SECUREHOSPITALS.EU

RAISING AWARENESS ON CYBERSECURITY IN HOSPITALS ACROSS EUROPE AND BOOSTING TRAINING INITIATIVES DRIVEN BY AN ONLINE INFORMATION HUB

D2.1. Stakeholder involvement roadmap and engagement strategy

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 826497.

PROJECT DESCRIPTION

Acronym: **SecureHospitals.eu**

Title: **Raising Awareness on Cybersecurity in Hospitals across Europe and Boosting Training Initiatives Driven by an Online Information Hub**

Coordinator: INTERSPREAD GmbH
Reference: 826497
Type: CSA
Program: HORIZON 2020
Theme: eHealth, Cybersecurity
Start: 01. December, 2018
Duration: 26 months
Website: https://project.securehospitals.eu/
E-Mail: office@securehospitals.eu

Consortium: **INTERSPREAD GmbH**, Austria (INSP), Coordinator
Erasmus Universitet Rotterdam, Netherlands (EUR)
TIMELEX, Belgium (TLX)
Fundació Privada Hospital Asil de Granollers, Spain (FPHAG)
Cooperativa Sociale COOSS Marche Onlus, Italy (COOSS)
Arbeiter-Samariter-Bund, Austria (SAM)
Johanniter International, Belgium (JOIN)
European Ageing Network, Luxembourg (EAN)

DELIVERABLE DESCRIPTION

Number:	**2.1**
Title:	**Stakeholder involvement roadmap and engagement strategy**
Lead beneficiary:	**COOSS Marche Onlus**
Work package:	WP2
Dissemination level:	Public (PU)
Type	Report (R)
Due date:	28.02.2019
Submission date:	28.02.2019
Authors:	**Marco Antomarini,** COOSS **Francesca Cesaroni,** COOSS
Contributors:	**Tessa Oomen,** EUR **Jason Pridmore,** EUR **Stela Shiroka**, INSP **Yung Shin Van Der Sype,** TLX **Georg Aumayr,** JOIN **Marc Jofre,** FHAG **Karel Vostry,** EAN **Sigrid Panovsky,** SAM
Reviewers:	**Stela Shiroka**, INSP

Acknowledgement: This project has received funding from the European Union's Horizon 2020 Research and Innovation Action under Grant Agreement No 826497.

TABLE OF CONTENT

EXECUTIVE SUMMARY

Cyber-security is a new challenge for all the modern economies carrying out the digitalization of their services: while there are significant benefits deriving from the expanded use of technology, the greater connectivity also exposes to cyber risks. The healthcare sector is particularly exposed to these risks, because clinical data and healthcare records contain sensitive information extremely attractive for cyber criminals.

SecureHospitals.eu aims to raise awareness on the threats and opportunities and boost the level and quality of training of IT staff in hospitals and care settings.

The present document proposes a roadmap to secure a strong involvement of key stakeholders and to organize different activities for outreach and engagement.

It starts from the identification of the key stakeholders and of the reasons why they should be involved, to arrive to propose the most suitable procedures to facilitate and maintain their engagement.

The document will support the creation of a Community of Practice, which will attract professionals and organizations either willing to share their knowledge and competences, or interested in learning more about the cyber security and risks. The Community of Practice will be supported in its activities by an Online Awareness and Information Hub, which constitutes an important milestone of the SecureHospitals.eu project.

TABLE OF FIGURES

TABLE OF TABLES

1. Introduction

1.1 General Scenario

Cyber-security is a challenge for all the modern economies carrying out the digitalization of their services, frequently victims of deliberate attacks or unexpected events. While there are significant benefits deriving from the expanded use of technology, the greater connectivity also exposes to cyber risks, as deliberate attacks, wrong human behaviours, or unintentional events.

The healthcare sector is particularly exposed to these risks, because clinical data and healthcare records contain sensitive information extremely attractive for cyber criminals. In the health sector, a cyber incident may cause unauthorized access to sensitive information, operational disruption, data corruption, inaccessibility or loss, which can put patients' lives in danger (Chiaraluce et al., 2019).

The cyber risk management in healthcare concerns not only the technological side but also the human factor. Although it is commonly believed that the main cyber vulnerabilities derive from the technological aspects, it is widely demonstrated that the first element of vulnerability for health structures is instead the human factor, i.e. the lack of preparation and awareness of the personnel involved in the manipulation of patients' data. In second place, are the organizational aspects, namely the availability and adoption within the health structures of protocols and procedures adequate to contain cyber risk. Finally, there are the technological aspects, namely the allocation and implementation of hardware and software tools suitable to contain the cyber risk (ENISA, 2018b).

The damages resulting from a possible cyber attack may be incalculable, and therefore the implementation of a framework for cyber-security appears as a priority, to help an organization improve its knowledge of the cyber risk, translating it into a number of actions that enable the organization to minimize security costs and ensuring an appropriate risk reduction.

Suitable tools are needed to help hospitals and medical device manufacturers to assess and manage the cyber risk; training of managers, doctors, nurses and administrative employees are essential to improve the awareness of the problem, the perception of the risk and, globally, to increase the efficiency in healthcare services.

The GDPR imposed a change of perspective in this sense, moving from a data protection-based approach to a more structured process based on data governance.

1.2 Deliverable objectives

To respond to these challenges, SecureHospitals.eu aims to create a community of practice, supported by online approaches to raise awareness on the threats and opportunities and boost the level and quality of training of IT staff in hospitals and care settings.

Specifically, WP2 aims to initiate a strong involvement and integration of key stakeholders and to organize different activities for outreach and engagement.

The present document proposes a roadmap towards the implementation of an awareness-raising campaign, which starts from the identification of the key stakeholders and of the reasons why they should be involved, to arrive to propose the most suitable procedures to facilitate and maintain their engagement. It is the first step towards the creation of a Community of Practice, to be activated within and by the OAIH - Online Awareness and Information Hub (Milestone N.4).

1.3 Link to other WPs

The document is closely interlinked to:

WP3 – Aggregate, as the identified stakeholders will constitute the Community of Practice and will contribute to it both as knowledge providers and beneficiaries;
WP4 – Create, as the training needs and the results emerged from the engagement activity will inspire the definition of the training modules;
WP5 – Boost, as some of the stakeholders identified will benefit from the SecureHospitals.eu training interventions.
WP6 – Communicate, as the identified stakeholders will also steer the dissemination activities to be performed.

2. Contextualising engagement and involvement

As a first step, it is helpful to clarify the context within which SecureHospitals.eu intends to propose its engagement and involvement activities. Some basic scientific research introduces key issues investigated in WP2, namely the **main threats** to the health sector, the **human factor** that contributes to the exposure to these risks, the most significant **training needs**, and the relevance of **stakeholder engagement**.

With the digitisation process and the increasing interconnectivity of healthcare devices, the healthcare sector has become a more attractive target for a multitude of cyber threats (Coventry & Branley, 2018). In recent times, the trend of intentional cyber-attacks specifically has changed: from nuisances, such as website defacement or theft of patient data, to more malicious or pervasive attacks (Ayala, 2016, p.38). This includes causing some locations of the National Health Service in the UK to halt their services and cancel operations for a period of four days (Coventry & Branley, 2018, p. 50).

However, it is not just intentional attacks that remain a concern. The wide range of new publicly accessible and privately prescribed applications for patients, newly developed digital medical devices, shifts in protocols and processes, all can be a source of confusion which leads to mistakes made by end users – including both healthcare workers and patients themselves. As a result, personnel in healthcare settings at all levels and disciplines, need to acquire (new) digital skills that will ensure as cybersecure an environment as possible.

2.1 Main cyber threats for healthcare organisations

As all other organisations that offer digital services, healthcare organisations should be aware of and prepare for a wide range of cyber threats. The European Union Agency For Network And Information Security (ENISA) has clustered the main threats in five categories, as shown in Figure 1, namely: natural phenomena, supply chain failure, human errors, malicious actions, and system failure (ENISA, 2016, p. 21). These threats were originally defined for smart hospitals, yet they are also relevant for other healthcare services, such as nursing homes and home care services. The SecureHospitals.eu project focuses primarily on the role of human factors in cybersecurity in healthcare settings. User behaviour needs to be taken into account in cybersecurity, to achieve significant mitigation of risks. The most relevant threats to highlight in this section are related to human errors, but also to malicious actions that exploit insiders. Insiders can be current or ex-employees, contractors, vendors,

utility company technicians, and similar groups that are authorised to access the network and digital assets (Ayala, 2016, pp. 47-48)[1]. The threats in the category of **human errors**, and some of the category of **malicious actions** are the most relevant for the SecureHospitals.eu project.

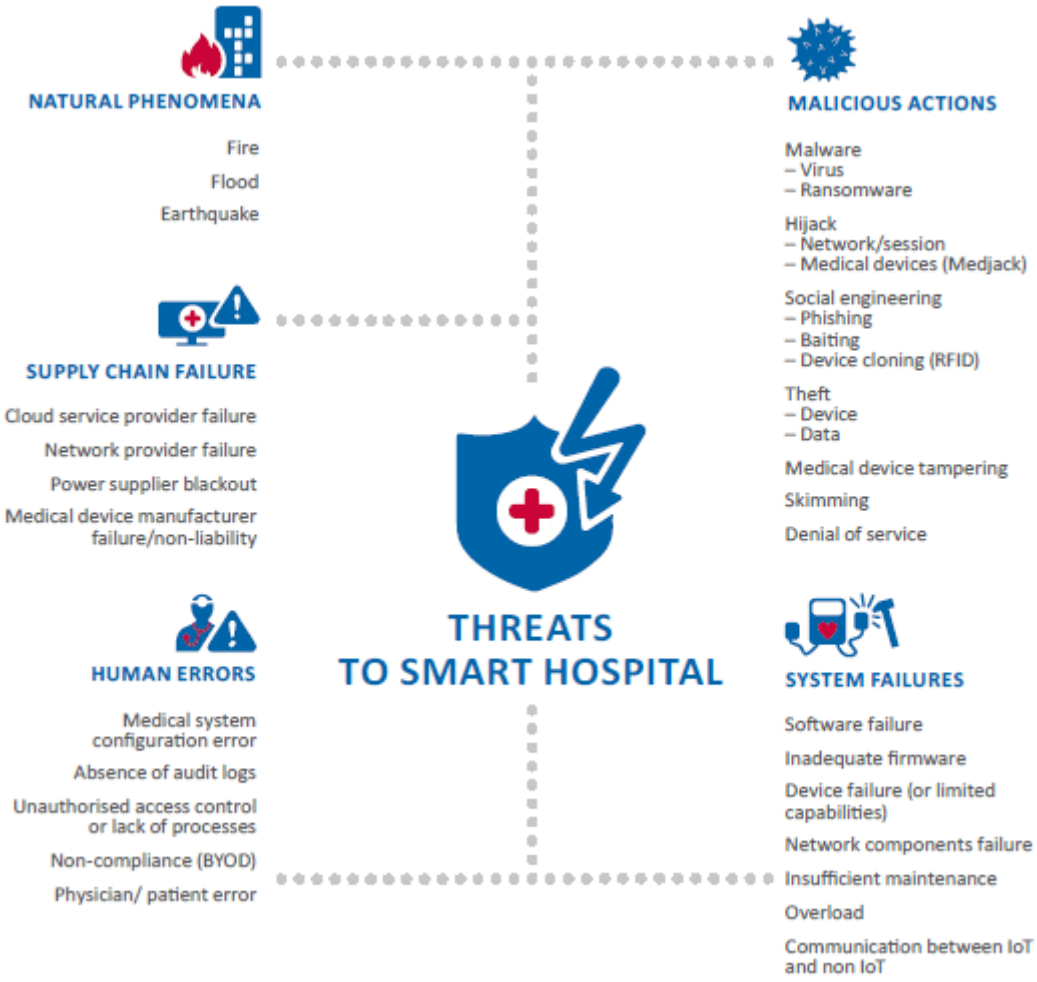


Figure 1 Threats to smart hospitals[2]

2.1.1 Human errors

Human errors are human-initiated actions that lead to a breach in the cybersecurity of a healthcare organisation. These actions are characterised by the absence of the intent to cause harm; they can be simple mistakes or accidents, or actions of which the perpetrator does not know or realise the possible consequences. Human errors are brought in connection to processes in an organisation and insufficient training (ENISA, 2016, p. 22). Examples of human errors are: physician and/or patient error, configuration errors, unauthorised access control or lack of processes, and non-compliance.

Physician and/or patient errors are considered 'a major threat' (ENISA, 2016, p. 22). These errors occur when medical staff or patients use digital services but are not IT experts, or when they have not received sufficient training. This type of error may also occur when the device or program is not

[1] For the purpose of this project we focus on unknowing insiders, not insiders who intentionally perform cyber-attacks.

[2] Reprinted from "Smart Hospitals. Security and Resilience for Smart Health Service and Infrastructures" by ENISA, 2016, p. 21. Copyright 2016 by ENISA. Reprinted with permission.

used as prescribed, e.g. the user employs a workaround in order to improve the workflow (Koppel, Smith, Blythe, & Kothari, 2015).

