SECUREHOSPITALS.EU

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

D5.1 Training Strategy 1

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:	**D5.1**
Title:	**Training Strategy 1**
Lead beneficiary:	**JOIN**
Work package:	WP5
Dissemination level:	Public (PU)
Type	Report (R)
Due date:	28.02.2019
Submission date:	04.03.2019
Authors:	**Georg Aumayr,** JOIN **Joachim Berney,** JOIN **Eva Pelgen,** JOIN
Contributors:	**Stela Shiroka**, INSP **Tessa Oomen,** EUR **Jason Pridmore,** EUR
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.	**Disclaimer:** The content of this publication is the sole responsibility of the authors, and does not in any way represent the view of the European Commission or its services.

TABLE OF CONTENT

EXECUTIVE SUMMARY

D5.1 is the first report of work package 5 (BOOST). It is dedicated to identifying primary channels to reach out and engage participants for the upcoming project trainings. It is meant to identify specific audience for the trainings by a stakeholder analysis and defines a value proposition for increasing the chance to reach the audience for trainings.

Within this document the results of a preliminary stakeholder analysis are presented and a discussion of the target groups of the project trainings is done with a focus on communication and command flows. This helps specifying the audience for training.

A value proposition is presented for a clear communication of objectives in relation to needs of potential participants in the trainings. This helps in a clear communication towards the audience of trainings.

Conclusion of this deliverable is a strategy of communication based on the idea of interpunction towards the dynamic communication between hospital management and health care staff. The main communication channel will be through eMail and online material in general. As described in D2.1, project partners are working on stakeholder lists at the organisational level, to be contacted for promoting project trainings and activities and further on for general awareness raising.

TABLE OF FIGURES

TABLE OF TABLES

1. Introduction

At the first training strategy report, the main focus is on the identification of key types of stakeholders that will be targeted by the trainings offered from the SecureHospitals.eu project, to have an impact on their organisational change. A crucial component of this is identifying the best communication channels to address these stakeholders for trainings.

In order to accomplish this, a first stakeholder analysis in relation to the project has been completed on an internal basis in accordance with the results of three independent interviews with people working on the topic of cybersecurity in hospitals, and the development of D2.1 which focuses on a roadmap for stakeholder involvement. This provides insight into the types of relevant stakeholders and how best to address them.

In a second stage, a group discussion at the kick off meeting focused on the most promising strategies for addressing primary end users and identifying flows of communication. The third stage of this report will describe the concrete communication channels to be used for reaching out to the training participants.

This report reflects the current state of research on potential training participants and means of engaging them. Further contacts will be collected throughout the project lifetime and the communication towards the entities that are supporting training and running training will be dynamically adapted towards the needs of the project and target groups. The main aim is to support the engagement of operative people into the project.

2. Value Proposition

In order to effectively engage the identified stakeholders in participating in the project trainings, it is necessary to identify their training needs and how these needs can be met by the training that will be offered by the SecureHospitals.eu project. This analysis will be used to produce our project's value proposition as outlined below, to be communicated through channels noted in section 5 below.

To develop the project's value proposition, it is necessary to define the target groups and customer segments to be addressed. A value proposition canvas is an effective tool to support a standardised and understandable analysis for this purpose. It helps define what the customer is willing to do and what kind of motivation and aims this group of people has. Customers in the sense of the SecureHospitals.eu project are health care staff and decision makers within hospitals who would commission a SecureHospital.eu training.

With this focus, a value proposition is a promise to fulfil the needs of "customers" by identifying their "pains" and "gains". The value proposition is also the definition of aims to be achieved by the product or development. Comparing our ideas for development and this might deal with the pains and gains of the customers delivers a clearer idea of how to communicate with a potential customer. A value proposition may change for each target group or customer segment.

Osterwalder (2010) formed a practical approach to address the value proposition by a graphical model, here in a version for SecureHospitals.eu in a draft version:

