CYBERHIMPREX CASE STUDY

Results and Lessons Learned

from a Digital Europe Programme Project

April 2025

CYBERHIMPREX
Cybersecurity of Healthcare
Improved in a X-border perspective

Cybersecurity of **H**ealthcare **Impro**ve**d** in a **X**-border perspective
https://cyberhimprex.policlinicogemelli.it

This project has received funding by the European Union Digital Europe Programme (DIGITAL) under grant agreement No. 101101322

Table of Content

List of tables

Disclaimer

Executive Summary

CYBERHIMPREX is a European Union investment project 50% co-funded under the DIGITAL EUROPE Programme, implemented from January 2023 to April 2025 by three healthcare organizations coordinated by the Università Cattolica del Sacro Cuore: Fondazione Policlinico Universitario A. Gemelli IRCSS, Fundació Privada Hospital Asil de Granollers and Seventh Healthcare Region of Crete.

This document is a Case Study about the CYBERHIMPREX project, aiming at sharing the results and the lessons learned with the relevant target audience

The project had the purpose to increase the cybersecurity of the involved organizations, to cope with the **healthcare sector challenges**, including

- **Structural challenges**. The *attack surface of HCOs is wide and dynamic*
- **Behavioural challenges.** Most of the staff working in the healthcare sector consider cybersecurity as a burden and distraction from treating patients effectively. This leads to *risky human behaviours*
- **Emergency related challenges**. The *COVID-19 pandemic* has amplified and made manifest risky situations for healthcare organisations (such as smart-working and telemedicine) when big emergencies hit
- **Regulatory compliance challenges**. Cybersecurity is an essential part of a high-quality healthcare service and is therefore a priority that the HCOs, also being Critical Infrastructures, comply with *European regulations and guidelines***.**

The project has delivered **outputs to strengthen three areas**, as summarized in the following table.

Strengthened area	Initiative	Key outputs
People	Basic technical training	• 27 ICT staff trained with a 80 hour course to get the CISCO CCNA SECURITY certification
	Specialized technical training	• 64 ICT staff trained with at least one of 6 courses specialization courses (on line, interactive) of 16-48 hours each
	Staff awareness	• A novel questionnaire to periodically map the cybersecurity awareness • 2.949 staff members trained with a 1.8-hour e-learning package
Organization and processes	Cyber Angels role	• Job profile of a role acting, while running her/his normal in her/his Unit, as the interface between the Unit's colleagues and the CISO and DPO)
	Cybersecurity by procurement (for software and medical devices)	• Detailed map of existing standards and regulatory documents to the 30 ENISA Good Practices • Cybersecurity requirements and examples of tools to be used in the procurement, deployment and assistance processes.
Technology	Endpoints reinforcement	• All workstations' Operating Systems have been updated

At initiative level the **value and the lessons learned** that can be relevant for the stakeholders are summarized in the following table

Strengthened area	Initiative	Value and Lessons learned
People	Basic technical training	1) The course is a low cost means for enhancing cybersecurity knowledge and awareness within the ICT departments 2) It contributes to comply with the Art. 21 item 2 of the NIS 2: "*the measures shall include … the basic cyber hygiene practices and cybersecurity training*" <u>Lessons learned</u>

		When designing and planning the training, make sure to 1) Match the course content with the staff roles 2) Enhance the course with practical exercises 3) Insist in certifying the knowledge gained 4) Involve professionals from the Clinical Engineering 5) Repeat the course after time as part of lifelong education
	Specialized technical training	<u>Value</u> The National Cybersecurity Authorities (NCAs) could recommend the training portfolio to 1) Diffuse a common background on cybersecurity 2) Ensure quick and correct up-taking of cybersecurity policies 3) Comply with NIS 2 on "*the cybersecurity training*" <u>Lessons learned</u> When designing and planning the training, make sure to 1) Match the course content with the staff roles 2) Consider the peculiarities of the medical devices 3) Involve also professionals from the Clinical Engineering.
	Staff awareness	<u>Value</u> The questionnaire is healthcare-specific informative and action oriented. NCAs could recommend it to all the HCOs of their countries, as a quick manner to 1) Assess the cybersecurity awareness 2) Identify the key actions to be done to raise the cybersecurity awareness of the healthcare staff across the country 3) Comply with NIS 2: "*the basic cyber hygiene practices and cybersecurity training*" <u>Lessons learned</u> Make sure to 1) Correctly formulate the questions in the local and organization's language 2) Include in the target population of the survey not only the HCO employees, but also to other staff (e.g. residents) 3) Collect open input (e.g problems, suggestions)
Organization and processes	Cyber Angels role	<u>Value</u> The Cyber Angel is a means to reach every staff member, through a manageable number of local interfaces between staff and the central functions responsible for the cybersecurity, thus coping with 1) Work culture that consider cybersecurity as a burden, 2) Staff rotation and new employees being hired. 3) Poor attention to password management. <u>Lessons learned</u> 1) The initiative to set up the Cyber Angel network should be managed jointly between ICT, DPO and HR. 2) Make sure that the persons selected as Cyber Angels are popular among the colleagues and are interested to the role
	Cybersecurity by procurement (for software and medical devices)	<u>Value</u> 1) The initiative strongly contributes to practically align the European HCOs with the ENISA good practices.

		2) The initiative contributes to the compliance with the NIS 2, "*Member States .. encourage the use of European and international standards and technical specifications relevant to the security of network and information systems*." 3) Some of the output can be used not only by the HCOs, but also by the suppliers, to be better compete in the tendering processes. 4) ENISA and the NCAs could invite all the HCOs, or the healthcare procurement agencies, to use the results of this initiative. Lessons learned We recommend other HCOs willing to implement a similar initiative to 1) Start the project from a gap analysis vs the 30 ENISA good practices, exploding each practice into the more detailed items 2) Assign to the project a multi-functional team, including ICT, Clinical Engineering, Legal Affairs, Procurement 3) Consider different procedures if needed (e.g. for clinical studies)
Technology	Endpoints reinforcement	Value These types of interventions bring value because 1) Set technical barriers to risky behaviours 2) Make possible to analyse more easily relevant information about events or errors that occurred over a certain period 3) Are an opportunity to clean and change the workstation technology also at hardware level 4) Allow to more easily integrate the workstations with the most advanced system agents, for functional and security purposes Lessons learned 1) When planning intervention involving all the workstations, consider that he rate of deployment may be lower than expected, 2) It is recommended to avoid the risk of limiting some necessary access to the web by some types of workers

From the **project as a whole** four types of indications can be extracted.

1) For up-taking the EU innovative projects results

The project has shown that it is possible to up-take innovative project results.
However, during the project some obstacles emerged and is recommended to the European Commission

- Make sure that the Project Officers play an active role in promoting the "peer" project collaboration
- Make eligible the full cost of the equipment, and not only the depreciation cost
- Define an "early-adoption" type of funding mechanism, to facilitate the adoption of innovative solutions produced by EU innovation actions (Research and Innovation Actions-RIA, Innovation actions-IA)
- Explore, when the IA or RIA project ends, the possibility to explicitly link, at least in case of methodologies, the ownership to the researchers.

2) For implementing a systemic approach and pursuing the regulatory compliance

Many European projects develop solutions that are systemic in nature. Even if they develop solutions that can be marketed individually, they would bring a much higher value if they were up taken as a system. But this is difficult, because each partner has its own priority and it is quite impossible to set-up a sustainable joint exploitation model.

It is recommended:

- To the European Commission to define a mechanism to fund (or facilitate) the creation of formal post-project continuation of the Consortium.
- To the NCAs to promote the systemic investments for cybersecurity.
- To the HCOs to plan the cybersecurity investments in a systemic perspective, also taking into account the results of their cybersecurity Audits

3) **For pursuing the regulatory and standardization compliance**

A trigger for investments is the need of the HCOs to comply with the regulations (in particular NIS 2, CRA, MDR) and the accreditation schemes, e.g. those of the Joint Commission International (JCI). For CYBERHIMPREX this has helped in ensuring the continuous support from the management.