Medical system configuration errors are mistakes that pertain to settings of devices and their operation or the system's security settings (ENISA, 2016).

Unauthorised access control or lack of processes may be a risk when access controls are not defined properly, personnel may have access to patient data while they do not have an active role in the patient's treatment (ENISA, 2016).

Non-compliance to policies in the organisation cause weaknesses in the security ecosystem. A prime example is healthcare organisations that have a "Bring Your Own Device" (BYOD) policy in place (ENISA, 2016). This type of policy allows personnel to use their personal devices to access internal IT resources (Ogie, 2016, p. 114). Personal devices vary immensely and are not under direct control of the IT department, so they may not have the proper security measures installed (Marshall, 2014; Ogie, 2016).

2.1.2 Malicious actions exploiting insiders

Malicious attacks are deliberate actions by persons or organisations with the intent to cause harm (steal or leak patient data, obstruct healthcare services, and other adverse consequences) (ENISA, 2016, p. 22). Many of the malicious actions target insiders directly as they require additional actions from insiders to become active/effective. Examples are various type of malicious software (malware), social engineering, and device and data theft (Ayala, 2016; ENISA, 2016).

Malware is short for malicious software and can range from viruses to worms and ransomware. Each type of malware has its own mode of infection and reproduction throughout the network to other ICT systems. Malware is considered a key threat from outsiders (ENISA, 2018a; EUROPOL, 2018)

Social engineering is a method that enables cybercriminals obtain sensitive information or bypass cyber-security measures. Phishing is a well-known type of social engineering and "the most effective defence against social engineering is the education of potential victims" (EUROPOL, 2018, p. 13).

Device theft can provide access to the network of a healthcare organisation. Data theft is done for financial gains and/or to facilitate further illegal actions (EUROPOL, 2018). Policies such as BYOD policies can increase the risk of a network breach when a device is lost or stolen (ENISA, 2018a; Ogie, 2016). Theft and breaches can be aggravated by personnel, by not adhering to security policies or not securing their devices properly.

2.2 Training needs

Healthcare institutions are an increasingly attractive targets for cybercriminals, as healthcare data is considered more valuable to sell than credit card numbers (Sulleyman, 2017, as referenced by Coventry & Branley, 2018). Credit card information theft is quickly detected and reported, enabling banks to respond immediately and block the involved credit cards. In the case of patient data, it is generally not caught as quickly, making it possible for cybercriminals to sell or use the information to acquire healthcare services, medicine, or file fictional claims with insurances.

With the increased digitisation in healthcare and the accumulation of patient data, cyberattacks and human errors may become more common. Consequently, healthcare institutions are important

targets for cybersecurity improvement programs. The SecureHospitals.eu project aims to develop new training modules and materials to facilitate cybersecurity improvement in healthcare organisations. The training needs within healthcare organisations will at least in part correspond with the most relevant threats mentioned in the previous section. To holistically improve cybersecurity in healthcare settings, four areas are of interest: culture, people, processes, and technology (Coventry & Branley, 2018). For this project, culture and people are of particular interest.

2.2.1 Culture

The culture of an organisation has a strong influence on the activities and behaviour of personnel in that organisation. This is crucial for understanding cybersecurity practices within healthcare organisations. Organisational culture is influenced by what personnel believes to be the accepted beliefs and values. As a result, it steers group and individual behaviour (Thomson, von Solms, & Louw, 2006; Van Niekerk & Von Solms, 2010).

Values and beliefs develop slowly, which means that changing the organisational culture takes time. However, both values and beliefs are subject to what personnel has knowledge of (Van Niekerk & Von Solms, 2010), so by investing in training efforts on cybersecurity, the culture in healthcare organisations can grow to become cybersecurity positive.

2.2.2 People

Human errors are linked, among other factors, to inadequate training (ENISA, 2016) In many cases, education and awareness are the most effective strategy for defence (EUROPOL, 2018). Current healthcare personnel are in need cybersecurity-related knowledge and skills as well as a clear idea of their own role and responsibility in the organisation. Providing training programs on these topics will help to diminish the chance that cybersecurity incidents will occur in the future.

2.2.3 Processes

Processes support risk mitigation to an organization's information by defining an organization's activities, roles and documentation (Dutton, 2017). Processes should be under continuous review as the threat landscape is develops quickly. When processes are considered impractical, personnel will find workarounds to these issues to improve workflow (Koppel et al., 2015). In some cases, personnel resist newly implemented processes from the beginning (Merhi & Ahluwalia, 2019).

2.2.4 Technology

Traditionally, technology is the central factor in cybersecurity, and its critical role is undeniable. Due to considerations of for instance usability, cost and privacy concerns, trade-offs in the development and implementation of technology are made (Coventry & Branley, 2018; Lyon, 2017). Especially usability is diminished when security measures are implemented (Van Niekerk & Von Solms, 2010). Long and random passwords are safer than short passwords, yet are harder to remember without writing it down (Lyon, 2017). As shown before, personnel will find a way around technology that is deemed unusable or difficult to operate (Koppel et al., 2015). Healthcare organisations should therefore make sure that the technology they adopt is has an optimal balance between security and usability. The diversity of profiles, skills and competencies required to formulate and implement an effective cybersecurity training strategy can be daunting for healthcare organisations. To manage cybersecurity improvement programs, various different skills are required: computing or digital skills, but also a detailed knowledge of the dynamics and management processes of the healthcare institutions, the existing internal constraints, the available hardware and procedures for data

security. While training opportunities for many aspects of cybersecurity exist and cover several of the needs in the market, it seems that additional elements regarding the use of cybersecurity programs for non-technical stakeholders are still relevant and necessary.

2.3 Stakeholders and stakeholder engagement

The previous sections make clear that cybersecurity should be addressed in many ways. Cybersecurity is a multi-dimensional and multidisciplinary issue that is constantly changing and increasingly complex (Tisdale, 2015). It is an issue that cannot be solved from one perspective or without the support of all stakeholders.

2.3.1 Stakeholders of cybersecurity in healthcare settings

As it affects all parts of an organisation, everyone becomes a stakeholder in cybersecurity (Tisdale, 2015, p. 193). This means that each person, group, organisation, or other entity that participates directly or indirectly in cybersecurity in healthcare organisations is an important stakeholder for the SecureHospitals.eu project. Through the literature on cybersecurity in healthcare, many different types of stakeholders can be identified:

- Hospitals and other health delivery organisations, government institutions/regulators, medical equipment manufacturers, (IT) maintenance and operations specialists, procurement officers, the clinical community, cybersecurity researchers, patients, (Schwartz et al., 2018);
- Policy makers and employees (Li et al., 2019);
- Legislators and data protection officers (Coventry & Branley, 2018, p. 50);
- Employees, medical equipment vendors, and other internal and external stakeholders (Ayala, 2016, p. 78);
- Security professionals and scholars that are interested in open/emerging issues of cybersecurity, decision makers, security architects, risk managers, scholars and end-users, and professionals of any specialty, who are interested in understanding the state of play in the area of cyber threats (ENISA, 2018a).