Target Group Primary End-User healthcare Staff

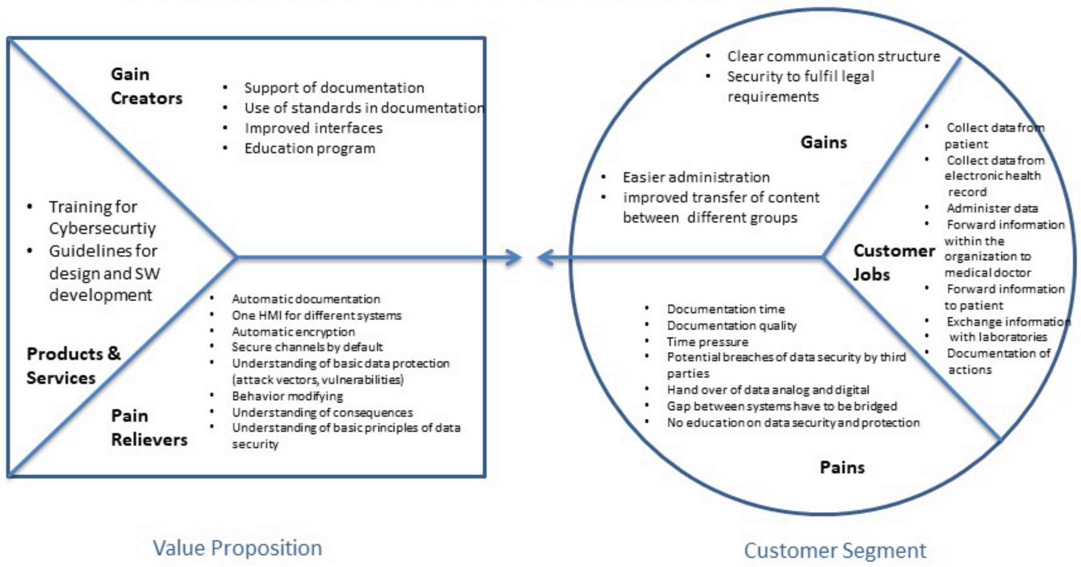

Gain Creators
Support of documentation
Use of standards in documentation
Improved interfaces
Education program
Training for Cybersecurtiy
Guidelines for design and SW development
Products & Services
Automatic documentation
One HMI for different systems
Automatic encryption
Secure channels by default
Understanding of basic data protection (attack vectors, vulnerabilities)
Behavior modifying
Understanding of consequences
Understanding of basic principles of data security
Pain Relievers
Clear communication structure
Security to fulfil legal requirements
Gains
Easier administration
improved transfer of content between different groups
Collect data from patient
Collect data from electronic health record
Administer data
Forward information within the organization to medical doctor
Forward information to patient
Exchange information
with laboratories
Documentation of actions
Customer Jobs
Documentation time
Documentation quality
Time pressure
Potential breaches of data security by third parties
Hand over of data analog and digital
Gap between systems have to be bridged
No education on data security and protection
Pains
Value Proposition
Customer Segment

Figure 1: Value Proposition Canvas

This Value Proposition Canvas demonstrates the connection between needs of stakeholders and developed solutions. Osterwalder uses terms like customer, gains, pains etc. because of the fast understanding of these terms. Customers could also be stakeholders, decision makers or investors. GAINS could also be benefits, motivations etc. PAINS refer to similar kind of negative motivations and troubles a customer would handle during his or her job.

For SecureHospitals.eu this approach was used to allow a focused analysis of needs and stakeholders at an early stage of the project. This would also fit into the topics for trainings and to build up a course with a high level of acceptance.

2.1 Customer JOBS

Customer jobs are tasks that need to be fulfilled by the primary end-user and that are in the focus of development. In the case of SecureHospitals.eu this includes healthcare staff. Osterwalder used this term to allow a better understanding of the nature of this element as jobs need to be done and are not always something people chose. It is more holistic than tasks.

For Cybersecurity and the project perspective on this subject, in a first iteration, the customer jobs were identified as:

- Collecting data from patients
- Collecting data from electronic health records
- Administering data
- Forwarding information within the organization to medical doctors
- Forwarding information to patients
- Exchanging information with laboratories
- Documenting actions

Within these actions, information and data is exchanged or processed between administrative units. These actions are sensitive to potential cybersecurity breaches. From the project perspective, these are key concerns for training interventions.

2.2 PAINS

The burdens of 'customers' are identified and described as 'pains' which lists either pressure, failures, and increased chances for errors and system failures. For SecureHospitals.eu these pains were identified as:

- Documentation time
- Documentation quality
- Time pressure
- Potential breaches of data security by third parties
- Handover of data analog and digital
- Gaps between systems that have to be bridged
- Limited education on data security and protection
- Financial constraints

2.3 RELIEVERS

The concept of 'relievers' describe the means for easing the identified pains. Compared to the gain supporter, this is pointing at solving mis-situations and troubles directly. For SecureHospital.eu relievers as such were identified:

- Automated documentation
- One HMI (Human Machine Interface) for different systems
- Automatic encryption

- Secure channels by default
- Understanding of basic data protection (attack vectors, vulnerabilities)
- Behaviour modification
- Understanding and awareness of consequences
- Understanding basic principles of data security

2.4 GAINS

The GAINS of customers are focused on potential benefits and comforts. Things that make work easier and provide an increased efficiency to work are referred as GAINS. For SecureHospital.eu primary end-users (PEU) could be identified as:

