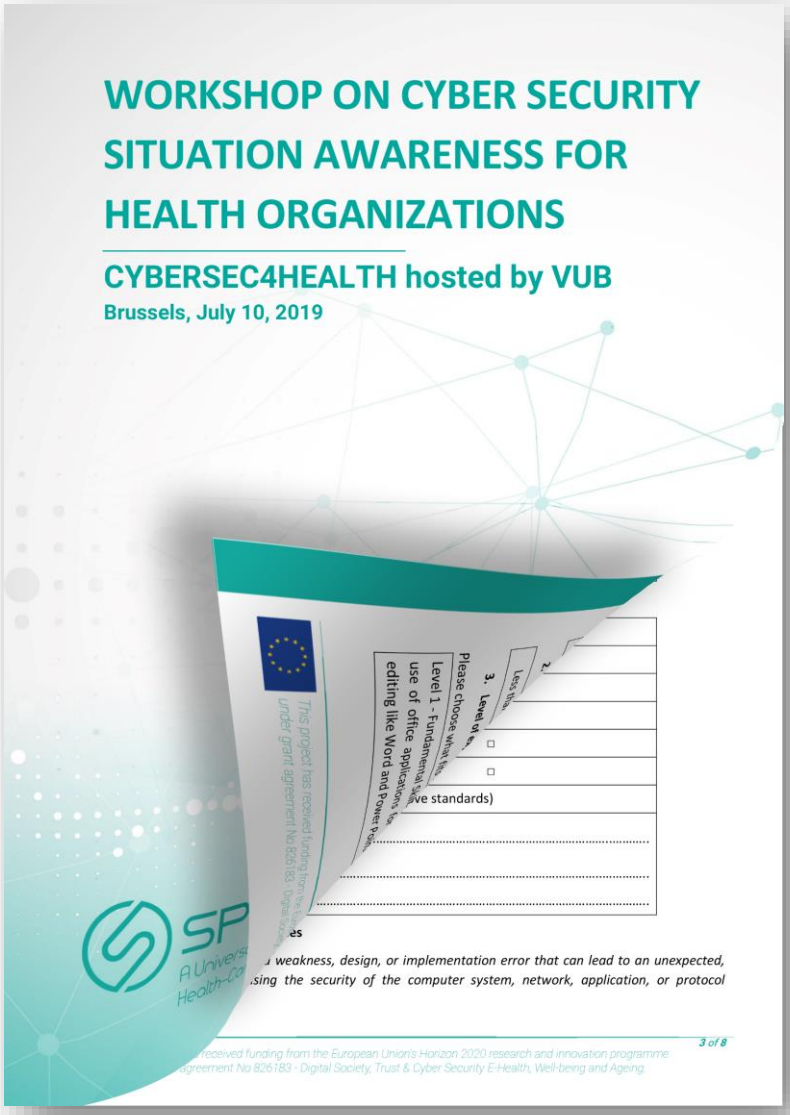
Knowledge management Seminar

- Increased patient trust and safety through Legal and Technological toolset

Clustering Event & Requirement Validation

- United we thrive

Questionnaire



Aims

- Cyber-security/InfoSec awareness level per role
- Better understanding of the needs and requirements of stakeholders
- Existing infrastructure
- Needs and requirements for proposed solutions

Notes

- The questionnaire is anonymous
- Don’t worry if you don’t recognise some jargon. We don’t expect everyone to know it.
- Be open (without becoming a vulnerability yourself)
- Ask questions.

SPHINX
A Universal Cyber Security Toolkit for Health-Care Industry

Onwards to Session one!

https://sphinx-project.eu

Twitter: https://twitter.com/ProjectSphinx

Facebook: Sphinx-project.eu

LinkedIn page: linkedin.com/company/sphinx-project

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183
Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing