SECUREHOSPITALS.EU

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

D4.2 Trainer Interviews Report

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 Universiteit Rotterdam**, Netherlands (EUR) **TIMELEX**, Belgium (TLX) **Fundacion 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:	**D4.2**
Title:	**Trainer Interviews Report**
Lead beneficiary:	**EUR**
Work package:	WP4
Dissemination level:	PU
Type	Report
Due date:	31.07.2019
Submission date:	07.08.2019

Authors:	**Tessa Oomen,** EUR **Jason Pridmore**, EUR
Contributors:	INSP, TLX, FPHAG, SAM, JOIN, EAN
Reviewers:	**Marco Antomarini**, COOSS

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

One of the objectives of the SecureHospitals.eu project is to develop new education materials, curricula, and innovative ways of promoting cybersecurity training and education. This report presents the outcomes of stakeholder engagement in the form of in person interviews, and it analyses both the training needs and the quality criteria required for training on cybersecurity in healthcare organisations in the European context.

By means of semi-structured interviews we engaged trainers and those involved in cybersecurity training in healthcare and explored their experiences. Semi-structured interviews were helpful in guiding the interview along the necessary topics, while allowing for flexibility to explore topics more extensively. Interviewees were selected on the basis of their expertise and current position. In total, 19 respondents were interviewed. Each interview was recorded and transcribed for analysis purposes.

Thematic analysis was applied to the interview transcripts. This method helped to identify central themes and the nuances, contradictions and contrasts within each theme. After completing the analysis, the themes and underlying codes were structured into a narrative.

We found that trainers operate in a high pressure context that is made up of 1) complex organisations with interlinked processes and limited resources, 2) proliferation of new technologies and medical data in which security is a secondary aspect, 3) a heterogeneous target audience faced with high workload and limited time, and 4) a complex topic that can be intellectually challenging as well as emotionally draining for trainees.

The following points were found to be actionable results for the SecureHospitals.eu project to focus on and to take into consideration when developing new training approaches and materials:

- Trainers for which cybersecurity training is only a small part of their overall workload are in most need of support
- Increase accessibility to usable materials and include fundamental knowledge in understandable language
- Maintain a flexible approach for integration and adaptation as well as training that addresses a heterogeneous audience
- Focus on relevant examples
- Increase recognition of cybersecurity as a complex set of issues that requires a holistic approach and make this a part of training initiatives
- Create workable understandings and responses to legislation and compliance issues
- Share trainer experiences with new process and technology implementation
- Expand a sense of ownership and participation in cybersecurity practices
- Recognize and respond to the role and impact of emotional responses to all training related to technology

Furthermore, our interviews provided insight into opportunities for the European Union to invest in, in order to support and promote cybersecurity in healthcare across Europe.

- Promote cybersecurity as part of proper patient care culture
- Stimulate and support cooperation on cybersecurity improvement in healthcare in the EU
- Boost the incorporation of digital skill classes as part of non-IT education programs
- Invest in opportunities and resources for professional training for trainers in the EU
- Provide guidelines and standards for the adoption of new technologies and innovations in healthcare.

1 Introduction

This report describes the promotional materials created at the first stage of WP5 describing At present, education and training on the topic of cybersecurity in healthcare remains limited. Part of the objective of the SecureHospitals.eu project is to develop new education materials, curricula, and innovative ways of promoting cybersecurity training and education. In order to develop relevant and quality materials, Task 4.2 of the project is designed to draw upon the knowledge, experiences and perspectives of current cybersecurity trainers that connect with or work within healthcare organisations.

In order to learn how cybersecurity knowledge is developed and disseminated within healthcare institutions, partners of the SecureHospitals.eu project consortium engaged in a series of interviews with key personnel involved in or implementing various forms of cybersecurity training. These interviews focused on discovering what the key training needs were and what sort of requirements these trainers felt was important for the development of future training. Trainers and those who perform related tasks are central to this study, as trainers engage in with both the healthcare organisations and their personnel. The knowledge, experiences and perspectives of trainers will prove valuable for future work of the SecureHospitals.eu project.

This report presents the outcomes of stakeholder engagement in the form of in person interviews, and it analyses both the training needs and quality criteria required for training on cybersecurity in healthcare organisations in the European context. The trainer and relevant experts' feedback enables the creation of powerful materials for training as well as the definition of quality criteria that will be dealt with in upcoming tasks for this project. Additionally, their input will help create understanding of the existing needs, the potential barriers and opportunities for cybersecurity training.

1.1. Link to other work packages

This task has close links with previously completed work and future work of the SecureHospitals.eu project.

- **WP 2 - INVOLVE:** The collection of relevant stakeholders and engagement strategy laid first ground in connecting with interviewees.
- **WP 3 - AGGREGATE:** This report adds to the collection of existing knowledge and approaches to cybersecurity in healthcare.
- **WP 4 - CREATE:** This report is part of WP 4 and provides input for the new material, curricula and innovative training material that is to be created as part of the SecureHospitals.eu project.
- **WP 5 - BOOST:** This report provides input for new training material that will be created as part of this project.
- **WP 6 - COMMUNICATE:** Connecting with trainers, hospitals and care organisations has provided the opportunity to introduce the SecureHospitals.eu project to relevant stakeholders and to create a larger professional network.

1.2. Structure of the report

The structure of the report is as follows. In chapter 2, the methodology for the interviews and analysis is presented. It explains the choice for using semi-structured interviews and applying thematic analysis. Chapter 3 contains the results of the analysis, focusing on trainer profiles, the challenges trainers face, the context that trainers work within, the methods trainers use and the responses they receive from training participants. It also contains a list of suggested content and communication about cybersecurity. Chapter 4 consists of the conclusion and describes policy recommendations for the European Union.

2 Methodology

The core objective of Task 4.2 is to determine quality criteria for materials to be developed as part of the SecureHospitals.eu project. Additionally, we aim to create understanding of the existing needs, the potential barriers and opportunities for cybersecurity training. To this end, it is necessary to engage with trainers regarding their training processes and practices for cybersecurity in healthcare settings. These persons are key experts that are actively working within the field and the type of persons that this project seeks to work alongside and support as a coordination and support action.

2.1 Semi-structured interviews

Qualitative methods are best for in-depth exploration into the knowledge, experiences and perspectives of trainers. For the purpose of this task, semi-structured interviews were selected as the most appropriate method to complete this task. Semi-structured interviews are helpful in two ways. First, predetermined questions on relevant topics helped guide our interviews, ensuring that key issues and relevant topics were addressed. Second, this method allows for further exploration of topics that are brought up by the interviewee. As an added benefit, the ability to diverge from the selected questions ensures the interview flow as a natural conversation (Boeije, 2014).

The questions for this study were designed to be open-ended, and included follow-up questions where applicable. Overarching topics for the interview questions are questions about 1) the trainer and his or her role in the organisation; 2) experience and knowledge transfer; 3) training practices and materials; 4) personal orientation to work; 5) participant profile and motivations; and 6) experiences with participants. The interview guide encompassing the questions for this study are presented in appendix I.

The interviews were recorded using a recording device and then transcribed. Some partners transcribed manually, while others used an automatic transcription service.

2.2 Interviewee selection

The group of respondents consists of 19 persons. Each respondent is involved in training related to cybersecurity, information security and/or privacy within the context of healthcare. The respondents were approached via the professional networks of the SecureHospitals.eu consortium partners. Additionally, organisations found through the development of previous deliverables (see D2.1 on stakeholder engagement and D4.1 on course collection of this project) were contacted to request their participation in this task. The final selection of participants occurred on the basis of their expertise and their role within the organisation they work for. The list of pseudonyms and profiles can be found in appendix II.

In total, nineteen interviews were conducted by the consortium partners. Interviews lasted between 30 and 75 minutes. For each interview, a verbatim transcript was made for the purpose of analysis.

2.3 Thematic analysis

In order to fully explore the relevant themes that were addressed in the interviews, a thematic analysis was applied. In the words of Braun and Clarke (2006, p.79): “Thematic analysis is a method for identifying, analysing and reporting patterns (themes) within data.” Themes are found by allocating codes to the data (transcript) and finding commonalities. The analysis will be data-driven (Braun & Clarke, 2006).

A code is a word or short phrase that portrays the meaning or salience of a section of text. The code can consist of language used by the interviewee or a descriptor. A theme describes important aspects of the data in relation to the research question. Ideally, a theme presents itself in multiple transcripts, but the frequency of a code does necessarily determine the significance of the theme.

The following iterative steps were followed for the analysis:

1. Reading the transcripts and noting down initial ideas.
2. Allocating codes to sections in the transcripts.
3. Merging codes that are similar or related into larger categories. These are the initial themes.
4. Re-reading transcripts and adding, removing or adjusting codes.
5. Revision of and improving the themes. Definitions for each theme are developed based on context. In this phase, we paid particular attention to nuances, contradictions and contrasts that exist in our interviews.
6. A selection of key quotes that are illustrative of a theme or code were collected.

After completing the analysis, the themes and underlying codes are structured into a narrative. Key quotes are used to illustrate the findings and to provide deeper insight into the experiences of trainers.

3 Results

The results are divided into five sections. First, the characteristics of trainers and their backgrounds are discussed. Second, relevant contextual factors for trainers are addressed. Third, the challenges trainers face are described. Fourth, the training process and strategies, content and responses of trainees are presented. Key quotes from the interviews are used to illustrate and contextualise these results. The fifth and final section includes a list of suggested content and approaches that were brought up by interviewees.

3.1 Who are cybersecurity trainers in healthcare?

3.1.1 Trainer profiles

Trainers are primarily specialised in (one of) the following four topics: 1) technical security; 2) law and regulations, 3) security awareness and human behaviour; or 4) education and didactics. However, trainers usually master each of these four to a certain degree or collaborate with experts specialised on other topics, because they intersect and relate in many ways.

> *"I work here as an education specialist. I embed my expertise with the knowledge and experience of the information security expert, our clients' experiences, and expertise of our multimedia specialists."* Barbara*, education specialist for a security awareness (online) training organisation in Northern Europe.*

Trainers can be specialised in the content or on how to effectively engage with students and/or affect behaviour change. However, both areas are important to be an effective trainer.

Trainers received formal education and professional development is supplemented with self-study, learning on the job, and classes or peer interaction, among others. Interviewees usually went through traditional education programs, such as vocational education or university programs, in their respective fields. They remain up to date with new developments through self-study, by learning on the job, through contact with other professionals or by following additional courses or trainings - often obtaining additional certificates in the process.

Training is often only a (small) part of trainer responsibilities. Cybersecurity training within healthcare organisations is not necessarily conducted by full-time trainers. Many of the trainers are employed by one or more healthcare organisation.

> *"Usually you have people who are responsible for certain tasks in their daily work who provide training. For instance, someone who is responsible for data management in the hospital will teach courses on data management to other staff members."* Chris*, clinical researcher for a major academic hospital in Northern Europe.*

More often than not, trainers are specialised in the content they teach, meaning that trainee engagement is a secondary specialisation. Only a few of the trainers that were interviewed had a background in education or didactics. This may be a key weakness that can be in part addressed by this project.

If trainers are internal to the healthcare organisation, they usually provide specialised training. Within that organisation they fulfil a role that can focus on (cyber) security in general, on privacy, data protection, or other relevant topics. This may have the added value of incorporating organisation-specific experiences.

> *"You teach the dos and don'ts – and you make it real by giving real life use case examples. And if you know the company very well you can you can give examples from the company."* Liam*, security expert and trainer active in Northern Europe*

Trainers who know the organisation they train for, whether they are an employee or a knowledgeable external person that has experience with that company, are able to relate to the experiences of the group they train, which Liam experienced before.

The advantage of having 'in-house' trainers is that they have in-depth knowledge of the organisation and they are specialists on the topic they train in. However, training schedules depend on demand, and some specific trainings are only given once or twice per year. This irregular schedule comes at the cost of getting into a routine, especially because trainers often have other responsibilities to tend to, which can cost trainers time and effort when preparing a new round of training.

> *"The course is not taught on a regular basis, and this can interrupt you in your daily tasks. You have to prepare for it, set up presentations, and find interesting exercises. But you don't get a real routine, which is a disadvantage."* Edward*, clinical IT specialist and data management support for a major academic hospital in Northern Europe.*

As Edward states, training is often not the core activity of trainers. This could lead trainers to consider training as a burden and as a limitation to the time they have for their primary tasks.

External trainers usually work as consultants, either as part of an organisation or self-employed. Similar to internal trainers, training or implementing security awareness programs is often only a part of a larger innovation or security project. External trainers are more likely to be part of the design and implementation of such projects, while internal trainers are more likely to have a smaller role in these. However, some external trainers or organisations are specialised in a specific service, such as design of information security education programs.

3.1.2 Trainer motivations

Most trainers have a high interest in cybersecurity from the start or they develop this in their job. Our interviewees suggested that this passion is a necessary driving factor, and that this quickly intersects with their personal lives and affects their potentials for future jobs.

> *"I think that everybody who works here developed the passion to work in the field of security awareness. It either is your passion or it becomes your passion. The topic is highly motivating."* Barbara

As Barbara sees this as a highly motivating topic, this possibly serves as counterbalance to the risk of having training as just one of many responsibilities most trainers have. For many interviewees, the intrinsic reward of being able to at least partially work on this dynamic topic made the opportunities to train others in this area one of their more engaging responsibilities.

Furthermore, a higher level of passion is needed as a security professional to push developments within the healthcare organisation. Organisational complexity, lack of resources, and other barriers may hinder the implementation of cybersecurity measures, as will be mentioned below.

> *"If we would give up, it would stagnate. You have to keep it up with this topic and be relentless. If not this year, then the next."* Frank*, Information Security Officer CISM and DPO at a hospital in Northern Europe.*

> *"And, then again, a local security officer says 'I am capable, I am going to do this for my whole theme', another says 'I only have this little role. I distribute to the manager, and the manager of the several departments within my theme has to do it in their own and distribute it'."* Albert*, CISO of an academic hospital in Northern Europe*

These quotes indicate how both Frank and Albert have seen differences in results depending on who drives forward the training and knowledge about cybersecurity. Those that are more engaged and passionate about cybersecurity issues are generally more effective than those who lack this intensity.

This passion also supports trainers in their professional development. **Trainers often have intrinsic motivation and drive to stay up to date with developments in the field of cybersecurity and awareness.** It does not appear to be common for the healthcare organisation to push (in-house) trainers to do additional training, but organisations often do support requests to participate in professional development activities. For those who work in (technical) security, certificates are still relatively common.

> *"The hospital doesn't arrange further education or development opportunities, but if we have a request, they support and honour it. I did some security trainings in my previous workplace, and my colleagues and I do have certificates."* Frank

As experienced by Frank, healthcare organisations generally do not offer opportunities for professional development, but at the same time, employers do support those who wish to enrich their knowledge and experience. The risk is that only the trainers who are driven actively search for these types of opportunities, increasing the possible divide in effectiveness with trainers who are less passionate about their work.

Trainers are motivated to teach healthcare staff about cybersecurity, a topic that is often overlooked. Trainers consider cybersecurity and information security as crucial topics for healthcare workers and like facilitating learning in healthcare staff. Motivating training participants can be challenging factor which adds or detracts from the enjoyment trainers take of their work.

> *"My role is to bring them a topic that they would not [necessarily] touch by themselves. I have to be a surprise for them. Otherwise they would not listen to me and I would not like to spend a full day with them as well. This is where I get a bit more of an immaterial payoff."* Tim*, system architect and trainer in Central Europe*

> *"What motivates me to do this job is that information security is not really on your mind if you have never heard of it, but at the same time it is a very important topic."* Barbara

Trainers consider cybersecurity and information security as crucial topics that their target audiences are largely unaware. This immaterial payoff that Tim suggests shows that trainers enjoy bringing about a change in their target audiences – however this requires that trainees are willing to actively engage in the training process.

Trainers gather feedback to improve the content and strategy, and their own performance. This feedback can be gathered through, among others, formalised evaluation processes, through informal approaches, and by gauging responses from trainees or management. In general, trainers state that positive feedback reinforces their passion to work on cybersecurity training in healthcare.

> *"When you get feedback from a client, saying that they notice their employees apply what they learned to their daily work, it always makes me happy."* Barbara

The feedback from training audiences and clients affect the enjoyment trainers take from their work. As Tim mentioned previously, direct feedback from training audience affects his personal enjoyment of the training. The experience for those who develop e-learning training programmes is invariably different given that they do not directly engage their target audience. In these contexts, feedback is still gathered from trainees, but occurs indirectly through the client organisation.

3.2 What are the contexts trainers work within?

3.2.1 Cybersecurity in healthcare organisations

Cybersecurity is increasingly important for healthcare organisations. Especially with the rise in adoption of various digital applications and services in this sector, the risks for healthcare organisations are rising.

> *"Information security is important for any organisation; data is used everywhere. But in healthcare they work with more sensitive personal data than other organisations."* Barbara

> *"The Internet of Things phenomenon enters medical technologies – many medical appliances can read our data, save them, send over internet into all kinds of cloud storage."* Alex*, trainer and Data Privacy Officer for multiple organisations in various sectors in Central Europe*

> *"I think when you get higher in the management chain, the priority for cybersecurity and information security rises. If you, as an organisation, have a data leak, you always end up looking badly, also in the public eye."* Chris

The ubiquity of the highly valued data from healthcare heightens the risks healthcare organisations face from cybersecurity incidents. The multitude of consequences, ranging from financial loss to reputation damage, can have long lasting effects those active in the healthcare sector.

Medical data is considered to be highly valuable, and the motivations and actors behind obtaining this category of data are diverse. Even just a few medical files can provide those with ill intent the ability to commit identity fraud, and larger datasets can be used by commercial organisations to gain profit through falsified documentation, insurance pay-outs and more. However, there is still much to be learned about how and why medical data can be seen as valuable.

> *"It is relatively opaque because no one has a clear idea of why these things are sold with so much value."* Gino*, cybersecurity expert and lecturer in Southern Europe*

> *"A medical file does not just contain medical data, but also social security numbers, birth dates, and sometimes payment information. I think it's easy to commit identity theft and fraud when you get your hands on medical files. Also, insurance companies and organisations specialised in medical analytics want to gain access to this information, which is difficult or impossible to come by via the normal and regulated routes."* Gemma

This mixture of both access for direct financial gain and analytical value makes the financial implications of cybersecurity issues in healthcare more pressing. Understanding the motivations for obtaining medical data and the actors involved can provide insight into relevant actions to undertake to increase and maintain cybersecurity in healthcare.

3.2.2 Cybersecurity mosaic

Cybersecurity can be conceived of as a mosaic, something that consists of many parts that together make up the whole. This analogy, raised by one of our interviewees is indicative of how cybersecurity entails, among other things, technical, legal, behavioural and physical aspects. An issue on one or more of these aspects can significantly damage or break the cybersecurity chains. This can range from implementing a program that raises vulnerabilities to human errors that subsequently provide access to hackers. This mosaic view widely supported by our interviewees.

> *"I do not want to generalize but in everyday work and regular staff it is all about detail – lock, log out, do not send, do not forward to everyone, verify. Details which, when put together, create a mosaic of cybersecurity and securing data in general."* Robin*, trainer cybersecurity in multiple sectors in Central Europe*

> *"Constructing a security system is very important and it is the exercise of many actors. Everyone has to do their part, but breaking it is very easy. If only one actor breaks one of those steps in the chain and it will bring down the whole castle."* Sophia*, Professor in technical cybersecurity in Southern Europe.*

> *"It's not just the cyber part or the aspect of access to personal data, but physical security is also important for information security. Cleaning staff has access to all areas, and they have to remember to close rooms after their work, [but should] not browse through people's files or personal belongings."* Barbara

This mosaic view puts pressure on trainers to respond to a variety of aspects related to cybersecurity within healthcare. The ways and depth in which processes are interlinked with cybersecurity can complicate the ability to isolate the different factors (for the purpose of training and beyond) when a cybersecurity issue occurs.

The human factor is invariably seen as a critical risk to the cybersecurity chain. This does not mean that humans are always to blame. Rather, the methods of cybercriminals become more and more refined and processes to infiltrate or disrupt security practices become increasingly sophisticated. For instance, phishing attempts become more believable and people are unable to recognise the difference between honest and official requites and those that are done on the part of hackers.