- Clear communication structure
- Security to fulfil legal requirements
- Easier administration
- improved transfer of content between different groups

2.5 CREATORS and Supporters

Creators and supporters are focused on the transfer from GAINS towards an operative aim of development. For SecureHospitals.eu creators could be identified as:

- Support of documentation
- Use of standards in documentation
- Improved interfaces
- Education program

3. Stakeholder Analysis

The stakeholder analysis is supporting the identifying of contacts for training by using the target group and setting it into an analysis with its environment. The stakeholder groups are estimated by their influence and power in several domains (see Figure 2). This allows an understanding of where financial power lies, where staff power is hidden, where expertise is involved, and experience was gained already. With this understanding of stakeholders, a better communication towards potential partners is supported and efficient.

As part of D2.1, the relevant stakeholders for the SecureHospitals.eu have been identified. These stakeholders are divided in seven groups:

1. Hospitals
2. Care centers
3. Research organizations
4. Healthcare professionals
5. Cybersecurity solution providers
6. Cybersecurity trainers
7. Policy makers

The stakeholder groups benefit differently from the SecureHospitals.eu project. As such, they are categorised as follows: primary end users, secondary end users and tertiary end users. The communication and engagement of each stakeholder group should be appropriate to the level to which they belong.

3.1 Primary end-user

The primary end user is the individual directly benefiting from the proposed training. In the context of the SecureHospitals.eu project, the healthcare professionals and other staff of healthcare organisations (group 4) are considered the primary end users. Examples are medical doctors, nurses, administrators, cleaning staff, security staff, maintenance staff, and many more.

3.2 Secondary end-user

The group of secondary end users consist of the organisations that provide healthcare services, such as hospitals and care centres (group 1 and 2). They are the employers of the primary end users. The secondary end users are in direct contact with SecureHospitals.eu project members. This can be a group of people, individuals or functions of a system.

3.3 Tertiary end-user

The tertiary end users are stakeholders that create or provide policies, regulations or institutional structures. These stakeholders, such as policy makers (group 7) are not in contact with SecureHospitals.eu in a direct or indirect way. However, this group are important stakeholders as they influence the environment of the project and its customers.

The three remaining groups, namely research organizations (group 3), cybersecurity solution providers (group 5) and cybersecurity trainers (group 6), are not considered to be end users, but are part of the solution chain. Their involvement will follow their value chain. As in Figure 3 is shown, these are the groups with the highest direct benefit of SecureHospitals.eu. This shows the potential of motivation to support actions of this project to favour their own purposes.

3.4 Stakeholder influence

To further determine the influence of each stakeholder group, the project team clarified the relation of the stakeholders towards the project and the topic. Eight categories were used, ranging from 1 to 5. The categories are: **experience with similar projects, organisational power, financial resources, staff power, professionality, expertise, public resonance and lobbying power**. A visualisation of the results, in the form of a network graph, are shown in Figure 2. Higher values mean a strong expression of a factor whereas a low value is indicating a weak expression of the factor. The expression is done in relation to other subjects in the sample. So, it is mostly useful for analysis in samples smaller than 10 elements. Lobbying power is referencing towards the possibility to place topics in public discussions and provide groups of interest that force this topic in a certain direction. Experience with similar projects is referring towards work done on the dedicated topic. Organisational Power is indicating the strength of a subject to manage and coordinate tasks. Financial resources are potentially dedicated resources towards the special topic. Staff Power is the dedicated amount of people that can support work on the topic. Professionality is asking for the degree of people who are working on a professional base. This is diverting volunteers from paid staff and working mentality as well. Expertise is asking for the experience and knowledge in an organisation. Public Resonance is focused on the impact of communication of an organisation.

As a result of this stakeholder analysis, the main actors for cybersecurity training will be the cybersecurity trainer and policy makers/governmental initiatives. Cybersecurity Trainers have the highest staff power and policy makers have the highest financial resources. A second option is through hospitals themselves to their health care professionals. The lowest potential type of stakeholders for an active involvement are research organisations (Figure 2).