It is recommended to the HCO:

- To monitor the progress of the regulatory and standardization landscape during the life of the project, to promptly identify new needs
- To identify, through a gap analysis, the regulatory, standardization and accreditation targets, to better shape the investment project
- To ensure and track the fulfilment of the targets during the project

4) **For an effective project implementation**

The CYBERHIMPREX project has been structured in three Work Packages: Coordination, Procurement, Implementation. From the project management point the key issue have been the “silos” behaviours, with impact on the time, mainly for the procurement activities. This has driven delays in implementation and in the possibility to deliver a content-rich dissemination.

It is recommended to the HCO to

- Ensure the deep involvement of all the relevant internal functions (ICT, Clinical Engineering, DPO, Procurement, Legal Affairs, Internal Audit), in the project design and implementation
- Agree with the Procurement Department a “fast track” procedure, appoint the reference persons for the steps of the procedure, do periodic meetings
- Anticipate as much as possible the involvement of the potential suppliers, to mitigate their low responsiveness and the complexities of the registration procedure of new suppliers (foreigners).

Acronyms

Acronym	Description
FPG	Fondazione Policlinico Universitario A. Gemelli IRCSS
FPHAG	Fundació Privada Hospital Asil de Granollers
HCO	Healthcare Organization
NCA	National Cybersecurity Authority (or Agency)
7HRC	Seventh Healthcare Region of Crete
UCSC	Università Cattolica del Sacro Cuore

1. Introduction

The CYBERHIMPREX project has been co-funded by the European Union Digital Europe Programme (DIGITAL) and has had the purpose of improving the cybersecurity capabilities of the three Healthcare Organizations

Healthcare Organizations (HCOs) partners of the CYBERHIMPREX consortium. The project has been implemented from January 2023 to April 2025.

This document is a Case Study about the CYBERHIMPREX project, aiming at sharing with the relevant target audience

- European Healthcare Organizations (HCOs)
- European and National policy makers and agencies, including the National Cybersecurity Authorities/Agencies (NCAs).
- Supply chain actors

the

- description of the project in terms of results, highlighting the aspects that may be of value for them
- lessons learned and recommendations that may help to successfully facilitate, promote, support, fund, plan and implement investment projects aimed to increase the cybersecurity resilience of the HCOs 1) up-taking the EU innovative projects results, 2) implementing a systemic approach, 3) pursuing the regulatory compliance

The document is structured in the following manner:

- Section 1 provides purpose, scope and structure of the document
- Section 2 provides a quick overview of the challenges that the partners of the project wanted to address co-investing in the CYBERHIMPREX project
- Section 3 provides a quick introduction to the CYBERHIMPREX project, in terms of origin, funding framework, purpose and scope, partners and actors involved and a summary of the six initiatives that have been implemented, clustered by the factors impacting the cybersecurity level of an organization (people, organization/processes, technology)
- Section 4 provides, for each initiative, the key results, their value for the target audience and recommendations for their implementation or adoption in other HCOs of the project
- Section 5 provides, for the overall project, valuable takeaways and recommendations that can help European HCOs and policy makers to ensure, through similar projects, higher cybersecurity resilience through the uptake of EU projects' innovations, holistic approach, regulatory compliance

2. The challenges

According to the European Commission "in 2023 alone, EU countries reported 309 significant cybersecurity incidents targeting the healthcare sector – more than any other critical sector. As healthcare providers increasingly use digital health records, the risk of data-related threats continues to rise. Many systems can be affected, including electronic health records, hospital workflow systems, and medical devices. Such threats can compromise patient care and even put lives at risk"[1].

Coping with this scenario requires that the Healthcare Organizations (HCOs) increase their capability to address challenges specific to their sector[2]:

- **Structural challenges**. The *attack surface of HCOs is wide and dynamic* because of the multiplicity of connected endpoints, increasing digitalization, many non-secure legacy medical devices and increasing levels of inter-organisational data sharing. The hospitals' working areas (and endpoints) may be easily accessed by many non-workers (patients, their relatives; students, in case of university hospitals): this is a characteristic of hospitals, this does not happen in the other sectors
- **Behavioural challenges.** Most of the staff working in the healthcare sector consider cybersecurity as a burden and distraction from treating patients effectively. This leads to *risky human behaviours*. According

[1] https://commission.europa.eu/news/bolstering-cybersecurity-healthcare-sector-2025-01-15_en
[2] Updated version of an analysis included in https://www.panacearesearch.eu/news/lessons-learnt-panacea-cyber-protection-hospitals-and-care-centres

to ENISA,[3] "healthcare end-users assess that, despite underreporting, social engineering threats remain a significant concern for the sector, calling for increased awareness raising campaigns. Phishing amounted to 8% of the significant health-related incidents reported under the NIS directive in 2021 and 26% in 2022". The Joint Commission International (JCI) Accreditation Standards for Hospitals and Academic Medical Centers includes the phishing among the key risks to be mitigated to get accreditation.

- **Emergency related challenges**. The *COVID-19 pandemic* has amplified and made manifest risky situations for healthcare organisations (such as smart-working and telemedicine) when big emergencies hit, pushing known malware taking new forms or using COVID-19 to boost their social engineering tactics[4], bringing also new risks, such as the fast onboarding of new staff, and the need to quickly turn non-healthcare sites, e.g., hotels, into structures for healthcare operations.
- **Regulatory compliance challenges**. The *mission of the HCOs, together with thire nature of Critical Infrastructure*, more than for any other industry, implies that cybersecurity is not only financially, but also socially relevant in that successful cyber-attacks have a high impact not only on data privacy but also on quality of care, and patient safety. Cybersecurity is thus an essential part of a high-quality healthcare service and is therefore a priority that the HCOs comply with *European regulations and guidelines* such as the Directive on Security of Network and Information Systems (**NIS 2**), Cybersecurity Resilience Act (**CRA**) General Data Protection Regulation (**GDPR**) and their National implementations, Medical Device Regulations (**MDR**) and the related MDCG-16-Guidance on Cybersecurity for medical devices, **ENISA Procurement Guidelines** for Cybersecurity in Hospitals, **European action plan on the cybersecurity of hospitals and healthcare providers.**

3. The CYBERHIMPREX project

To address above challenges, the CYBERHIMPREX project[5] has been set-up to implement a set of initiatives acting on technical, organizational/governance and human aspects.

CYBERHIMPREX project has been co-funded (50%) by the European Commission under the Digital Europe Programme[6], which has the goal of strengthening the capabilities of the Union for resilience and protection of its citizens and organisations aiming - amongst others - to improve the security of digital products and service. One of the purposes of the European funding has been to promote the adoption of market-ready innovative cybersecurity solutions, including solutions developed in the framework of EU-supported research and innovation projects. The project has therefore been an opportunity for HCOs that had been partner in two Horizon 2020 (H2020) projects (PANACEA[7] and CUREX[8]) to act as early adopters of some of the solutions that they had contributed to develop with the role of end-users.

The project has been implemented by a consortium coordinated by the Università Cattolica del Sacro Cuore (UCSC), Italy, and includes three HCOs: Fondazione Policlinico Universitario A. Gemelli IRCSS (FPG)[9] in Italy, Fundació Privada Hospital Asil de Granollers (FPHAG) in Spain, 7th Health Region Crete (7HRC) in Greece.

The UCSC is one of the most renowned universities and medical schools in Italy for its academic excellence. It has coordinated the H2020 PANACEA project

[3] European Union Agency for Cybersecurity (ENISA), "ENISA THREAT LANDSCAPE: HEALTH SECTOR (January 2021 to March 2023)," 05 06 2023
[4] Interpol, GLOBAL LANDSCAPE ON COVID-19 CYBERTHREAT, April 2020
[5] https://cyberhimprex.policlinicogemelli.it/
[6] The project is co-financed (50%) by the European Commission (EC) under the topic DIGITAL-2022-CYBER-02-SUPPORTHEALTH of the Digital Europe Programme (DIGITAL).
[7] https://panacearesearch.eu/
[8] https://www.kios.ucy.ac.cy/projects_kios/curex-innovative-solutions-for-the-protection-and-security-of-health-data/
[9] FPG is the teaching hospital of UCSC

The FPG is an Italian academic hospital operating in all areas of health and clinical care and is one of the most important and internationally acclaimed healthcare providers in Italy. FPG has brought extensive experience and expertise on all facets of cybersecurity in healthcare, testing the tools developed in the H2020 PANACEA project.

The FPHAG is a Spanish healthcare, socio-sanitary and social care centre, integrated into the comprehensive healthcare system of Catalonia. Is made up of the Geriatric Center Adolfo Montaña and the General Hospital of Granollers, which provides health care assistance both for acute and non- acute patients. It has been partner of the H2020 CUREX project

7HRC is the Greek regional authority responsible for the specification development of health policies for Crete Iland. It is the only health region in Greece operating an Integrated Health Information System used by all hospitals and primary health care units, spanning Health Centres and Urban Primary Health Care Units, which are interconnected. It has been partner of the H2020 PANACEA project .

The project has been implemented from January 2023 to April 2025, with a final cost of about 2 M€[10]

It has implemented six initiatives, which, following the NIS 2 systemic approach[11], act on three areas, as summarized in the following Table 1.

Table 1 Summary of the initiatives by strengthened area

Strengthened area	Initiative	Key outputs
People	Basic technical training	• 27 ICT staff working at 7HRC trained with a 80 hour course (on line, interactive) on topics regarding cybersecurity to get the CISCO CCNA SECURITY certification
	Specialized technical training	• 64 ICT staff working at FPG trained with at least one of 6 courses specialization courses (on line, interactive) of 16-48 hours each
	Staff awareness	• A novel questionnaire to periodically assess cybersecurity awareness level across the HCO, used to do a survey: 1.814 staff members responded, i.e. 29% of the invited • Awareness map, built using the results from the survey • Plan for awareness raising, based on the map • 2.949 staff members trained with a 1,8-hour e-learning package, i.e. 46% of the invited
Organization and processes	Cyber Angels	• Job profile of a role (the Cyber Angel) acting, while running her/his normal duties (clinical, technical, administrative) in her/his Unit, as the interface between the Unit's colleagues and the CISO and DPO)
	Cybersecurity by procurement (for software and medical devices)	• Detailed map of the standards and regulatory documents to be considered when aligning the procurement and assistance processes with the 30 ENISA Good Practices[12] • Alignment with the 30 ENISA Good Practices, through ✓ Cybersecurity requirements (regarding both products and suppliers) to be inserted in Requests for Proposal and Contracts

[10] The cost includes both the cost of the procured services and cost of the HCOs personnel, corresponding to about 180 Person Months (including about 55 PMs for the participation as trainee to the trainings).

[11] NIS 2-Article 21: "*1.Member States shall ensure that essential and important entities take appropriate and proportionate* ***technical, operational and organisational measures*** *to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services*".

Whereas (78): "*Cybersecurity risk- management measures should* ***provide for systemic analysis, taking into account the human factor****, in order to have a complete picture of the security of the network and information system*."

[12] ENISA*, Procurement guidelines for cybersecurity in hospitals,* February 2020

		✓ Categorization and examples of tools (for technical testing and compliance validation) supporting the procurement process ✓ Guidelines for deployment, with focus on the supplier's responsibilities ✓ Guidelines for assistance, with focus on the supplier's responsibilities ✓ Embedding in the procurement process the mandatory involvement of a cybersecurity & privacy committee
Technology	Endpoints reinforcement	• All workstations' Operating Systems have been updated

4. The results, their value and lessons learned from the initiatives

4.1 Basic technical training

Goal and scope

The main purpose of this initiative has been the training of the ICT staff working at the 7HRC (Central Administration, hospitals) to make them aware of the necessary scientific specialization in the fields of Digital Systems Security, Cybersecurity and protection of the IT infrastructure of public healthcare providers in the region of Crete.

Results

The initiative has consisted in defining, procuring and delivering one on-line 80-hours course (see the content in Table 2) during to a target population of 27 ICT professionals, which have interacted on-line with the trainers[13] through a well-structured curriculum combining theory and practice to achieve the expected learning outcomes. The course was implemented through an electronic platform, remotely, with answering questions and parallel practical training of the participants in real time with the assistance of the trainer. The Packet Tracer tool was used to create a virtual network, offering the trainees the opportunity to be trained in real network conditions without the need for physical infrastructure and associated costs.

Table 2-Basic technical training: key features

Course title	Key target participants	Duration (hours)	Topics
Implementation and management of CISCO Security Solutions (CCNA SECURITY V1.0)	ICT Staff	80	• Introduction to CISCO Security Technologies and Solutions. • Modern Network Security Threats • Securing Network Devices • Authentication, Authorization and Accounting • Access Control Lists • Intrusion Prevention Systems • Securing the LAN • Cryptographic Systems & Services • Implementing VPNs • Adaptive Security Appliance Introduction & Implementation • Introduction to ASDM • Managing a Secure Network

Value for the target audience

[13] The training has been delivered by the Research Centre of the University of Piraeus. The training package had been developed in the H2020 CUREX project

1) The course implemented by the 7HRC through the procurement of scientific expertise from the University of Piraeus and the certification of the Cisco Academy could be considered as a tool for enhancing cybersecurity knowledge and awareness within the ICT departments of the HCOs, with a limited cost (as an average: less than 700 € per person). This knowledge ensures that ICT staff have identified cybersecurity concepts and attacks as a core issue that needs to be addressed, continuously monitored and constantly scientifically evolving.
2) The fact that the course involved participants from different HCOs settings in the region of Crete has spread the importance of cybersecurity at regional level. Given the lack of equivalent training at regional level across Greece and the certified outcome, it could also be recommended as a training strategy by the NCAs to all the HCOs of their countries, public and private, as a quick manner to:
    - get robust, well-trained ICT departments
    - underline the importance of cybersecurity investments
    - ensure that every new national cybersecurity policy is easily up taken and correctly implemented
    - indirectly push the suppliers to provide more secure software applications, medical devices and assistance services.
3) The methodology applied contributes to comply with the Art. 21 item 2 of the NIS 2: "*the measures shall include … the basic cyber hygiene practices and cybersecurity training*"

Lessons learned

When designing, procuring and implementing the training, make sure to:

- assess prior knowledge of participants and match the content of the course with their roles and existing infrastructure
- enhance the course with practical exercises and scenario hands-on solutions
- ensure the active participation of the participants throughout the course and insist in certifying the knowledge gained by taking the respective certification exams
- involve as participants also professionals from the Clinical Engineering, both those that procure new medical devices and those that manage them during their life and phase out
- repeat the course after time as part of lifelong education
- give incentives to ICT staff to participate into equivalent or more advanced courses.

4.2 Specialized technical training

Goal and scope

The main goal of this initiative has been to improve the cybersecurity skills of staff working in the Information and Communication Technology (ICT) at FPG, through a training package made up of courses aimed at increasing their knowledge and awareness in the cyber security domain, considering the starting expertise level and the role played by each person. The concept driving the content and the target population is that all the ICT professionals (development project managers, architects, operations staff, helpdesk staff) must be aware of cybersecurity issues and risks, even if they are not directly playing cybersecurity management roles.

Results

The initiative has consisted in defining, procuring and delivering 6 courses (see Table 3) to a target population of 64 ICT professionals, which have interacted on line with the trainers and performed some exercises.

Table 3 Specialized technical training: key features

Course title	Key target participants	Duration (hours)	Topics
NIST & Cybersecurity	IT Managers and coordinators	16	• Standard ISO/IEC 27001:2022 NIST Cybersecurity Framework
Cyber risk analysis	IT supervisors	24	• Analysis of the cyber-risks related to IT projects
Secure coding web application	Software Developers	24	• Secure coding • Security by design (GDPR)
Threat hunting	Cybersecurity team	32	• Threat hunting • Incident response
CompTIA Security+	ICT staff	40	• Cyber security concepts, • Threats, vulnerabilities & mitigations, • Security architecture, Security operations
Certified Ethical Hacker (CEH)	Cybersecurity team	48	• Ethical hacking, Vulnerability assessment • Penetration test

Value for the target audience

1) The portfolio of trainings adopted by FPG could be taken as a quick manner to diffuse a cybersecurity knowledge base and awareness within the ICT departments of the HCOs, with a limited cost (as an average: less than 1.000 € per person).