> *"In our experience most of the data breaches and the consequences are of personal behaviour."* Albert

> *"You can't always stay ahead. They find new tricks and they become increasingly professional looking, so people are easily fooled."* Frank

> *"And you know it's a scam, but there is that little voice that says: but what if it is? Your conscience can get in the way."* Gemma

Cybersecurity has become an ongoing process of dealing with present and staying ahead of future cybersecurity issues. This requires an intention by organisations to continually adapt, develop, and improve their response process and engage their employees effectively. In order to succeed in this, trainers need to understand and train their audiences in recognising how the human factor is targeted and exploited.

The risks of cloud services and third party suppliers can be unclear for healthcare organisations. Knowing the details of potential risks is not always possible, due to the sheer amount of services, devices and applications that exist within healthcare settings. However, this does not need to be a problem by default. The awareness of potential risks and critical thinking by employees then becomes increasingly necessary in multiple contexts.

> *"That risks exist is not necessarily the problem, as long as we are aware of them and take basic measures to prevent them from happening. For example, the cloud is a bit of a blind spot. You can't tell from the outside what kind of solution it is, or whether it is designed according to the 'privacy by design' principle. If a doctor has a private account with a cloud service and uploads a dataset with traceable data, we wouldn't know about it. So, it is important that staff members are aware and ask themselves whether they should do it or not."* Frank

> *"Third party services can be a risk. You need a data processing agreement. What are the agreements with the external processing party for your data, both processing and storage?"* Frank

It seems that healthcare organisations struggle to maintain control over the cybersecurity chain, as services and processes can fall outside of their direct supervision. Trainers can support healthcare organisations by enabling staff to make critical assessments about their actions, without having to go into detail about the multitude of risks for each services.

Current strategies for improving cybersecurity remain superficial and do not always focus on addressing core issues. Some trainers consider the current methods and interventions not adequate for increasing cybersecurity in healthcare.

> *"But what I see in my daily routines and in the system design, cybersecurity is still something that is just touched on the upper part. The real vulnerable issues are something deeper in the cores."* Tim

As Tim suggests, most cybersecurity issues are not addressed at the root. As such, new training solutions should strive to reach long term and sustainable effects. These are the issues that the SecureHospitals.eu project can begin to raise and resolve, although more depth requires greater investments from those involved.

3.2.3 Regulatory compliance and GDPR hysteria

Healthcare organisations have to organise cybersecurity and privacy related processes in compliance with EU wide and/or national standards. The General Data Protection Regulation is an EU wide regulation for data privacy that came into effect in May 2018. For example, ISO/IEC 27001 is an internationally acknowledged standard for information security management systems. The NEN 7510 is the Dutch standard for information security in healthcare.

> *"It is not legally required to be certified for a certain norm or standard, but organisations are legally required to use and apply the norm or standard to their systems."* Gemma

The regulations and standards support the design of processes that pertain to the collection, processing, and storing of data. Trainers should be aware of the regulations and standards that apply to the healthcare sector, and that there is a difference between being compliant to the standard and having the certification.

Regulations and standards do not always provide clear requirements for healthcare organisations to assess which security measures are in compliance. This can create uncertainty about how to develop and address cybersecurity within organisations.

> *"The norms are not detailed enough. You only know which topics you have to address, not how you should address them. This is something you have to find out for yourself. This is where risk analysis comes into play. You analyse the areas that carry the most risk and act based on that."* Frank

Based on Frank's statement, variations in security chains among healthcare organisations may exist because the standards do not provide detailed guidance on how to comply. Furthermore, it is likely that each organisation's risk assessment may lead to different outcomes and thus different solutions.

The GDPR caused unwarranted hysteria. In the period before and just after the GDPR came into effect, trainers report that there was a lot of unrest surrounding the new EU regulation.

> *"Awareness around personal data has increased [due to the GDPR] and more interests are involved, because the consequences [of incidents] are much more severe. In essence, nothing has changed between ten years ago and now, if you leak patient data. It has always been problematic, but now there are larger consequences in the sense of fines, the obligation to report, reputation damage, and many more."* Barbara

> *"It is worth mentioning that the campaign started only two years after the regulation was approved. So, a month before the regulation became legally binding, it was everywhere, on TV, on the radio and it started all the hysteria. I would say that the people approached it with lots of exaggeration."* Robin

Like Robin, most of our interviewees agreed that the GDPR was met with unnecessary hysteria. Barbara explains that the commotion was unnecessary, because the GDPR did not significantly change the responsibilities of healthcare organisations. However, there are still aspects of the GDPR that can be cause of concern for healthcare providers. Trainers and the SecureHospitals.eu project have a role in supporting EU healthcare organisations in this regard.

In relation to the GDPR, medical data has been the primary concern, while other risks have been overlooked. The second largest source of data for healthcare organisations is personnel files. Many organisations have overlooked the risks attached to secondary processes.

> *"With the GDPR, a lot of attention was brought to medical data. But many organisations have forgotten or underestimated the amount (of sensitive) information they have on their employees, and that HR processes need updating too."* Gemma

In addressing GDPR concerns, Gemma found that many of her clients forgot or did not think to address data sources that do not contain medical or patient data. This is still considered a weak spot in the security chain of many healthcare organisations, which trainers and the SecureHospitals.eu project aim to address.

The GDPR helped set behaviour change in motion, but in some cases this seems to stem more from self-preservation than concern for patient privacy. The potential fines seem to be a stronger motivator than intrinsic factors.