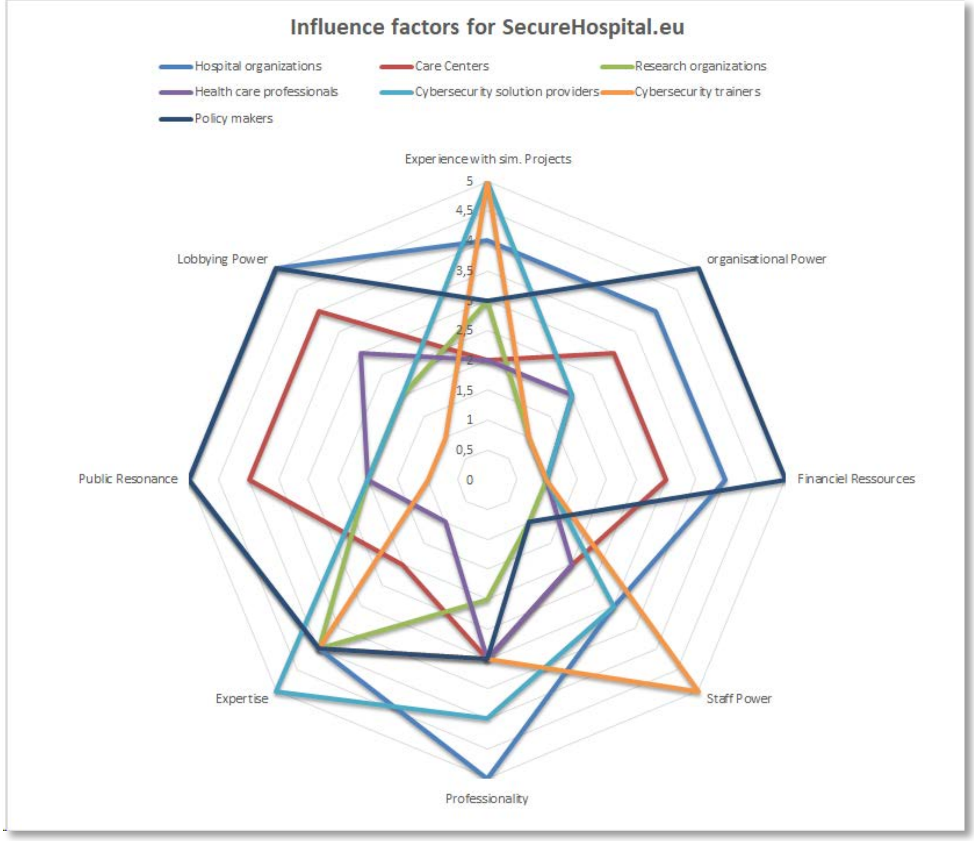
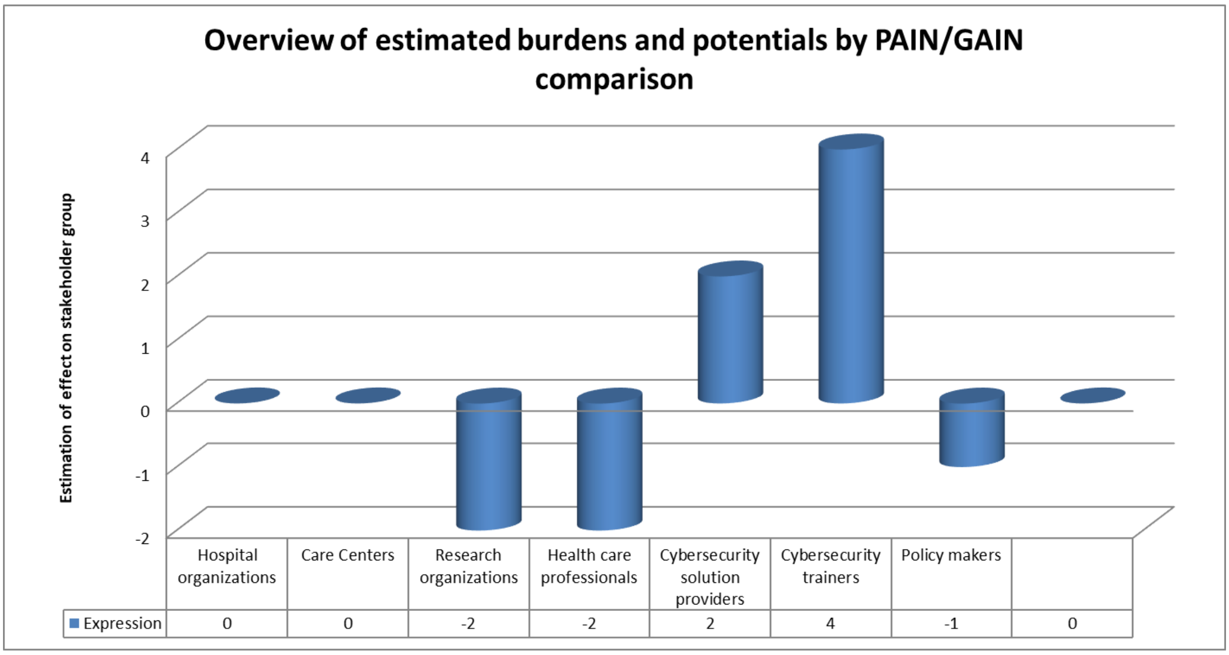


FIGURE 2: Stakeholder analysis Influence factors

An additional approach for identifying potential influence for getting involved in the project trainings to the stakeholder groups is a pain/gain analysis. This provides an overview of potentials benefits and losses of stakeholder groups, which shows the chance for an active contribution.