   This knowledge makes sure that the specialized cybersecurity roles find in all their ICT colleagues the due collaboration when procuring and operating cybersecure information services

   The portfolio could be taken an example by individual Healthcare Organizations (HCOs)

2) We think that It could also be recommended by the National Cybersecurity Authorities (NCAs) to all the HCOs of their countries, public and private, as a quick manner to

   - establish across all the ICT departments of the country a common background for managing the information systems in a cybersecurity perspective
   - ensure that every new national cybersecurity policy is easily up taken and correctly implemented
   - indirectly push the suppliers to provide more secure software applications, medical devices and assistance services.

3) The methodology applied contributes to comply with the Art. 21 item 2 of the NIS 2: "*the measures shall include … the basic cyber hygiene practices and cybersecurity training*"

Lessons learned

3) When designing and planning the training, make sure to

   - match the content of the course with the roles of the participants
   - consider the peculiarities of the medical devices
   - involve as participants also professionals from the Clinical Engineering, both those that procure new medical devices and those that manage them during their life and phase out.

4) Both the training supplier and the HCO must be flexible, to cope with the high and unpredictable workload of the IT staff. This is quite important for the training sessions that require the set-up of simulation environments: these sessions may have a high cost and the training delivery would inefficient if not all the planned participants do not attend.

4.3 Staff awareness raising

Goal and scope

The main goal of this initiative has been to raise the awareness of all types of HCO staff (nurses, doctors, residents, admin, technical staff) through:

- Assessment of current behaviour-related risks and of the cybersecurity awareness, contextualizing two methodologies developed by two H2020 projects (SBNT[14] of PANACEA, CH[15] of CUREX)
- Planning and implementation of awareness raising measures driven by the results of the assessment

An additional goal has been to create an internal capability of applying the assessment methodology and how to analyse the results to define a m mitigation plan.

Results

FPG has now obtained:

- A good Questionnaire[16] to assess the cybersecurity awareness in a Hospital work and technological environment .
- A quite complete picture of the cybersecurity awareness, by job categories, age, risk category, source of problems (e.g. use of USB), based in the Questionnaire
- A method to extract types of risk reduction measures (or "controls") from the results of the survey.
- A plan of action to raise the awareness
- An indication about the communication channels on cybersecurity and privacy currently used and to be used
- 2.949 staff members (46% of the invited), at 15/04/2025, have successfully completed a 1.8 hour e-learning module.

Moreover, two FPG professionals now are able to use the assessment methodology.

The Questionnaire is structured in five sections and includes 50 items for the consideration of the respondent. The content of each section is summarized in Annex 1.

The survey has been sent to 5.668 persons (including FPG regular staff + 577 medical residents) and has reached a response rate of 29%.
The picture of the awareness extracted from the survey has an information granularity that has allowed to draft a non-generic awareness mitigation plan, with clear prioritization about

- WHO, i.e. the top four (out of 10) categories of staff to be targeted with higher priority due to their high criticality[17]
- WHAT, i.e. the top five topics on which to focus the interventions for each category of the four categories of staff, selecting those (out of nine, listed in Table 4) that for all the categories score "high need" AND "low awareness" of the negative consequences[18].

[14] SBNT (Secure Behaviour Nudging Tool)is a method to identify, design and deploy "nudges" to assure secure behaviours (e.g. Posters, Memes, Screensaver messages) specific to the behaviour at hand.

[15] CH (Human Centric Cyber Hygiene) is a survey-based risk assessment methodology for raising cybersecurity and data privacy awareness of different employee groups in healthcare organisations. See https://curex-project.eu/content/cyber-hygiene-ch

[16] The Initiative 4 has benefitted from the scientific guidance of Prof. Lynne Coventry, Abertay University (cyberQuarter), Prof. Christos Laoudias, University of Cyprus KIOS Research and Innovation Center of Excellence, Prof. Christos Xenakis, University of Piraeus Systems Security Laboratory University of Piraeus and Apostolos Koutsoulelos, MSc student University of Piraeus

[17] The risk level is the product of likelihood and impact. The likelihood is driven by the risk assessed with the Questionnaire, by the quantity of staff and by the organizational influence on other staff; the impact is estimated considering the variety of systems that the category can access and the level of access (read, read & write, read & authorize, read & write & authorize)

[18] E.g. the category has a *high need to share the password* and also a *low awareness of the negative consequences of this behaviour*

Table 4 Behaviours that may require awareness raising action

Topic	Need to be addressed
PASSWORD SHARING 1	I need to share passwords to do my work
PASSWORD SHARING 2	Sometimes I need to share my password with the ICT/Service Desk.
CYBER INCIDENTS	Sometimes I'm too busy to report a cybersecurity incident
EMAIL	It is sometimes useful to copy patient data in non-institutional emails
CORPORATE EMAIL	I need to use my corporate email for personal interests
PERSONAL EMAIL	Sometimes I need to use my personal e-mail to carry out work activities
SMARTPHONE	Sometimes I need to share sensitive hospital information via my cell phone
USB	I need to use USB flash drives at work
LINK	I need to click on links contained in emails as part of my work activity

- HOW, i.e. the mitigation measures most appropriate for the type of topic, and the communication channels most accepted by the staff (see Table 5)

Table 5 Catalogues of mitigation measures and communication channels

Mitigation measures	Communication channels
• Deliver training for all the staff • Draft Instructions • Provide alternative devices • Introduce technological constraints • Create/enforce policies • Use nudging • Insert Agenda items in periodic Unit management meetings • Use qualified peers to monitor and recommend behaviours	• Corporate intranet • Email • e-leaning packages • tutorials • service desk • Department/office colleague designated as liaison with ICT/DPO (Cyber Angel) • Nudging means ((e.g. influence by the boss, games, video clips on hospital screens, screen savers, stickers)

<u>Value for the target audience</u>

1) The questionnaire is healthcare-specific and has proven to be quite informative and action oriented
    - We recommend its use by other HCOs to support the planning of focused awareness raising actions.
    - We think that It could also be recommended by the National Cybersecurity Agencies (NCOs) to all the HCOs of their countries, public and private, as a quick manner to assess the cybersecurity awareness of the healthcare staff, both in private and in public HCOs
    - The results of each HCO could be collected on a confidentiality basis by y
2) The methodology to elaborate the responses from the questionnaire and to build the plan provides a structured way to use the results of the survey
    - We recommend its use by other HCOs to support the planning of focused awareness raising actions.
    - We think that It could also be recommended by the NCOs to all the private and public HCOs of their countries, as a standard manner to identify the key actions to be done to raise the cybersecurity awareness of the healthcare staff across the country
3) The methodology applied contributes to comply with the Art. 21 item 2 of the NIS 2: "*the measures shall include … the basic cyber hygiene practices and cybersecurity training*"

Lessons learned

1) Make sure that the questions are correctly formulated in the local and organization's language
2) Make clear which questions are not applicable for a job category in your context
3) Include in the target population of the survey not only the HCO employees, but also the staff that have access to the HCO information system (e.g. residents in case of university hospital)
4) Add to the questionnaire a final box to collect open input (e.g problems, suggestions) that can be then elaborated with, e.g. a Chat GPT type of software (if secure).

4.4 Cyber Angels

Goal and scope

The main goal of this Initiative is to establish a role (named Cyber Angel) acting as the interface between the staff of the Hospital and the roles for managing cybersecurity (the Chief Information Security Officer-CISO, ICT) and privacy (the Data Protection Officer-DPO).

The "angel" is not a full-time role; she/he runs normal duties (clinical, technical, administrative) in her/his Unit (office, clinical ward, laboratory), but is also a reference person in the cybersecurity/privacy domain in the Unit. The initiative included the definition of the role, the identification of the persons playing the role of Cyber Angels, their training to play the role.

Results

The Initiative has obtained three results:

- Job profile of the Cyber Angel
- High level design of the training of the Cyber Angels
- A first group of 37 persons have been identified for playing the role of Cyber Angel.

The *Job profile* (see Table 6) includes the Job description (mission and activities) and the job requirements (type of staff, skills and values, knowledge).