The types of stakeholders are grouped and divided into eight categories in the next section, as seen in table 1.

The wide range of diverse stakeholders can complicate the progression of the SecureHospitals.eu project, as each stakeholder will have specific requirements and interests that must be met. These can conflict with cybersecurity measures, requiring the consortium to find a satisfactory balance between each (Lyon, 2017; Schwartz et al., 2018, p. 105). For example, employees will find workarounds for organizational processes or policies, or even outright reject them (Koppel et al., 2015; Li et al., 2019) and medical device development can be subject to trade-offs (Coventry & Branley, 2018; Lyon, 2017). At the same time however, cybersecurity improvement is a multidisciplinary challenge (Tisdale, 2015) and ignoring a set of stakeholders may lead to ineffective cybersecurity improvement programs. Building on the experiences of stakeholders, and including them in the development and testing of innovative training solutions, will only be beneficial to the SecureHospitals.eu project.

2.3.2 Stakeholder engagement strategy

Including stakeholders is essential to the success of the SecureHospitals.eu project. Strategic communication is at the core of a successful engagement strategy and will help raising awareness on

the project and project outcomes. It will keep stakeholders interested in the developments and it will help to attract new interested parties (European Commission, 2014).

The goal of the stakeholder engagement strategy for the SecureHospitals.eu project is three-fold: (1) to expand the consortium's network in the healthcare sector and the IT sector, (2) to raise awareness on the SecureHospitals.eu project and its goals, and (3) to ensure the continued use and success of the Online Information Hub after the project is completed.

Identification of the relevant stakeholders is the first step in the engagement strategy. The list in the previous section gives the consortium a clear overview of who in their existing networks they can involve. It also provides an indication in which areas new or additional connections need to be made. The next step of the engagement strategy is communication with the identified stakeholders. In WP 6 Communicate, the communication and dissemination activities are described.

A project website will serve as the main channel for communication to the stakeholders and interested parties (task 6.1). Regular updates of project developments and outcomes will be presented on the project website. Additionally, by employing social media, such as Twitter, Facebook and LinkedIn, the reach of communication efforts is increased. Newsletters, factsheets, leaflets and infographics will contain updates on project activities and the content that is created (task 6.2). These will be disseminated through the project website and social media channels. Visiting conferences and publishing on external communication platforms, such as blogs, will improve the outreach to a wider network (task 6.3). Creating an extensive exploitation strategy will ensure sustainability of the outcomes of the project and future use of the knowledge of the consortium partners and stakeholders (task 6.4). Finally, the consortium will organise a conference and invite all stakeholders and interested groups involved in the SecureHospitals.eu project. The conference will serve as a way to celebrate a successful ending to the project, and to ensure future use and success of the Online Information Hub.

3. Engagement Plan

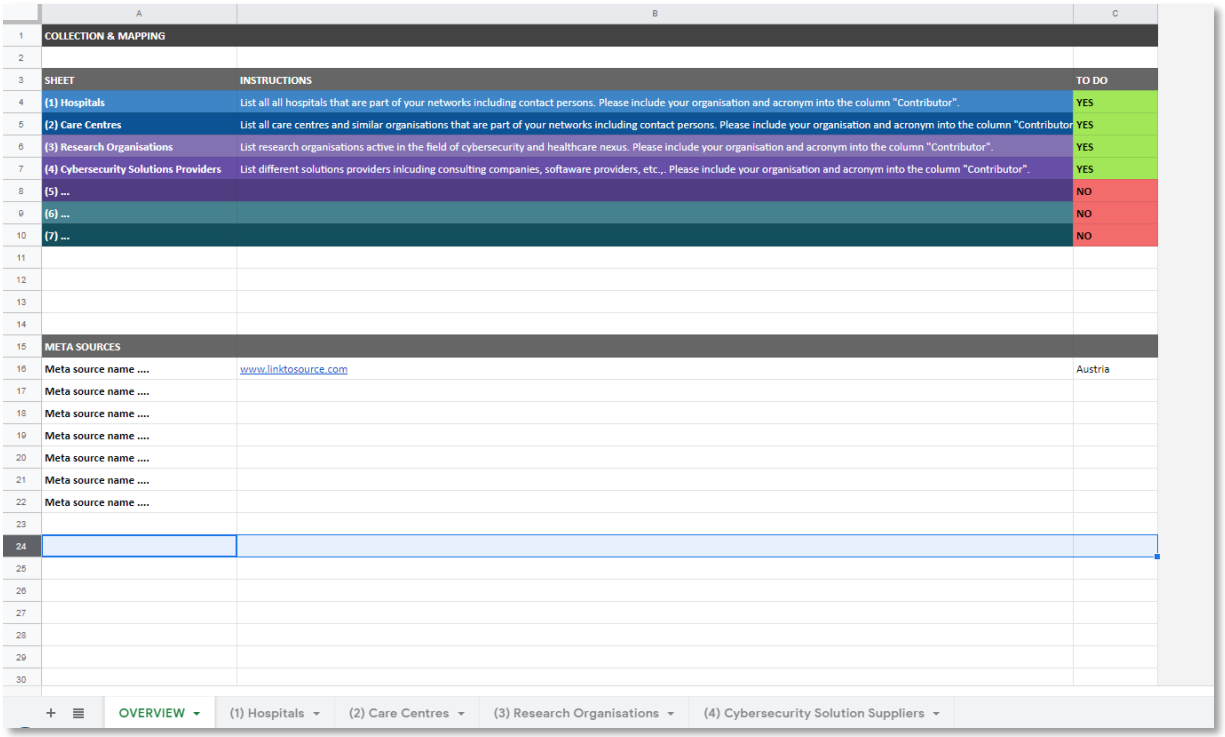
This Plan describes the process the consortium will carry out to identify the key stakeholders, the challenges and needs they are facing and the engagement approaches to be implemented. Specifically, the INVOLVEMENT phase will serve the purposes to:

- Identify the key stakeholder to be involved in the project activities (**WHO**)
- Explain the reasons why these stakeholders should be involved (**WHY**),
- Elaborate actions to attract them and gain their interest and engagement (**HOW**)

3.1 Stakeholders identification (WHO)

Since the beginning of the project, the partnership has identified a set of stakeholders' typologies potentially interested in the project activities and outcomes. Collection tools, in the form of excel sheets, have been created and shared by online service; the sheets are continuously filled in by SH Consortium with the aim to make available relevant information on professionals and organizations to be gathered and then contacted and engaged. Partners have started filling them in, initially including contacts from their own networks, then they will enrich the lists with new entries during the project life. This approach will allow the implementation of a repository of data and information to be used for other WPs and Deliverables to come.