	Hospital organizations	Care Centers	Research organizations	Health care professionals	Cybersecurity solution providers	Cybersecurity trainers	Policy makers	
■ Expression	0	0	-2	-2	2	4	-1	0

FIGURE 3: Pain/Gain analysis. Negative Values estimate potential risks

Figure 3 shows a calculation of Pain and Gain estimation on the outcomes of the project for the stakeholder groups. Negative results show predominantly pains for the stakeholder. Positive values demonstrate predominantly gains by the project outcomes. The group of stakeholders that would benefit the most from the SecureHospital.eu project would be the group of cybersecurity trainers, followed by the cybersecurity solution providers. Policy makers, healthcare professionals and research organizations have a potential for negative effects. Negative effect is meant as a potential burden. This groups have to invest more action and resources than their direct benefit would be. This is because of the increased responsibilities in parallel with limited competences to react on special occasions. This needs to be reflected in the communication with these groups. Their potential return of investment is based on a long-term perspective over some years and a decreased risk factor for security breaches and an increased trust by patients. But therefor, some initial burdens have to be crossed. This is a core of successful communication towards these target groups: Direct solutions to their “PAINS” and long-term perspective for their “GAINS”. Hospitals and care centres are neutral in the relation of benefit/cost ratio at this time.

4. Results of Group Discussion

As part of the SecureHospitals.eu' Kick-Off Meeting, the identification of steps to implement the DoA were initiated by INSP. Through this initial task in WP5, we were able to gather input from all partners and provide a project perspective on the situation of field access for 'recruiting' training participants.

These elements were discussed according to their interrelations and connections between different levels of stakeholder and user groups. The final form, as shown in Figure 5, shows the results with different channel approaches. Arrows mark the way of the communication flow and show influence directions.

A channel was defined as a way to transfer information from one layer to another and within a layer.

As the communication flow is strongest at the Management board of a healthcare facility, this is a good vector to advance with contacting organisations.