Table 6 Job profile of the Cyber Angel

Job description

Mission

- The Cyber Angel is the point of contact between the company functions responsible for cybersecurity and data protection and her/his colleagues in the organizational unit (example: department, clinical ward, administrative office).

Activities

- Collects and reports any risks or operational management difficulties relating to compliance with these company policies
- Contributes to the drafting of policies and procedures regarding cyber security and personal data protection
- Promotes among the peers of her/his Unit correct behaviors, in line with security and privacy policies, including

  Login credentials

  ✓ Instructs on the ways of obtaining/managing/storing access credentials, identifying incorrect methods indicating the alternatives envisaged and possibly reporting to ICT the emergence of new situations not yet managed by company policies.

  ✓ Reports problems relating to access credentials to ICT to optimize department's work processes (e.g.: Manages any group passwords associated with department clients (kiosk users)

  Management of corporate, personal and acquired hardware and software

  ✓ Provides documentation on the management of company devices to staff who have not received it

  ✓ Warns about the risks associated with the use of pen drives

- ✓ Interfaces with ICT/ING clinic regarding the implementation of IT/electromedical solutions and urges interested parties to inform the Service Desk
- ✓ Warns about the risks associated with the use of personal devices (e.g. checks whether personal laptops are equipped with antivirus and alerts ICT if they are not)
- ✓ Warns about the risks associated with leaving personal and company devices unattended

Corporate and personal e-mail

- ✓ Warns about the risks and prohibitions linked to the improper use of company emails (e.g.: registration of company domains for personal services)
- ✓ Warns about the risks and prohibitions associated with the use of personal emails (e.g.: opening attachments in the company and using company data through personal emails)

Processing of personal data

- ✓ Promptly report personal data violations according to the appropriate procedure and work to mitigate their effects, together with the competent company functions
- ✓ Warns of the risks and prohibitions related to saving personal data of FPG's staff/patients on personal or university clients/devices/clouds
- ✓ Promptly takes care of requests concerning rights by subjects, with the support of the DPO and the competent functions

Job requirements

Type of staff

- FPG employee, working in the Unit where she/he acts as Cyber Angel
- Is indicated and approved by the head of the Unit

Skills and Values

The person covering the role must

- Be sensitive to cyber security issues, have an interest in technology and be available for periodic updates.
- Be reliable
- Have good communication and problem solving skills
- Adhere to the Foundation's values

Knowledge

The person covering the role must have

- Knowledge of IT applications used in one's work environment
- Knowledge of regulations, internal procedures and company organization chart, with reference to the topic of cybersecurity and data protection.

AA

The *training,* based on a high level design activity, will include a basic e-learning module(currently, it is Cyber Gym) and a one-day in presence training, with the structure and content described in Table 7.

Table 7 Structure of the in-presence training of the Cyber Angels

Delivery model

- Duration of one day
- Delivered in presence
- Delivered by internal staff, from the ICT, DPO and Clinical Engineering functions
- Classes of 20 participants, in the phase of the establishment of the role at FPG

Content

- Basic concepts
  1) Basic concepts of cybersecurity (threats, vulnerability, types of attack) and data protection
  2) Notions on cybersecurity related to the medical devices
  3) Cybersecurity and data protection processes, regulatory framework
  4) Role of the staff as a risk factor and as a risk mitigation factor, with examples of situations specific to the Hospital work context

- FPG technology, organization and measures for cybersecurity and data protection including
  1) Types of applications and data, Types of medical devices, networks and devices
  2) Key roles (CISO, DPO, Help Desk, …)
  3) Policies, procedures, types of technical measures
- Cybersecurity Angels role
  1) Mission and activities
  2) Indications on how to perform the activities, with examples of situations specific to the Hospital work context

Value for the target audience

In the Hospital work context is difficult to get and keep staff awareness about the cybersecurity risks, for many reasons, including[19]

- Work culture can lead to security being overlooked or being perceived as a burden, particularly if it is seen to detract from patient care.
- The working environment is also prone to regular changes to team structures through staff rotation and new employees being hired.
- In many cases, staff involvement with information systems and medical devices follows a many-to-one scheme: many staff members in clinical wards and laboratories access the same workstation (or interface) many times during the working day. This increases the risk of poor attention to password management and unlocked workstations. Healthcare operators may have to log in and off more than 80 times a day in clinical wards.
- The hospitals (particularly the big ones) have a highly articulated organization structure with long hierarchical chains. Each Unit, in particular the clinical ones, are “silos”. So, both the vertical and the horizontal (formal and informal) communication is difficult

The Cyber Angel is a means to reach every staff member, establishing a manageable number of local interfaces between each individual staff member and the central functions responsible for the cybersecurity.

Lessons learned

1) The initiative to set up the Cyber Angel network should be managed jointly between ICT, DPO and HR. This should ensure that both cybersecurity and data protection aspects are taken into consideration and that the initiative is correctly communicated to the management and to the staff
2) Make sure that the persons selected as Cyber Angels are popular among the colleagues and are interested to the role

4.5 Cybersecurity by procurement

Goal and scope

The main goal of this Initiative has been to reengineer the FPG and FPHAG procurement and deployment process to ensure that new connected Medical Devices and new Information Systems (clinical, administrative) fulfil cybersecurity requirements and do not introduce new vulnerabilities. The reengineering has been performed to comply with *ENISA, Procurement guidelines for cybersecurity in hospitals, February 2020*, which recommend 30 Good Practices (GPs).

[19]PANACEA project, *Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres*, 2021 https://www.panacearesearch.eu/sites/default/files/WhitePaperA4_December2021_final_0.pdf

Results

The Initiative[20] has produced

- Six types of documental artifacts providing requirements and guidelines for the procurement, deployment and assistance stages of software applications and medical devices. They are briefly described in Table 8

Table 8 Artifacts to implement the "cybersecurity by procurement"

Artifact	Content
Process description	Integrations to the procurement process (roles, committees, workflow)
RFP/RFO	Cybersecurity/Privacy requirements for Request for Proposal/Offer, including lists of technical requirements
Contract	Cybersecurity/Privacy clauses/annexes for Contract
Tools	Requirements for tools to pre-assess cybersecurity and privacy robustness and regulatory compliance
Guidelines for deployment	Guidelines for deployment, including indications to ensure that internal users adopt «Cyber-safe» behaviour with new devices/systems and to ensure securely insertion of the new products in the existing physical and technological environment
Guidelines for assistance	Guidelines for assistance, including indications to ensure «Cyber-safe» behaviour of third parties with regard to cybersecurity and privacy

- A detailed identification of the norms (standards regulatory documents) to be considered when aligning the procurement processes with the 30 ENISA good practices. For each norm, the relevant articles have been identifies (see Annex 2). Each of the identified norm's article has then been analysed to derive the cybersecurity requirements and to state which of the artifacts should/could host them in the procurement/deployment/assistance process.

  In Table 4 there is an example of this type of analysis, extracted from a long table including all the ENISA Good Practices (GPs) and the identified Norms.