There are actually three different collection tools (excel sheets) aiming to *map* the context: The Project Landscape, the Stakeholders Landscape and the Training Landscape. The Stakeholders Landscape Sheet is particularly relevant for present document scope (Figure.2)[3].



	A	B	C
1	COLLECTION & MAPPING		
2			
3	SHEET	INSTRUCTIONS	TO DO
4	(1) Hospitals	List all all hospitals that are part of your networks including contact persons. Please include your organisation and acronym into the column "Contributor".	YES
5	(2) Care Centres	List all care centres and similar organisations that are part of your networks including contact persons. Please include your organisation and acronym into the column "Contributor	YES
6	(3) Research Organisations	List research organisations active in the field of cybersecurity and healthcare nexus. Please include your organisation and acronym into the column "Contributor".	YES
7	(4) Cybersecurity Solutions Providers	List different solutions providers inlcuding consulting companies, softaware providers, etc.,. Please include your organisation and acronym into the column "Contributor".	YES
8	(5) ...		NO
9	(6) ...		NO
10	(7) ...		NO
11			
12			
13			
14			
15	META SOURCES		
16	Meta source name	www.linktosource.com	Austria
17	Meta source name		
18	Meta source name		
19	Meta source name		
20	Meta source name		
21	Meta source name		
22	Meta source name		
23			
24			
25			
26			
27			
28			
29			
30			

OVERVIEW | (1) Hospitals | (2) Care Centres | (3) Research Organisations | (4) Cybersecurity Solution Suppliers

Figure 2 Collection Tool – shared table to collect stakeholders contacts

The stakeholders are presently categorized in 8 groups (Tab. 2). The last two categories have been identified as potential stakeholders after the collection tool had been created, and will be added to it. Should other relevant categories emerge during the project lifetime, they will be added to the list, either.

[3] The collection sheets used in the project (responding to the terms set out in the Grant Agreement), include a repository of personal data within the meaning of Article 4, 1 of the Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR"). In order to ensure that the data processing procedures within the consortium comply with all the legal obligations set forward by the GDPR, the legal partner TLX has drafted an agreement regulating the processing of personal data in the context of the Grant Agreement. The agreement has been reviewed and signed by all partners.

Table 1 Stakeholders categories

(WHO) STAKEHOLDER CATEGORIES
Hospitals
Care centres
Medical Research organizations
Health professionals (freelance specialists)
Cybersecurity solutions providers
Cybersecurity trainers
Policy Makers
Networks and umbrella organizations

It has to be taken into account that organizations employ a variety of professional profiles, with different roles and technical skills, whose specific needs will have to be identified and mapped, in order to provide customized training.

3.2 Stakeholders needs and challenges (WHY)

It is essential to think why to engage someone and what needs are to be met. A cybersecurity program should be able to capture the key stakeholders' needs and their organizational requirements to build an effective training concept.

SecureHospitals.eu has been following a four-steps procedure to identify relevant stakeholders, the reasons why to engage them and their training needs:

- **Step one**: in this very first phase of the project, the consortium has signalled organizations and stakeholders belonging to their own networks, whose needs and challenges are already known or can be easily investigated. Their motivation to join the SecureHospitals.eu are clear and their engagement in its activities guaranteed.
- **Step two**: a more in-depth literature review will be carried out, to gather further knowledge on the needs and problems of specific stakeholders' typologies;
- **Step three**: an on-line survey will be carried out, to gather further information from stakeholders the consortium hasn't direct contacts with, but who can be interested in the project and in contributing to its activities and outputs through the OIAH. Different information gathering tools are available, among which the CTI Maturity Model, proposed by the ENISA Threat Landscape report 2018 [4], which can be used to evaluate the state of cybersecurity programs and to ascertain whether certain preconditions are met in the implementation of such programs. The consortium will identify other available tools and will propose other questions they deem as relevant for the SecureHospital.eu purposes.

- **Step four**: all the contacts will be invited to join the OIAH, to create an online Community of Practice for the lively exchange of experiences, problems, suggestions, materials and good practices.

The following table provides a preliminary framework, which will be expanded during the project progress:

Table 2 Risks and related training needs

STAKEHOLDERS	WHY	TRAINING NEEDS
Hospitals	– *Favourite targets for cyber attacks;* – *Setting up complex digital services;* – *Using new ICT-based devices;* – *Multi-actor staff with different competences;* – *Complex organizational structure;* – *Data management procedures not clear to all;* – *Obsolete Technology*	*Increase awareness on risks;* *Technical training* *Human mistakes and how to avoid them.*
Care centres	– *Possible targets for cyber attacks;* – *Under digitalization processes;* – *Using ICT-based devices;* – *Health staff, with low technical skills and awareness about possible risks;* – *Obsolete technology* – *Poor attention to the management of data*	*Increase awareness on risks;* *Technical training* *Human mistakes and how to avoid them.*
Research organizations	*Low awareness on cyber risks connected with the digitalization of care services*	*Technical training* *Human mistakes and how to avoid them.*
Cybersecurity solutions providers	*They can offer solutions but don't have a clear overview of the different stakeholders needs*	*Match the cyber threats with stakeholders and their needs*
Cybersecurity trainers	*To adapt and update their training/knowledge to the need of the different stakeholders*	*Match the cyber threats with stakeholders and their needs*
Policy makers	– *They can mainstream cyber security* – *Increase their awareness of risks*	*Awareness, adequate guidelines, legislation, EU directives*
Umbrella organizations Networks	– *Possibility to reach a big number of stakeholders*	*Modular training adaptable to the different contexts*
Health professionals	– *Possible targets for cyber attacks;* – *Under digitalization processes;* – *Using ICT-based devices;*	*Increase awareness on risks;* *Technical training*

3.3 Stakeholders engagement methods and tools (HOW)

Stakeholders Engagement is a continuous and systematic process by which an organization establishes a constructive dialogue and a fruitful communication with its key stakeholders. It requires the possibility of a confrontation and the search for solutions that best fit the specific social and environmental context. Building trust-based relationships is a key to success. More than one engagement methods do exist to best approach the different interlocutors, their selection depending on the level of confidence and relations established with them. For the project purposes, two main categories of engagement methods are proposed:

1. Methods to be used with partners' direct contacts, whose interest and engagement in the project is guaranteed (**High truthfulness/personal contacts**);
2. Methods to be used with potential stakeholders, who can be reached through the partners' networks but whose engagement cannot be given for granted (**Low confidence**).