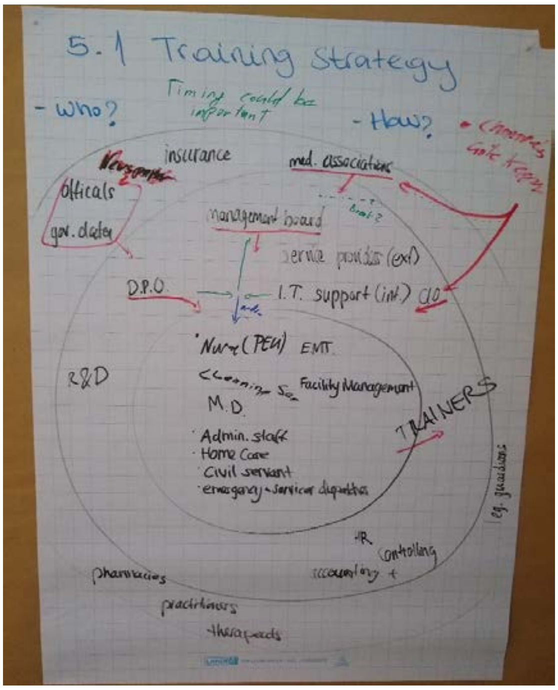


FIGURE 4: Workshop flipchart from kick off meeting

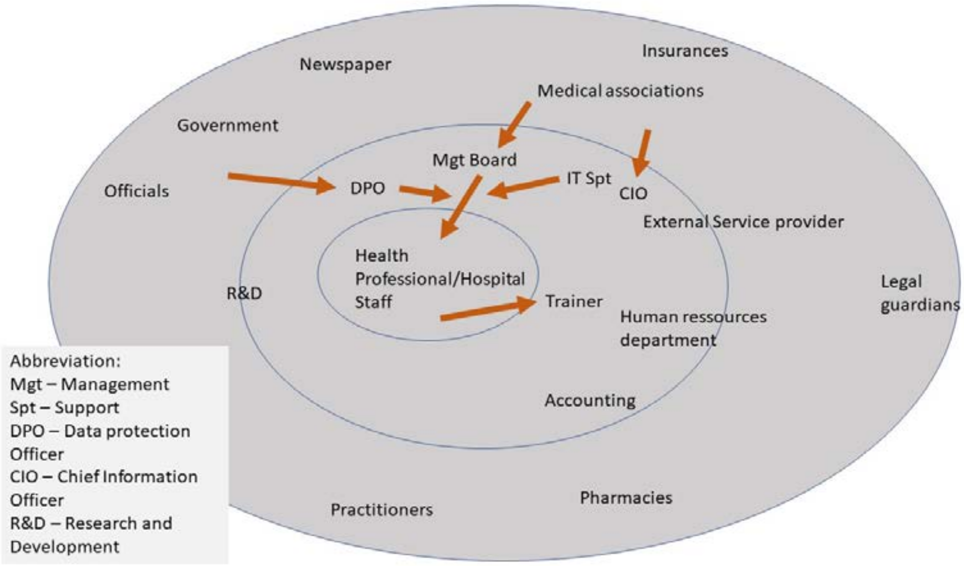


FIGURE 5: Overview of channel routes through stakeholder dimensions

These results reflect findings from the stakeholder analysis (Annex 1, Chap. 3 in this report). A strong link between hospitals and policy makers is pushing towards the primary end-user (PEU). The primary end-user (PEU) is deflecting the pressure towards the trainer for cybersecurity. The channels used for this are regulations towards the PEU, which then tries to withstand or adapt to the situation with the request to a trainer.

5. Roadmap for communication

The roadmap for communication is an overview of the timing for communication and when-to-address-whom within the stakeholder groups for training. Two parts describe this timing and explain mechanisms in project communication and utilitarian communication. A third section presents a table with upcoming conferences where the project partners can meet trainers and solution providers.

5.1 Interpunction of communication

The directions of communication flows could be identified – towards the PEU and from PEU away (Fig. 5). In analogy to a black box model, a direct influence and control of the information-flow is not possible. But the INPUT-signal must follow the way through policy makers and hospital management. This is a controllable information vector to those two stakeholder groups. This input will produce a stimulus to the primary end-users (PEU) that will react in an OUTPUT-signal towards trainers and back to the management. The output towards the trainers is producing a demand at this point that can be solved by SecureHospitals.eu finally. The communication idea is to produce request and demand and catch at close to the zero- points of a Sinus-wave like timing (Figure 6). This is based on the idea of Interpunction of interaction and communication (Willemse & Ameln, 2018). Interpunction is the point where a communication process is taken up or entered by a party on an already existing flow of communication.