> *"With the arrival of the GDPR you notice a lot more attention is given to information security and privacy."* Frank

> *"What often occurred was taking a picture of your screen and sending it to a fellow doctor asking if they could take a look at it. This no longer happens as often, because the punishment can be significant. It's more that people get punished for wrong behaviour, than that they intrinsically feel that they have to be careful."* Chris

While the GDPR created a momentum for healthcare organisations to check their processes, as Frank states, the incentives were not always constructive. Chris mentions that he has seen changes in colleagues' behaviour, but that these are not intrinsically motivated. During training and awareness interventions, trainers could address this motivation to adopt privacy and security enhancing behaviours.

3.2.4 New processes and technologies

Information security is not a new concept in healthcare, but the related processes have changed. This requires healthcare workers to gain new understanding and skills.

> *"The fact that we want to send information from A to B has not changed. However, the media with which we do, and the grasp we have on those, has. And this requires different knowledge than before."* Gemma

Gemma begins to outline her concern here. She continued by discussing an example of how one might check whether the correct address is used on an envelope when sending a letter. However, compared with so-called 'snail mail', the speed with which emails are sent can be a source of additional problems. Other healthcare practices have changed as a result of new technologies and innovations. If trainers aware how these processes have changed in practice, they can help guide training participants through these developments.

The proliferation and adoption of new technologies seem counterproductive to effective and efficient healthcare. It becomes too difficult for healthcare workers to keep up with innovations. Other new technologies are not yet fully 'mature', or user friendly, and can obstruct healthcare workers in their daily practices.

> *"Sometimes new technologies are just inconvenient, especially if they have not reached maturity."* Martin*, Head of IT at a care provider in Central Europe*

> *"Technical evolution has been going on since forever, and won't be stopped. But, recently, it has become very fast – sometimes too fast."* Jeremy*, Head of department/CEO in Central Europe*

> *There is an incredible workload in healthcare. They simply don't, or can't, absorb these things anymore, all these new innovations. Also, the thing with new digital applications and innovations is, there are increasingly more of them, but none of them are removed."* Daphne

Many of our interviewees, like Martin and Jeremy, expressed concern about the rate with which new technologies are developed and adopted in healthcare settings. Daphne adds concern for the staff, because new technologies are constantly added but none are eliminated. While trainers can support healthcare workers with learning to use new technologies, there seems to be a lack of guidance on the organisational, national and even European level. To some degree, the materials from the SecureHospitals.eu project will begin to highlight on these issues and to address opportunities for change.

New processes that are not specifically related to cybersecurity topics can still provide learning opportunities for healthcare staff to improve cybersecurity. Many processes are interrelated, and often have an element of cybersecurity or information security that can be highlighted.

> *"When we implemented a new personnel file system, we used that moment to initiate a related project to make people aware of the personal accounts, and what the consequences are if they share account information."* Frank

> *"If the hospital decides to install a password system the user must be involved in the design, contributing to the level of usability of the project to improve awareness. This is very important, involve them from the beginning, it's a way to raise awareness."* Sophia

Frank and Sophia explain how cybersecurity training does not have to be a complete and standalone program. Security awareness can be raised in many different ways, and especially if resources are limited, trainers can use other processes as an opportunity to highlight related security themes. This way, trainers can highlight security as a component in every process within healthcare organisations and connect with the daily practices of healthcare workers.

3.2.5 Ownership and responsibilities

Drivers for change on the topic of cybersecurity may be legal reasons or ethical reasons, or even both. The specific reason for the organisation may affect the approach trainers should or could take to training development.

> *“Many hospitals make our training a mandatory element. I think this also has to do with compliance and certifications, such as the NEN 7510 or ISO27001. Every hospital has to demonstrate how they work on information security.”* Barbara

> *“Some organisations almost consider it a moral duty to improve their information security.”* Gemma

Barbara and Gemma describe different reasons for healthcare organisations to comply with regulations and standards. This can be important context for trainers, as it may affect the type of intervention healthcare organisations will want and fund. How the organisational perspective affects the attitude of their staff on this topic is something that could be further explored.

The success of cybersecurity-related interventions depends on people in key positions, those who take ownership of the issue and can push for change within the organisation. While all layers of the organisation are a part of the cybersecurity chain, those in management positions or their advisors are most likely able to initiate change.

> *“It depends on the people in crucial positions. What does a director think about it? What does the IT manager do? And can they activate the people around them?”* Gemma

> *Everyone needs to be engaged, but the top level management should always take the lead in cybersecurity and say “Okay, let's lock this down.”* Liam

> *“There is also a lack of secure tools. If the organisation doesn’t implement secure tools properly, a lot can and will go wrong.”* Daphne

Based on our interviewees’ experiences, management level staff in healthcare organisations are crucial drivers for change in an organisation. These person can help trainers connect with people in key positions to promote training ideas and gather support for new initiatives.

It can be unclear where ownership over and responsibility for cybersecurity and privacy related issues lies for both staff and management. As mentioned before, cybersecurity is a mosaic that everyone in the organisation contributes to. However, sometimes people are unsure or unaware of their responsibilities.