Table 9 Example of analysis to translate ENISA Good Practices into artifacts

GP	Norm	Appicabilty to ...		Text from the Norm	Requirements based on the Norm	Artifacts					
		Clinical information systems	Medical Device			Process	RfP	Contract clauses	Tools	Guidelines for Deploy	Guidelines for Assista
GP 6. Establish Business Continuity plans	ISO 22857 11.9	x	x	Business continuity plan It is necessary for the organization to be able to continue with its business such as the diagnosis and treatment of its patients even when disaster overtakes its processing facilities. There needs to be a clear assessment of the disasters that need to be accommodated and proper plans need to be drawn up, tested and documented for use if such disasters arise. It is too late to invent the plan when the problems have arisen. The consequences of various forms of system failure should be part of risk analysis. The development of a business continuity plan, including a disaster recovery plan, is a significant project that depends on the processing that is undertaken. It should be tested and updated regularly.	Is the organization able to continue its activities, such as diagnosing and treating patients, even when a disaster strikes its processing facilities? Is there a clear assessment of the disasters that need to be addressed and adequate plans in the event of a disaster? Is there a business continuity plan, including a disaster recovery plan? If so, is it tested and updated regularly?	x		x			x

The artifacts that have been delivered include

- For the Procurement stage

[20] The Initiative has benefited from the services of RINA Consulting, with both its Italian and Spanish branches

- Documents containing contractual clauses, lists of requirements, tools and guidelines that can be used when procuring software, medical devices and when procuring and managing the related assistance services. The clauses and the requirements regard both the products and the suppliers (software providers, medical device manufacturers and distributors).
- Categorization into 8 categories (see Table 10) and 20 examples of tools supporting the procurement process

Table 10 Categories of tools

Category description
Generic tools that allow to verify the good practices to be followed in the procurement process and to search for known vulnerabilities on specific devices.
Tools that assist users in evaluating the medical device and the system development process throughout all lifecycle phases.
Comprehensive evaluation of a network's security posture to identify vulnerabilities, weaknesses and potential threats. The goal of this assessment is to ensure that the network is secure from unauthorized access, data breaches and other security threats.
Simulated cyberattack against a computer system, network, or application to identify and exploit security vulnerabilities. The primary objective is to discover weaknesses before malicious hackers do, allowing organizations to remediate these issues and strengthen their security posture.
Examination and evaluation of the low-level software that operates hardware devices, such as routers, IoT devices, and embedded systems. The goal is to identify vulnerabilities, understand functionality, and ensure the firmware is secure and behaves as expected.
Static Application Security Testing (SAST) is a white-box testing method that analyzes the source code, bytecode, or binary code of an application to identify security vulnerabilities without executing the code. Dynamic Application Security Testing (DAST) is a black-box testing method that examines an application in its running state. It simulates external attacks on an application to identify security vulnerabilities during execution.
Tools using hypothetical scenarios, system diagrams, and testing to help secure systems and data. By identifying vulnerabilities, helping with risk assessment, and suggesting corrective action, threat modeling helps improve cybersecurity and trust in key business systems.
Software applications or platforms designed to assist security teams in identifying cybersecurity incidents.

- The results of three pilots, that have been performed to validate the security requirements for software and medical devices. The pilots regard a software application for the secure sharing of clinical information between FPG and FPHAG and two medical devices: a Mass Spectrometer and a Pathological Anatomy Scanner

- For the Deployment stage
  - Integration of the deployment phase of software lifecycle with security requirements, with regard to Environment Preparation (Environment Isolation, Secure Configuration, Access Control), Software Distribution (Integrity Verification, Data Encryption, Automation), Post-Deployment Review (Security Assessment, Feedback and Improvement)
  - A contractual clause regarding the training on a new medical device
- For the Assistance stage
  - Integrations to the existing contractual clauses about the policies for Audit of the supplier’s organizational practices , Vulnerability Management, Patch Management, Log Management and Incident Management, Maintenance Management
  - Addition of cybersecurity aspects related to suppliers' access to software applications, within the “Domain User Management” FPG Operating Instruction.

Value for the target audience

1) ENISA, based on the consideration that "Cybersecurity should be considered in the early days of purchasing assets (infrastructure, software, systems, devices etc.) for healthcare organizations" published procurement guidelines and good practices for the security of Healthcare services [21]. The main value of the output of the initiative is that it strongly contributes to practically align the European HCOs with the ENISA good practices, for 3 of the 10 types of procurement identified by ENISA: Clinical information systems, Medical devices and Professional services[22].

2) Moreover, the initiative contributes to the compliance with the Articles 21[23] and 25[24] of the NIS 2, "*Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security of network and information systems*."

3) Some of the output are immediately re-usable, such as the list of applicable standards and regulations and of tools to assess vulnerability and compliance of the products.

   They can be used not only by the HCOs, but also by the suppliers, to be better prepared to compete in the tendering processes.

4) ENISA and the NCAs could invite all the HCOs, public and private, or the healthcare procurement agencies, to use the results of this initiative; this would allow them to get the benefits that FPG and FPHAG are going to obtain.

Lessons learned

We recommend other HCOs willing to implement a similar initiative to

1) Start the project from a gap analysis vs the 30 ENISA good practices, exploding each practice into the more detailed items

2) Assign to the project a multi-functional team, including ICT, Clinical Engineering (both those that procure and those that manage the medical devices), DPO, Legal Affairs, Procurement

3) Collect all the organizational procedures, operational instructions, testing procedures, contractual clauses, examples of contracts and request for offer, check lists already existing in the house in order to capitalize the expertise from the different parts of the organization

4) Consider also that some parts of the HCOs (e.g. the Research Department) may have different procedures, even if they connect their software and devices to the operational network (e.g. to run clinical studies): decide if and how to involve them in the project

4.6 Endpoints reinforcement

Goal and scope

The main goal of the Initiative has been to reinforce the entry points related to the workstations, updating the Operating Systems of the FPG's workstations and implementing other reinforcement actions.

[21] ENISA, *Procurement Guidelines for Cybersecurity in Hospitals_Good practices for the security of Healthcare services*, February 2020a
[22] The other types of procurement include: Network equipment, Remote care systems, Mobile client devices, Identification systems, Building Management Systems, Industrial control systems, Cloud services**.**
[23] NIS 2 Art. 21 item 2.: the measures shall include "*supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers*" and "*security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure".*
[24] NIS 2 art. 25: "*Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security of network and information systems*."

Results

The solution also guarantees the same level of security both to the workstations certified within the security perimeter of the HCO, or connected to the internal network or via VPN, and to those located outside the perimeter, such as it occurs for example in the case of users in smart working.

The Operating Systems of all the FPG's workstations have been updated to the latest version of Windows to reduce the risk of compromising the infrastructure due to vulnerabilities in outdated operating systems.

Value for the target audience

These types of interventions bring value because they

1) Set technical barriers to risky behaviours
2) Make possible to analyze more easily relevant information about events or errors that occurred over a certain period
3) Are an opportunity to clean and change the workstation technology also at hardware level, e.g. from hard disk drives (HDD) to solid state drives (SSD), and to install new generation software applications
4) Allow to more easily integrate the workstations with the most advanced system agents, both for functional and security purposes

Lessons learned

1) When planning these intervention involving all the workstations, consider that he rate of deployment may be lower than expected, because
    - the updating in itself removes the workstation from the operation, but it is not possible to remove too many workstation from the operations, otherwise the service delivery would be severely penalized
    - it may be difficult to find adequate additional manpower to feed the deployment capability.
2) It is recommended to proceed by batches of different types of users, performing pilots for each type, to avoid the risk of limiting some necessary access to the web by that some types of workers[25]

5. The value and lessons learned from the project as a whole

5.1 For up-taking the EU innovative projects results

The project has shown that it is possible to up-take innovative project results. CYBERHIMPREX has adopted methods and ideas developed in the PANACEA and CUREX projects[26].
This has been facilitated by the fact that

- The call explicitly pushed to include some “solutions developed in the framework of EU-supported research and innovation projects”.
- PANACEA and CUREX were two “peer” Projects that had responded to the same previous H2020 call. They had collaborated preparing and delivering some joint webinars and knew the complementarity of their portfolios of solutions. This allowed them to quickly prepare the proposal, and win.
- The partners of CYBERHIMPREX had been partners, as end-users, in the two projects and have involved as suppliers the partners that had developed those methods
- The Project Officer of the two projects was the same and promptly invited the two projects to consider taking the opportunity offered by the call.

However, during the project some obstacles emerged

[25] For instance, it was found that the Department dealing with poisons needs to access the dark web.
[26] This regards the methods used in the Staff Awareness initiative and the ideas used in the Cyber Angel initiative

- In some cases the individuals that had developed the solution had moved from the organization that had the formal IPR (being the partner of the H2020 project) to another one; this has raised the need to go through an agreement between the two organizations, inducing delays in the procurement process
- In case of solutions involving equipment, only the depreciation is eligible; this introduces a dependance of the final contribution on the actual equipment installation time; in case of delays vs the original plan, this reduces the expected financial benefit, if the end date of the project is not shifted ahead.