The two methods imply different approaches and tools for engagement, as shown in the following table (Figure 3):

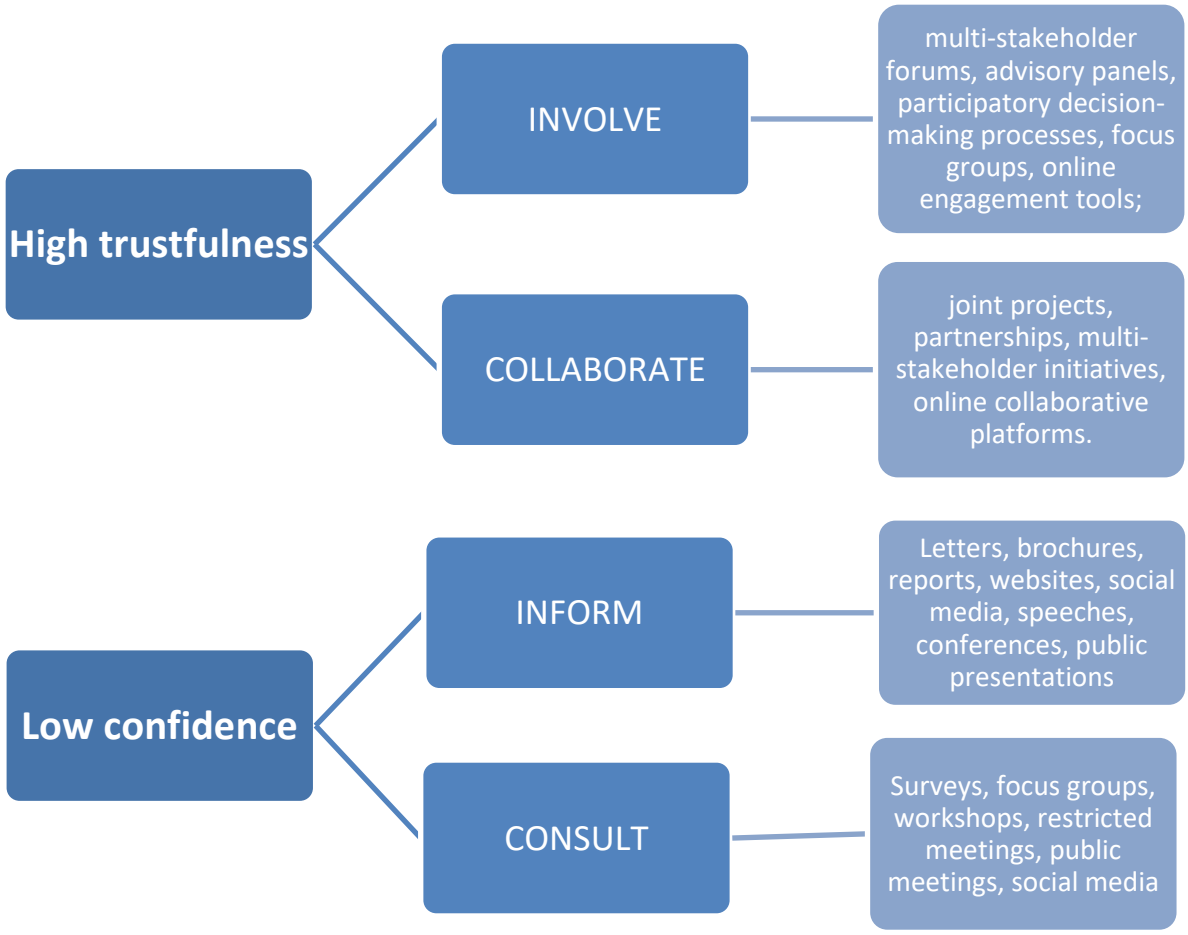


Figure 3 Engagement: levels methods and tools

A short description of the partners' engagement plans follows, with a preliminary indication of their contacts and the engagement methods to be applied.

3.4 Partners' engagement plans

INSP has several connections with health and care organisations or cybersecurity solutions providers through its involvement in research and innovation project with a focus on healthcare. As such INSP has started with the identification of existing partners from the field and drew their attention to the project aims and upcoming activities. The existing partners network includes a considerable number of to hospitals and care centres across Europe, medial emergency service providers, and cybersecurity solution providers. Based on the required inputs or types of engagement in several project stages, existing partners will be contacted directly and asked for their inputs. The secondary targeted audience for INSP is the community of stakeholders in Austria. Through the connections with local authorities, closer ties with hospitals, care centres, knowledge institutes and umbrella organisations will be sought. The ultimate goal of stakeholder mobilisation for INSP is to draw attention on the Open Information and Awareness Hub and make it a lively space in which the community comes together and useful resources for healthcare organisations and professionals. To do so it will employ its expertise in research marketing and online campaigns for targeting a third circle of stakeholders from all around Europe.

EUR has outlined a three-fold strategy for the involvement of stakeholders. First, it will leverage already existing connections with two leading university hospitals, Erasmus MC and Amsterdam UMC to facilitate new connections particularly in relation to university or teaching hospitals in the Netherlands. These connections will be utilized to collect current practices and experiences with regards to digital healthcare practices, the solutions and solution providers they work with, as well as identify the needs that may exist within healthcare organizations and among their personnel. Second, it will connect with knowledge institutes and umbrella organizations to gain access to their network and member organizations to explore how their members implement digital healthcare and cybersecurity practices, and discern their most forward-thinking members to gather best practices and lessons learned. At present the access to these organisations is limited, but direct contact processes and an upcoming ICT and healthcare conference in March will help the process. Third, it will contact specific healthcare organizations identified to be leaders in terms of digital healthcare practices, to draw on their experiences and lessons learned, as well as identify their preferred solutions and solution providers.

TLX as a law firm, has only limited connections with healthcare providers. Nonetheless, TLX already started the engagement of several privacy, data protection and IT-security specialists. Firstly, TLX plans to involve a number of data protection officers and IT-officers from Flemish hospitals. To this end, TLX is currently discussing the involvement of a Flemish network of healthcare organisations that could bring the SecureHospitals.eu project closer to the data protection officers and IT-officers in Belgian hospitals. Secondly, thanks to TLX's long RIA/IA project history, TLX has built up a broad network of project partners specialised in privacy, data protection and IT-security (in the healthcare sector) who are potentially willing to collaborate with the SecureHospitals.eu project. TLX already reached out to a number of potential companies and research centres that are likely to engage in joint projects and partnerships (e.g. Cefriel, Engineering of the Hermeneut project and CITIP KU Leuven). Thirdly, TLX can rely on a broader network of privacy, data protection and IT-security specialists to further assist in reaching out and to inform a broader range of key stakeholders in the healthcare sector.