> *“Having dedicated people on cybersecurity or information security helps with ownership issues, however, it also becomes easier for others to say: ‘It’s not my job to do this, it’s yours’. So these people have to be able to turn a larger problem into a set of smaller ones, and to take up a coordinating role.”* Gemma

> *“It is often said that the security department is responsible for everything. No, if an employee makes a mistake and their account is compromised... This is where awareness comes in.”* Frank

Appointing a dedicated person with cybersecurity as their primary responsibility can both help and hinder ownership issues, as explained by Gemma. Frank suggests that awareness about each person's responsibilities may help solve this. Trainers can also address responsibility and ownership issues in training sessions, to make people aware about their position within the cybersecurity chain.

The implementation of new technologies is often the result of top-down decision making. This can mean that healthcare workers are not involved in the procurement of new technologies, and that they are merely subject to these changes.

> *"The relation between people and technology… they have to use it. They use it as part of their job. Nothing else. It is not their device, it is not their data capacity, and it is not their duty to care for security." Tim*

Tim explains how healthcare workers do not have or feel ownership over new technologies, but still carry the responsibility to work with them. This may affect the way staff approaches new technologies, for instance, because it is not clear what the added value of these innovations are for them. As a result, trainers may encounter resistance during training sessions thus they should be equipped with strategies to deal with resistance and other negative reactions from their audience.

3.3 What challenges do trainers face?

3.3.1 Organisational complexity

Healthcare organisations are complex. Trainers need to be aware of interconnections within the organisation and with external organisations or third party suppliers. This makes clear that trainers have to be aware of internal processes and connections with external services of various healthcare organisations to understand the context their clients and training participants work in, and to understand the risks that may exist in these various settings.

> *"I thought I had seen many complex organisations before I started to work at this hospital, but nothing is as complicated as a hospital. Almost everything, every process is linked in some way."* Frank

> *"We are arranged in themes, such as departments or even a complete sub-hospital within this hospital, and we have a local security officer for the total theme. And sometimes this is rather difficult to manage."* Albert

As both Albert and Frank suggest, the complexities and various levels of management make healthcare organisations difficult to organise in terms of cybersecurity issues, and as such increasingly vulnerable to attack. Awareness of these issues are crucial for the training process.

The size of healthcare organisations affects the type of challenges the organisation faces and the most effective ways to approach these. As mentioned above, larger organisations may have intricate structures that come with their own challenges. Reaching all employees with a newly implemented training initiative can be expensive and time consuming. Smaller organisations may struggle more with resources, such as expert knowledge and financial resources.

> *"Some organisations have 500 patients per year. Other organisations have 5000 employees. And each needs to be approached in a different way. You have to understand them differently, and the goals you try to reach vary per case."*

> Gemma*, information security consultant (care focused) for an IT consultancy firm in Northern Europe*

Based on Gemma's statement, flexibility in engaging training can increase the success of new training initiatives. A trainer needs not only understand their training audience, but also the organisations they work in. The context can help trainers to find the most appropriate way to design and implement training.

3.3.2 Resource management

Healthcare organisations deal with limited resources such as finances, time, required knowledge or manpower. As a result, they often have to choose what to invest in. The provision of healthcare remains the primary focus of these organisations and thus receives priority over all other investments. In addition, the potential gains of investing in cybersecurity measures and training are not always obvious or clear.

> *"For smaller organisations it can be complicated due to financial constraints. They can't just free up the funds to do it. That is relatively easier for larger organisations. But I think intrinsic motivation is more important than size or means."* Gemma

> *"After large investments, what do you get in return? Security, but what is that worth? A ROI [return on investment] is almost impossible. But what do you lose when an attack does happen? You can't express that in terms of money."* Frank

Cybersecurity is made up of intangible and invisible aspects, and investments do not provide clear or direct outcomes, as indicated by Frank. While the availability of resources can influence decisions to invest in cybersecurity, awareness of the risks and feeling the need to invest is a higher predictor for investing in cybersecurity, according to Gemma. Trainers thus need to be aware that cybersecurity awareness remains an important topic at management levels in healthcare organisations as well as at the level of those directly involved with patients or systems.

Information sharing within the organisation can be limited due to the structuring of the organisation, work pressure and time constraints. Trainers have to be aware of this issue as relevant knowledge related to cybersecurity may not be evenly distributed within the organisation and, consequently, among the participants of their training.

> *"If you go beyond the team of security officers, knowledge about security quickly diminishes, because everyone works in isolation, which makes it hard to share information and knowledge. Everyone is very busy, so it becomes difficult to structurally meet and share information."* Edward

The issue of siloed knowledge is that knowledge and experience are not shared and spread within the organisation, as Edward has encountered. Trainers have to try and overcome this by addressing the advantages of information sharing in their training.

Training quality should not be affected by the limited availability of resources. A more important criterion to judge trainings on is the methods trainers will use to interact with their audience. Additionally, one trainer suggested that healthcare organisations could work together and combine resources for the development of new materials, to share the burden.

> *"Success of the training is based on engagement, like in active engagement and commitment – not in terms of budget."* Liam

> *"Other organisations have created e-learnings about privacy (GDPR), and each has made a different one, there has hardly been any collaboration. So the proliferation of these education programs is quite high, but that brings its own risks. Small organisations invest money in the development and implementation, and this money can, of course, only be spent once."* Daphne, *self-employed innovation consultant (care sector) in Northern Europe*

Interactive training methods ensure higher quality than the availability of financial resources will, according to Liam. However, healthcare organisations can increase their budgets by cooperating and pooling funds. As Daphne mentions, cooperation among healthcare organisations on cybersecurity training is nearly non-existent. The SecureHospitals.eu project hopes to initiate and facilitate more collaboration with the development of the Online Awareness and Information Hub, the Massive Open Online Course, the Summer School and other project output.