Based on above lessons, it is recommended to the European Commission

- Make sure that the Project Officers play an active role in promoting the "peer" project collaboration
- Make eligible the full cost of the equipment, and not only the depreciation cost, at least for the uptake of the EU innovation actions (RIA, IA). Or, Consider to extend, only from an administrative point of view, the life of the project to cover the entire depreciation period (which normally is five years).
- Define an "early-adoption" type of funding mechanism, e.g. establish ad hoc procurement procedures and higher co-funding rate to facilitate the adoption of innovative solutions produced by EU innovation actions (RIA, IA)
- Explore, when the IA or RIA project ends, the possibility to explicitly link, at least in case of methodologies, the ownership to the researchers.

5.2 For implementing a systemic approach and pursuing the regulatory compliance

The rationale of the CYBERHIMPREX initiatives is that they make up a systemic portfolio. It has been possible because the project has been structured and led by a team that had coordinated the PANACEA project, that had applied a systemic socio-technical paradigm, developing a set of nine integrated tools revolving around people, processes and technologies based on multi-disciplinary skills and know-how[27].

This approach has been accepted by the FPG ICT Department also because a third party Cybersecurity Audit (at the end of 2023) had generated a "to do" list that was systemic in nature, including technological, organizational and people-related measures.

This is not a diffused approach in the HCOs, where the cybersecurity investments are governed mainly by the ICT department and have a technological nature. And it seems that a systemic offer and demand does not currently appear explicitly in the spending categories for IT security (e.g. those identified by ENISA and Gartner[28], see Table 11).

Table 11 Spending categories for IT security

Gartner categories	ENISA categories
Identity and access management	Multi Factors Authentication (MFA)
Network security	Wireless Access Firewalls (WAF)
	Distributed Denial of Service (DDoS) Protection & Prevention
	Network intrusion Detection & Prevention (NIDS, NIPs, etc.)
Data security	Data Loss Prevention Services (DLP)
	Data Discovery & Classification
Governance, risk and compliance management	Risk Assessment & Business Impact Analysis Services
	Security awareness and training
	Business Continuity Management & Program Solutions
Vulnerability management	Vulnerability Assessment Tooling
Application security	
Security analytics	Threat Intelligence
	Security Incident & Event Management (SIEM)
End point security	Device Encryption & Management
	Physical Security Technologies

[27] PANCEA Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres, https://panacearesearch.eu/sites/default/files/WhitePaperA4_December2021_final_0.pdf
[28] ENISA, *NIS Investments,* November 2021; ENISA list is at page 30, Gartner list is in Annex B.6,

However, many European projects develop solutions that are systemic in nature[29]. Even if they develop solutions that can be marketed individually, they would bring a much higher value if they were up taken as a system. But this is difficult, because each partner has its own priority and it is quite impossible to set-up a sustainable joint exploitation model.

Based on above lesson, it is recommended:

- To the European Commission to define a mechanism to fund (or facilitate) the creation of formal post-project continuation of the Consortium, so that it can operate as a formal entity, that can take contracts and invoice and, with some post-project funding, sustain the expenses for reaching TRL 9 and undertake the commercial efforts to engage the early adopters.
- To the NCAs to promote the systemic investments for cybersecurity.
- To the HCOs to plan the cybersecurity investments in a systemic perspective, also taking into account the results of their cybersecurity Audits

5.3 For pursuing the regulatory and standardization compliance

A trigger for investments is the need of the HCOs to comply with the regulations (in particular NIS 2, CRA, MDR) and the accreditation schemes, e.g. those of the Joint Commission International (JCI).

For CYBERHIMPREX this has helped in ensuring the continuous support from the management.

Based on above lesson, it is recommended to the HCO:

- To monitor the progress of the regulatory and standardization landscape during the life of the project, to promptly identify new needs
- To identify, through a gap analysis, the regulatory, standardization and accreditation targets, to better shape the investment project
- To ensure and track the fulfilment of the targets during the project

5.4 For an effective project implementation

The CYBERHIMPREX project has been structured in three Work Packages: Coordination, Procurement, Implementation. Coordination also included communication and dissemination. Both Procurement and Implementation have been internally structured by initiative.

From the project management point the key issue has been the time, mainly for the procurement activities, due to the

- Heaviness and complexity of the internal procedures
- Underestimation of the complexity of preparing some technical terms of reference
- Time of response of some suppliers
- Tendence of acting with a "business as usual" instead of a "project-oriented" mindset.

This delay has driven delays in implementation and in the possibility to deliver a content-rich dissemination.

Based on the analysis of what has happened, it is recommended to the HCO to

- Ensure the deep involvement of all the relevant internal functions (ICT, Clinical Engineering, DPO, Procurement, Legal Affairs, Internal Audit), both in the project design phase and in the implementation phase
- Agree with the Procurement Department a “fast track” procedure, appoint the reference persons for the steps of the procedure, do periodic meetings

[29] PANACEA, CUREX, DYNAMO are examples

- Anticipate as much as possible the involvement of the potential suppliers, to mitigate their low administrative responsiveness, due their approval procedures (in particular of the Universities) and the complexities of the initial registration procedure of new suppliers (in particular when they are foreigners).

Annex 1-Structure of the questionnaire for staff awareness assessment

Section	N. of items	Sub-sections	Examples of items (sentences/options) and agreement scale
1. Respondent's profile	**3**	• Category of staff • Age • Seniority - Attendance at FPG (years)	10 categories, of staff e.g. Administrative staff, Nursing staff, Medical Residents
11 Attitudes toward cybersecurity and privacy	**6**	• Patient care and hospital infrastructure (i.e., behaviour may affect patients or the hospital) • Privacy (i.e., only access the information you need for work, do not take it at home) • Social norms (i.e., doing the wrong thing because the rest of the team is doing so) • Doing work at work	Agree (*1=Totally disagree; 5=Completely agree)* • Proper cybersecurity behaviours protect patients from harm • The team I am part of works safely
12 Awareness of consequences	**7**	• Personal (personal financial loss, personal reputation) • Institutional (fines, ransomware-financial loss, reputation, etc.) • Patient (harm, lose life)	*Agree (1 to 5)* • Cyber security misconduct can lead to personal financial losses • Inadequate cybersecurity behaviors can cause harm to patients or result in their death
13 Risky behaviours	**31**	• List of risky behaviours relevant for the FPG: 1) *General* 2) *[USB]]* 3) *[EMAIL]* 4) *[CLOUD]* 5) *[COMMUNICATION VIA CHAT]* 6) *[PASSWORD]* 7) *[LINK]* 8) *[SOCIAL ENGINEERING]* 9) *[ATTACHMENTS]* 10) *[PASSWORD SHARING]* 11) *[BUSINESS EMAIL]* 12) *[PERSONAL EMAIL]* 13) *[CYBER INCIDENTS]* 14) *[PERSONAL DEVICES]*	*Agree (1 to 5)* *[USB]* • *I need to use USB flash drives at work* • *Any USB flash drive can infect a computer with computer viruses* *[CYBER INCIDENTS]* • *Sometimes I'm too busy to report a cybersecurity incident* • *Information security incidents or eventual risks should be reported immediately*
14 Interventions	**3**	• Where do employees stand on the ethical intervention ladder in terms of courses of actions • Which channels do employees prefer to receive the awareness messages? • Channels already in place • Additional channels	*YES/NO multiple choice* For each of the following courses of action, indicate whether you find them acceptable to you (Yes/No) • Make safe choices mandatory • Receive a warning if you perform an unsecure IT action • Receive more information about cybersecurity policies Channels (Yes/no) • Corporate intranet • Online training courses • … • Tutorials • Games • From a department/office colleague designated as the cybersecurity and privacy liaison