FPHAG has strong relationships with key stakeholders of level 1 in the area of Barcelona and surroundings, and will further expand organically using a strategy for the involvement of stakeholders belonging to level 1 and 2 at local level. Presently, FPHAG is in contact with an initial directory of relevant stakeholders. Primarily, with Hospitals, Care centres, research organizations and their health professionals, IT professionals, patients, carers. FPHAG will further contact initially identified potential stakeholders who may be interested in the project, which is aligned with FPHAG's research and innovation lines, and also could potentially benefit from the project. Addressing these stakeholders by using a consistent and methodological approach based in disseminating and communicating the outcome results of the project.

COOSS directly manages 8 care centres for elderly people within the regional territory: being of its own property, they can be placed under level 1 of the engagement plan. It also manages many other care centres for elderly, disabled and mental impaired people on behalf of local authorities, but because of the formal and bureaucratic aspects, they have to be placed at level 2. As for policy makers, COOSS collaborates with many Municipalities (many of them at level 1) and with the Regional Government (level 2). Finally, COOSS has active conventions with two universities (UNIVPM and UNICAM), both of which to be placed under level 1, and has links with other research centres and EU project partners, who belong to level 2.

SAM will try to win the interest of some other homecare organisations in Vienna, with 3 of them hopefully being interested enough to support our project. Regarding the other groups of potential stakeholders, we do not have connections there. We will instead focus on the experiences of our own staff with Cybersecurity issues.

JOIN will take up contact to the Johanniter Hospitals in Germany and to European Associations of Hospital Engineers. Furthermore, JOIN has a clinical working group staffed with medical doctors from several hospitals, who will be involved in contacting additional stakeholder units. As JOIN is located in Brussels, the office group will visit dedicated events for cybersecurity and health care services to increase visibility of the project on EU Level and increase contacts.

EAN has already asked their members (means associations and social Services providers) for their contacts - specifically the relevant persons who are responsible for data security. They received several answers and promises for cooperation. They are also in touch with the Czech company IRESOFT which is provider of software in ca. 600 social care facilities in CZ. Hope they will be able to help us and provide us with their solutions.

3.5 Risks factors and mitigation plans

When different stakeholders are engaged, the human resources to be involved and their time constraints should be taken into account. Besides, communication channels, ICT availability, internal rules, social hierarchies and lack of shared understanding might reveal factors that can impede the ability of stakeholders to engage. To minimize these risks, the engagement process should ensure that:

- stakeholders are informed and invited to participate to the project activities in advance;
- communications are appropriate for each stakeholder;
- reasonable time is allowed to the stakeholders for reactions;
- engagement process and activities are well documented;

- activities are monitored and results evaluated.

3.6. Advisory Board Members

The set up of an external Expert & Advisor Board (EAB) is foreseen, to deliver valuable inputs and feedback at different stages of the project.

A list of possible candidates has been signalled by the partners, based on their competences in different fields of interest for SecureHospitals.eu. In general, the EAB is expected to provide additional quality assurance in the form of high-level reflections and guidance for the SecureHospitals.eu actions. For the purposes of WP2, these experts will promote the participation of other external and associated stakeholders in the project and will support the linkages for networking activities.

At the time of this deliverable, the following experts have expressed their interest to support the project activities:

Dr. Enrico Frumento (IT), expert in secure code development, hacking/cracking techniques, Social Engineering and cybercrime prevention;

Dr. Herlinde Toth (AT), has been working in health IT for more than 30 years in various executive positions. She is e-health coordinator of the city of Vienna and spokesperson for ELGA and e-health within the forum of the IT managers of Austrian KH carriers

Dr. Henk A. Marquering (NL), associate professor at the Amsterdam UMC, location AMC, working on combined heterogeneous imaging with clinical data analysis with a growing interest in cybersecurity issues.

Frederic Lievens (BE), expert in quality standards for telehealth services, standardization around ICT-based products and services to support active and healthy ageing, technological innovation in home healthcare, in which cybersecurity, privacy and safety are among some of the major concerns.

Csaba Virág (HU), Head of Cybersecurity Competence Center, senior cybersecurity expert with a strong focus on training and healthcare.

Dr. Ad Van Berlo (NL), psycho-gerontologist and mechanical engineer, expert in the field of biomedical technology and e-health. He is manager R&D of Smart Homes and works in the area of smart houses, telemedicine, e-health and AAL, mainly for welfare, care and ageing.

4. Roadmap

The project engagement plan can be summarised in a roadmap which, starting from the identification of the stakeholders (WHO) which might be interested in taking part to the project activities (WHY), indicates possible methods and tools for their engagement (HOW) (Figure 4).