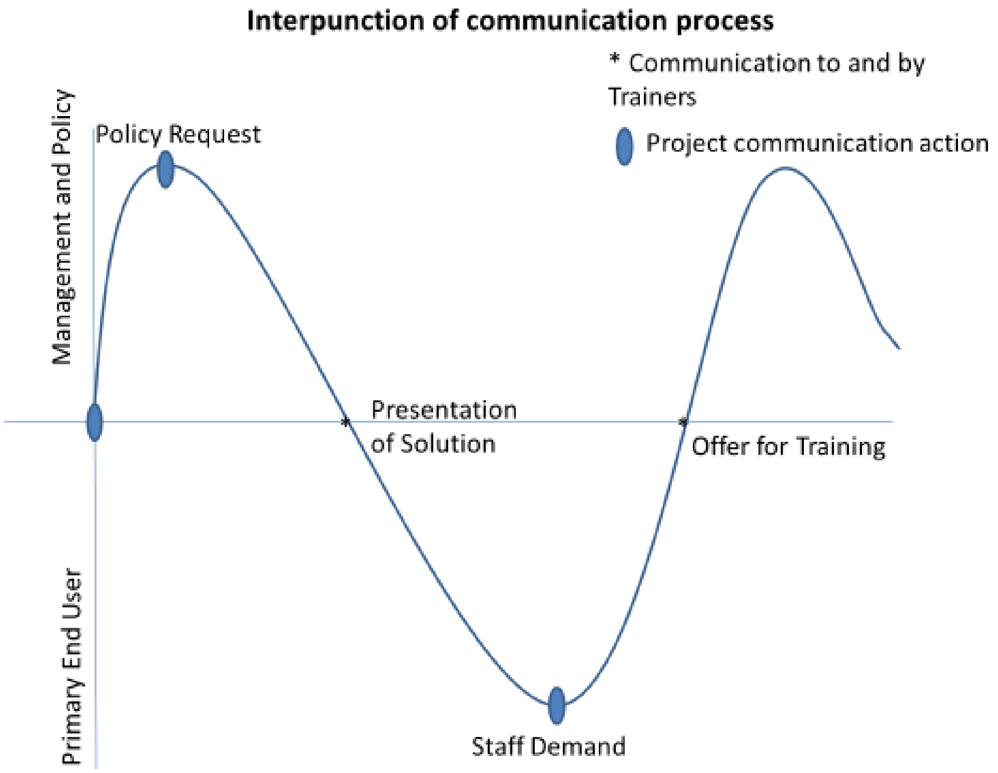


FIGURE 6: Interpunction of communication for SecureHospitals.eu

Primary stimulus

For the initial stimulus, the best option is to have a real case portrayed in a media campaign as headliner material. This concept is described in general for media campaigns in warfare and globalization of communication streams (McLuhan, Fiore, & Agel, 1968). Another stimulus could be a change in legislation. For the topic of cybersecurity, this change in legislation could be the GDPR of the European Union. This is already a topic with a lot of training activities and offers. So, the main build-up process of the topic (first peak of the wave) is reached already. By this, it is an option to address the trainers for a train-the-trainer concept instantly and use the flow of GDPR issues to support the topic of cybersecurity. This allows a cheap and effective free-rider strategy. Realistically this would need to be done within a timeframe of 18 months after the initiation of the GDPR (since 25.05.2018). That would fit the scope of the project if the main product would be ready until project month M12. Otherwise the free-ride effect would not be strong enough to carry the topic forward.

5.2 Information Process

For a realisation of this idea, it is necessary to address the target groups of communication with appropriate information material. First with “awareness raising” at the level of policy makers and hospitals. Then with the cybersecurity trainers to start a train-the-trainer concept, followed by activities to support the trainers with information material, like folder or info-mails, for hospital staff through training agencies, in order to provide a solution for hospital staff and their demand on training for cybersecurity.

Awareness for the promotion of the SecureHospitals.eu project could be raised with an information campaign. This campaign shall consist of:

1. Hackathon – get into the health record system together with Policy Makers (awareness for SecureHospitals.eu)
2. Information of Trainers and sign-up process (incl. promotion of Summer School)
3. Promoting the idea of SecureHospitlas.eu towards PEU (incl. promotion of MOOC participation)
4. Support trainers in bid management (incl. promotion of local workshops and international exchange)

For the region of Austria as a practical example, cooperation partners for each stage would be:

1. AWS (Austria Wirtschafts Service) (Chamber of Economics)
2. WIFI (Wirtschaftsförderungsinstitut) (Education Institute/Trainer Community)
3. KAV (Wiener Krankenanstaltenverbund) (Hospitals)
4. ARS (Akademie für Recht und Steuern) (Training Agency for Professionals)

At this stage, all partners are identifying and collecting local and regional cooperation partners that will be contacted in the later project stages for awareness raising and participation in the project activities.

5.3 Conferences and Events 2019

To increase awareness about SecureHospitals.eu and the upcoming trainings, the authors recommend visiting a large number of conferences and events about cybersecurity and healthcare to network with potential training participants. Adding up to the list of conferences already identified as part of the Description of Action, a list of additional conferences and events of relevance is provided below.

Table 1: Upcoming references and events

Name of Conference	Type of Audience	Potential date and location
Portugal eHealth Summit	eHealth Researchers, Solutions Providers,	March 2019, Lisbon Portugal
IDIMT	Management, hospital staff, researchers	September 2019 in Kutna Hora
Cyber Security and Cloud EXPO	Management, Solution Providers, Trainers	June 2019 in Amsterdam
9th annual European Data protection and privacy conference	Solution providers, researchers, management	March 2019 in Brussels
Cyber Security Tech Summit Europe	Solution Providers, Trainers, management	March 2019 in Bonn
Vienna Cyber Security Week 2019	Trainers, Solution Providers, Researchers	March 2019 in Vienna
Security Summit 2019	Management, Trainers, Solution Providers	Mai 2019 in Vienna
Information Security in Healthcare Conference 2019	Health Care Staff, Policy makers, Solution Providers, Trainers	June 2019 in Cham
Cyber Security Exchange in Healthcare 2019	Health Care Staff, Policy makers, Solution Provider, Trainers	May 2019 in Dallas
InfoSec Healthcare Connect	Management, Health Care Staff, Policy makers, Solution Providers, Trainers	August 2019 in Fort Lauderdale
Healthcare Cybersecurity	Health Care Staff, Policy makers, Solution Providers, Trainers, Management	January 2020 in Manchester

6. Conclusion

6.1 Key channels

The main communication channel for trainers as well as PEU is through eMail. Nevertheless, this is not suitable at this point of the project because there is no repository of contacts available. During the first phase of the project, the partners of SecureHospital.eu are collecting contacts of several stakeholders. This is a first chance to enter the communication process.

Secondly, a newsletter system where trainers and PEU can sign up has been created and will be continuously promoted through the social media channels.

Table 1 shows and overview on of identified means of contact for each of the stakeholder groups.