Annex 2-ENISA procurement good practices and standards/regulations

GP 1. Involve the IT department in the different stages of procurement to ensure that expertise in cybersecurity aspects is considered	ISO 27001, 5.3, 7.2 , GDPR art. 32, ISO 80001-1 5.4.7, 6.2.2 c), ISO 22857 10.11
GP 2. Implement a vulnerability identification	ISO 27001 controllo 8.8, NIST CF ID.RA-01, ISO 14971 5.4, HL7 6.1.0, ISO 80001-1 6.1.2.3 e 6.2.2, EUCC 2.9 e 2.11
GP 3. Develop a policy for hardware and software updates	ISO 27001 5.9, IEC 62304 -5.8.4,7, 8, MDR art.10.9, ISO 80001-1 6.2.6, EUCC 2.8.5, IVDR art. 3.1, ISO 27017 8.1.1 & 8.1.2
GP 4. Enhance security controls for wireless communication	ISO 27001 controlli 8.20, 8.21 e 8.22, GDPR art. 32, ISO 27017 13.1.1
GP 5. Establish testing policies	ISO 27001 controllo 8.29, ISO 27799 14.2.8, ISO 13485 7.3.6, MDR Annex I chapter II (17.2), NIST CF ID.IM-02, GDPR art.32, IEC 62304 5.7, EUCC 2.7
GP 6. Establish Business Continuity plans	ISO 27001 5.29, 5.30 ISO 27799 17, NIST CSF RC.RP, GDPR art.32, ISO 22857 11.9
GP 7. Take into account interoperability issues	ISO 27001 controllo 5.20, ISO 27799 15.1.2, HL7 FHIR, MDR Annex I chapter II 14.5 and 23.4 (q), GDPR art.20, IEC 62304 5.1.5, ISO 80001-1 6.2.4, ISO 27017 15.1.2
GP 8. Enable testing of all components	ISO 27001 controllo 8.29, ISO 13485 7..3.6, IEC 62304 5.5 e 5.6
GP 9. Allow auditing and logging	ISO 27001 controllo 8.15, ISO 27799 12.4 , DICOM PS3.15 Annex A.5, HL7 6.1.0.6, NIST PR.PS-04, GDPR art.30, ISO 27017 12.4.1 &12.4.3, ISO 22857 11.4
GP 10. Encrypt sensitive personal data at rest and in transit	DICOM PS3.15 Annex B e Annex D, NIST PR.DS-01, PR.DS-02, PR.DS-10, ISO 27001 controllo 8.24, ISO 27799 10, GDPR art. 32, ISO 27017 10.1.1 & 10.1.2, ISO 22857 10.10.3 e 11.2
GP11. Conduct a risk assessment as part of the procurement process	ISO 14971, ISO 27001 controllo 5.19 e clausola 6.1, ISO 27799 15, IEC 62304 4.2, MDR art. 10 (2) , GDPR art. 32, art 24 , NIST CSF GV.SC-03, ID.RA, ISO 80001-1 6.1 e 6.2.2, ISO 27017 15.1.1, ISO 22857 10.10.2, 10.10.13, 11.10
GP 12. Plan network, hardware and license requirements in advance	ISO 27001 controllo 8.6, ISO 27799 12.1.3 , ISO 13485 6.3, IEC 62304 5.2, GDPR art.25, ISO 80001-1 5.4, ISO 27017 12.1.3
GP 13. Identify threats related to procurement products or services	ISO 27001 controllo 5.19, 5.20 , ISO 27799 15, ISO 14971 4.2, 5.4, GDPR art. 25, NIST GV.SC, ISO 80001-1 6.1.2.3 e 6.2.2, ISO 27017 15.1.1 &15.1.2
GP 14. Segregate your network	ISO 27001 controllo 8.22, ISO 27799 13.1.3, GDPR art.25 e 32
GP 15. Determine network requirements	ISO 27001 controlli 8.20,21,22,23 , ISO 27799 13.1, NIST PR.IR-01, DICOM PS3.15 6.2 E Annex B, HL7 FHIR 6.1.0.3, GDPR art.25 e 32
GP 16. Establish eligibility criteria for suppliers	ISO 13485 7.4.1, ISO 27001 controllo 5.19, MDR AnnexIX chapter I -2.2, ISO 27799 15.1.1, DICOM PS3.15 6.2, 6.3, 6.4 e Annex B, C, D, NIST GV.SC, GDPR art. 24 e 25, ISO 27017 15.1.1
GP 17. Create a dedicated RfP for procuring Cloud Services	Iso 27001 controllo 5.21 e 5.23 , MDR Annex IX chapter I -2.2, ISO 27799 15.1, DICOM PS3.15 6.2, 6.3, 6.4 e Annex B, C, D, NIST CSF GV.SC, GDPR art. 32 e 44, ISO 27017 15.1.3
GP 18. Require cybersecurity certification	MDR article 10 (1) , Annex IV, ISO 27001, ISO 13485 7.4, IEC 62304 4.1, ISO 27799 15.1, NIST CSF GV.SC, GDPR art. 24 e 25
GP 19. Conduct data protection impact assessments for new products or services	GDPR art. 35
GP 20. Set gateways to keep legacy systems/machines connected	ISO 27001 controllo 8.20 & 8.22, ISO 27799 13.1, NIST CSF PR.IR, ISO 27017 13.1.1
GP 21. Provide cybersecurity training on the organization's security practices to staff and external consultants	ISO 27001 controllo 6.3 , ISO 13485 6.2, ISO 27799 7.2.2, NIST CSF PR.AT, GDPR art. 39, ISO 80001-1 6.2.5, ISO 27017 7.2.2, ISO 22857 10.11.3
GP 22. Develop incident response plans	ISO 27001 controllo 5.24, 6.8, IEC 62304 9, MDR art.87, ISO 27799 16.1.1, NIST CSF ID.IM-04, RS e RC, GDPR art. 33 e 34, ISO 80001-1 6.2.6, ISO 27017 16.1.1, 16.1.2, ISO 22857 11.8
GP 23. Involve vendor/manufacturer in incident management	ISO 27001 5.19, 6.8, MDR art.83, ISO 27799 15 e 16, NIST CSF GV.SC, RS e RC, GDPR art. 33 e 34, ISO 80001-1 6.2.6, ISO 27017 15.1.1, 16.1.2, ISO 22857 11.8
GP 24. Schedule and monitor maintenance operations for all equipment	ISO 27001 controllo 7.13, ISO 13485 7.6 & 8.2, IEC 62304 6.1, MDR article 10 (i), article 83, ISO 27799 11.2.4 e 15, GDPR art. 32, ISO 80001-1 6.2.6
GP 25. Remote access should be minimised and administered	ISO 27001 controllo 5.15, 8.3 , ISO 13485 7.5.6, MDR annex I chapter II (17.4), HL7 FHIR 6.1.0.3 & 6.1.0.4, ISO 27999 6.2.2, 9.1, 9.2 e 15, NIST PR.AA-03, PR.AA-05 e PR.IR-01, GDPR art. 32, ISO 27017 9.1.2, ISO 27017 9.4.1, ISO 22857 10.10.5 e 11.3
GP 26. Require patching for all components	Iso 27001 controllo 8.8, IEC 62304 6.1 & 9, ISO 27799 12.5 e 12.6, 15 e 17, NIST PR.PS-02, GDPR art. 32, ISO 80001-1 6.2.6, ISO 12.6.1
GP 27. Raise cybersecurity awareness among staff	ISO 27001 controllo 6.3, ISO 14971 4.3, ISO 13485 6.2, ISO 27799 7.2.2, ISO 27017 7.2.2, NIST CSF PR.AT, GDPR art. 39, ISO 80001-1 5.5, ISO 22857 10.11.3
GP 28. Perform asset inventory and configuration management	ISO 27001 controllo 5.9, 5.10, Iso 13485 7.6, IEC 62304 5.1.9 & 8, MDR chapter III Annex II technical documentation, ISO 27799 8.1, NIST CSF ID.AM, GDPR art. 32, ISO 80001-1 5.4.3 e 6.2.3, ISO 27017 8.1.1 & 8.1.2
GP 29. Establish dedicated access control mechanisms for medical device facilities	ISO 27001 controlli 8.2, 8.5,5.15, HL7 FHIR 6.1.0.5, ISO 13485 7.5.6, MDR annex I chapter II (17.4), ISO 27799 9 e 11.1.2, NIST CSF PR.AA, GDPR art. 32, ISO 27017 9.2.3, ISO 22857 10.10.5 e 11.3
GP 30. Schedule penetration testing frequently or after a change in the architecture/ system	ISO 27001 controlli 8.16, 8.25, 8., ISO 13485 7.3.9, ISO 27799 12.5, 12.6 e 15, NIST CSF ID.IM, GDPR art. 32, ISO 27017 14.2.1