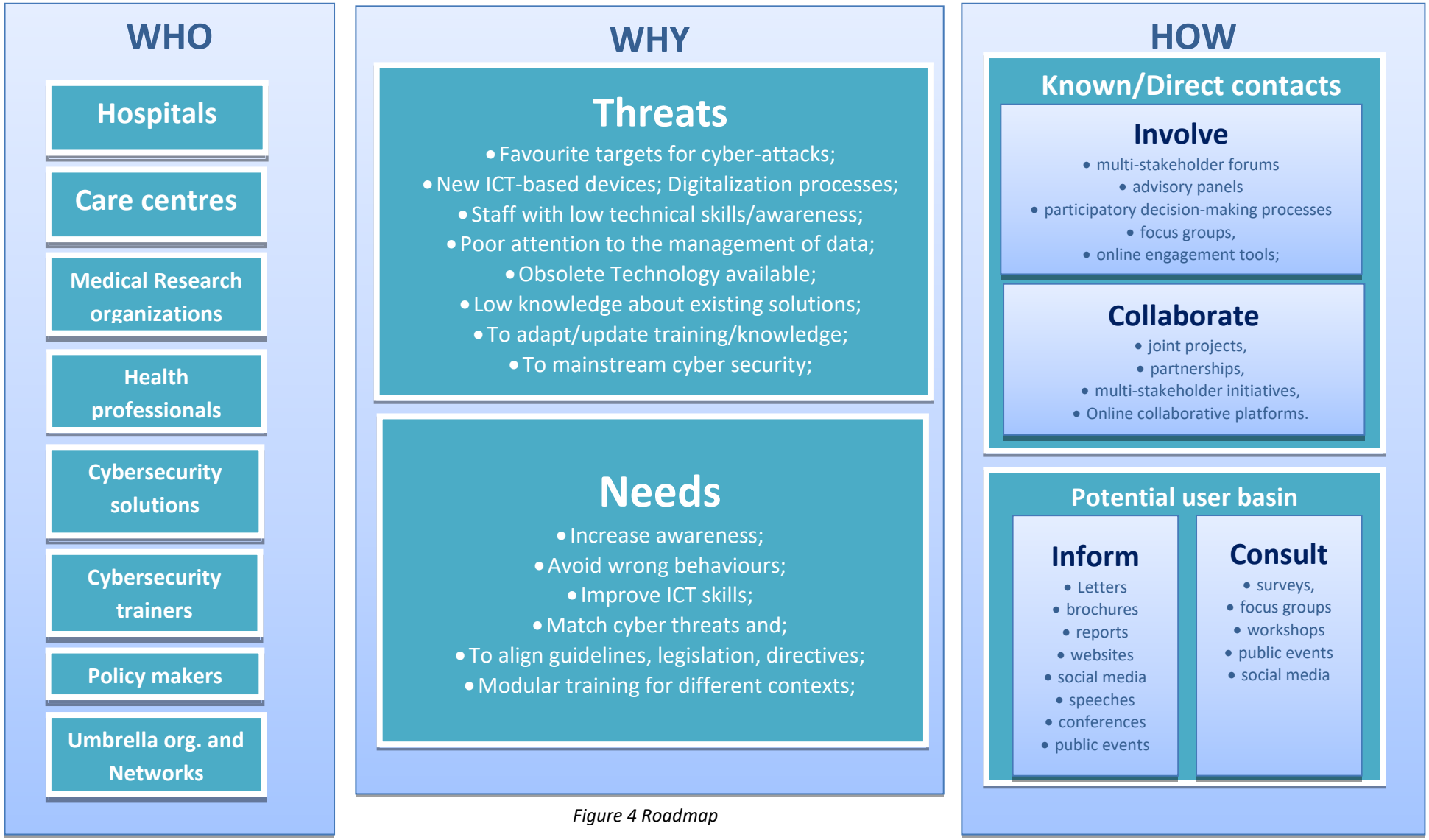


Figure 4 Roadmap

5. Conclusions

Cyber-threats can spread contagiously in the cyberspace causing long lasting damages, especially when organizations or individuals do not have the needed competence to adhere to good security practices, or to operate security systems. It is necessary that each organization includes cybersecurity strategies into its risk management plans, in order to anticipate crises or to properly face them.

End users are under permanent exposure to a vast number of attacks, mainly because of their lack of technical competences, or of the weak protection systems. It is imperative to fill this gap allowing all the subjects operating in the health and care services to access a specific knowledge customized to their needs and competences.

Because of the different profiles, skills and competencies operating within an organization, it can be difficult to formulate an effective cyber security strategy. Providing key stakeholders with effective tools for discussion and knowledge exchange is a key to success.

Much more training offerings has to be developed in order to satisfy the current market needs, in a form that is understandable by non-expert users.

The setting up a OIAH (Online Awareness and Information Hub) is the novel and affordable solution SecureHospitals.eu is proposing: this online space will enhance discussion on the topic of cybersecurity in health settings, will propose guidelines and assessment toolkits for the detection and analysis of vulnerabilities and will offer baseline training to all interested organizations, covering sectorial and low-maturity needs.

Stakeholders engagement is the primary key to success: this deliverable was meant to provide a roadmap for the involvement of relevant actors and organizations for all the project lifetime.

6. References

Ayala, L. (2016). *Cybersecurity for Hospitals and Healthcare Facilities. A Guide to Detection and Prevention.* Apress.

Chiaraluce, F., Ceravalo, M. G., Baldi, M., Maturo, N., Pepa, L., Rosetti, R., … Fattobene, L. (2019). The ASSECURE project - Final report. Retrieved from https://sites.google.com/view/assecure/home

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48–52.

Dutton, J. (2017, September 26). Three pillars of cyber security. Retrieved February 19, 2019, from https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security

ENISA (2016). Smart Hospitals. Security and Resilience for Smart Health Service and Infrastructures [Report]. Retrieved January 29, 2019, from https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

ENISA (2018a). *ENISA Threat Landscape Report 2018*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

ENISA (2018b). Looking into the crystal ball: A report on emerging technologies and security challenges. Retrieved from https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball

European Commission (2014). *Communicating EU research and innovation guidance for project participants* (pp. 1–13). European Commission. Retrieved from http://ec.europa.eu/research/participants/docs/h2020-funding-guide/grants/grant-management/dissemination-of-results_en.htm

EUROPOL (2018). Internet Organised Crime Threat Assessment (IOCTA). Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment

Koppel, R., Smith, S., Blythe, J., & Kothari, V. (2015). Workarounds to computer access in healthcare organizations: you want my password or a dead patient? *Studies in Health Technology and Informatics*, *208*, 215–220.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Lyon, D. (2017). Making Trade-Offs for Safe, Effective, and Secure Patient Care. *Journal of Diabetes Science and Technology*, *11*(2), 213–215. https://doi.org/10.1177/1932296816676281

Marshall, S. (2014). IT Consumerization: A Case Study of BYOD in a Healthcare Setting. *Technology Innovation Management Review*, (March 2014: Emerging Technologies), 14–18.

Merhi, M., & Ahluwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to Information Systems Security. *Computers in Human Behavior*, *92*, 37–46.

Ogie, R. (2016). Bring Your Own Device: An overview of risk assessment. *IEEE Consumer Electronics Magazine*, *5*(1), 114–119. https://doi.org/10.1109/MCE.2015.2484858

Schwartz, S., Ross, A., Carmody, S., Chase, P., Coley, S. C., Connolly, J., … Zuk, M. (2018). The Evolving State of Medical Device Cybersecurity. *Biomedical Instrumentation & Technology*, *52*(2), 103–111. https://doi.org/10.2345/0899-8205-52.2.103

Sulleyman, A. (2017, May 12). Why hackers just launched a huge cyber attack on the NHS. Retrieved February 18, 2019, from http://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable-to-sell-financial-a7733171.html

Thomson, K.-L., von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *2006*(10), 7–11. https://doi.org/10.1016/S1361-3723(06)70430-4

Tisdale, S. M. (2015). Cybersecurity: Challenges from a systems, complexity, knowledge management and business intelligence perspective. *Issues in Information Systems*, *16*(III), 191–198.

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476–486. https://doi.org/10.1016/j.cose.2009.10.005