Table 2: Means of Contact

	Hospitals	Trainer	Solution Provider
Contact	CEO, CIO, DPO	directly	CEO
Channel	eMail, personal contact	eMail	eMail, personal contact
Materials for first direct contact	Info folder	Info folder, Training guides	Info folder, training guides

6.2 Key contacts

Key contacts at this stage are training providers because of the instantly increased reach. For a second step, trainers, PEU and hospital management will be addressed directly. The mentioned contact lists of the consortium will support this.

As mentioned also in D2.1, the contact repository and contacting process that involve personal data the collecting of which is crucial for the implementation of the Description of Action, is regulated among the consortium through an agreement that ensures safety and confidentiality of data complying with the GDPR standards. All contacted persons and organisations will be informed about the means of processing and storing their contact data.

Reaching out to additional contacts

At this stage, it is necessary to understand that this is a situational report after three months of project runtime. Along the runtime of the project, more contacts will be available. Already at the early months of 2019, events like the eHealth Summit in Portugal, the Cybersecurity summit in Germany, the Security Summit in Brussels etc. will be addressed. At these events, leaflets of the project, provided by INSP, will be spread to potential stakeholders like training organisations, solution providers, hospital entities etc.

There is the expectation that these contacts will be more reliable in the further process than those, found by desk research because of a direct personal contact. That should increase the available contacts and will be a pillar for the contacting structure in the upcoming project period.

6.3 Next steps

In Task 5.2 of SecureHospitals.eu training promotional material is going to be created by EUR together with INSP, COOS and EAN. This material will use this deliverable as orientation for communication towards target groups and use the collected projects and contacts to distribute the material further for supporting the training activities.

Based on this deliverable, also the upcoming iteration of the training strategy (D5.3) will address the identified stakeholders in 'need for training' and provide a master plan for tailoring training packages based on the different types of needs.

7. References

McLuhan, M., Fiore, Q., & Agel, J. (1968). War and Peace in the Global Village. Abgerufen am 25. 2 2019 von https://amazon.com/peace-global-village-marshall-mcluhan/dp/1584230746

Osterwalder, A., & Pigneur, Y. (2010). Business model generation: a handbook for visionaries, game changers, and challengers. John Wiley & Sons.

Willemse, J., & Ameln, F. v. (2018). Die Interpunktion von Interaktion und Kommunikation. Abgerufen am 25. 2 2019 von https://link.springer.com/chapter/10.1007/978-3-662-56645-9_8

Annex 1

The tables in Annex 1 are providing the data of the stakeholder analysis in a score format. The range of scores in all schemes was a scale between 1 and 5. Its purpose is to provide a fast overview of the stakeholder positions by expert's opinion. For this, three expert interviews were done and computed average scores were used for the final table. Higher scores express a stronger, more powerful position on the related item.

Short info on expert sample:

- 1 Technical Director of Hospital in Vienna
- 1 System architect of insurance group
- 1 Microsoft Chief Security certified System Administrator of an international Bank and advisor for security systems in health care

STAKEHOLDERS	EXPERIENCE WITH SIM. PROJECTS	ORGANISATIONAL POWER	FINANCIAL RESSOURCES	STAFF POWER	PROFESSIONALITY	EXPERTISE	PUBLIC RESONANCE	LOBBYING POWER
HOSPITAL ORGANIZATIONS	4	4	4	3	5	4	5	5
CARE CENTERS	2	3	3	2	3	2	4	4
RESEARCH ORGANIZATIONS	3	1	1	1	2	4	2	2
HEALTH CARE PROFESSIONALS	2	2	1	2	3	1	2	3
CYBERSECURITY SOLUTION PROVIDERS	5	2	1	3	4	5	2	2
CYBERSECURITY TRAINERS	5	1	1	5	3	4	1	1
POLICY MAKERS	3	5	5	1	3	4	5	5
STAKEHOLDER	Gain	Pain						
HOSPITAL ORGANIZATIONS	5	5						
CARE CENTERS	4	4						
RESEARCH ORGANIZATIONS	2	4						
HEALTH CARE PROFESSIONALS	2	4						
CYBERSECURITY SOLUTION PROVIDERS	5	3						
CYBERSECURITY TRAINERS	5	1						
POLICY MAKERS	4	5						
STAKEHOLDER	Strength	Weakness	Opportunity	Threat	Risk factor			
HOSPITAL ORGANIZATIONS	4	5	3	5	4			

CARE CENTERS	3	5	3	2	3			
RESEARCH ORGANIZATIONS	2	4	3	2	3			
HEALTH CARE PROFESSIONALS	2	4	2	5	3			
CYBERSECURITY SOLUTION PROVIDERS	5	3	5	3	4			
CYBERSECURITY TRAINERS	5	1	5	2	3			
POLICY MAKERS	3	4	3	5	4			