3.4 What is their training process and what responses do they get?

3.4.1 Training content and strategies

A training can be more effective when the trainer uses targeted content that reflects daily practices of training participants. Cases, real life examples and demonstrations, and (recent) news items are commonly used by the trainers we interviewed.

> *"As for the training, I always try to bring some case studies. And I try to pull people in with questions. This is what works for me, it gives the listeners a possibility to share what interests them."* Robin

> *"We consciously choose to first ask a question about something the learners will likely recognise from their work. This way, you activate already existing knowledge that can then be connected to new knowledge, which creates stronger connections in their memory."* Barbara

All trainers we interviewed shared the experience of how important it is to relate to their training audience. As Barbara also adds, by starting from a situation trainees recognise, it is possible to attach new information to those situations. This is an important requirement for the development of new trainings and training materials as part of the SecureHospitals.eu project and in general.

Interactive training methods increase learning efficiency and interest of training participants. Almost all trainers mentioned they actively engage participants during training. The added advantage is that trainees are more interested in the training content and it increases learning outcomes. In eLearning programs, this is more complicated, but not impossible.

> *"When people are engaged in the conversation or in a topic, they're also more likely to learn from it, to form their own opinions, and to get a broader interest in aspects of it that would allow them to more easily identify adverse attempts at a later point."* Jake, *cybersecurity expert active in Northern Europe*

> *"ELearning's focus mostly on knowledge and insight to a certain degree. Application is more difficult. There are different levels of thinking, according to Bloom's taxonomy. An eLearning does not support learning at the highest level. That is easier to do in classroom situations."* Barbara

Jake explains how interaction with trainees results in more successful learning outcomes. However, trainers should be aware that the structure they use to train affects learning outcomes of trainings, and they should adjust their expectations accordingly. As Barbara explains, eLearnings do not allow for the same methods as face-to-face settings do. This should not be a limiting factor to trainers, as new learning technologies allow for a variety of interactive approaches. However, it shows that training methods should be strategically chosen.

The size and structure of the healthcare organisation determines which strategies for training are appropriate for trainings. Larger organisations struggle with reaching all their employees. Interpersonal strategies are difficult to achieve. Time and financial resources become an issue.

> *"'Train the trainer' principle and 'face to face' instruction are regarded as highly efficient. Still, not all staff can be trained face-to-face, for this would be far too expensive."* Daniel*, Deputy CEO and DPO in Central Europe*

The need for a strategic choice for training methods also applies on an organisational level. As Daniel explains, it sometimes not possible to conduct face to face training, so other training approaches should be explored. Trainers should have the ability to adjust their approach to match with the healthcare organisation they work for.

Trainers should use language that the target group understands and uses in daily practice. This matters both in terms of professional language as native language.

> *"We noticed that hospitals are a particular target group which wants to be more directly addressed. In healthcare, different terminology is used. You don't really speak of customers, but of patients or clients."* Barbara

> *"Explaining the GDPR requires the use of examples, but still it requires knowledge of jargon, because when you read about it, or when you have to justify your work, you have to know what it means. But they don't use the related language in their day-to-day lives."* Daphne

As mentioned previously, being able to relate to trainees' daily practices increases engagement. This can be achieved by using the language trainees come across and use in their work, as Barbara and Daphne indicate. Daphne also explained that English programs may deter some groups from participating in a training, as they may not be proficient in the language or feel unsure about it.

Placing cybersecurity and information security in the context of the patient interest can be a motivational factor for healthcare staff. While not part of the primary process (providing care), in current times, cybersecurity and information security are part of good care provision practices.

> *"You can call them out on their motivation to work in healthcare and how [cybersecurity] is connected to patient security. You can show them why they should want to and have to protect patient information."* Barbara

Barbara believes that connecting cybersecurity to patient interest can be a motivational factor for healthcare workers, especially because technology and cybersecurity are now an integral part of providing care. However, this can be risky if trainees still struggle with ownership issues as mentioned previously. Trainers should be aware of the attitude of their target audience has towards the topic.

Certificates and accreditation points are seen as an added motivational factor for trainees. Trainees experience heavy workload and sometimes have to do training during working hours or in their personal time. Having a type of reward may be beneficial to their motivation.

> *"People will like it if you can complete a course and receive a certificate. I see a lot of posts on social media of people who announce that they have received a new certificate."* Daphne

> *"The importance given to accredited programs is different per client, but their staff, doctors or nurses, can really use the accreditation points."* Barbara

Other ways to motivate trainees to participate in cybersecurity training are related to an extrinsic reward. Daphne suggest certificates or diplomas, while Barbara has heard positive responses to accreditation points. Regardless of its form, clearly trainers need to consider how best to provide their trainees with some form of evidence that they completed the training.

Mandatory participation of training efforts should be determined per organisation and per intervention. Overall, our interviewees stated that mandatory training should not be a given for all organisations.

> *"We have to realize that there are so many obligatory trainings the staff has to go through that the quantity causes apathy and the attitude 'I am here, I will listen, I will sign the list of participants and that's it."* Robin

The issues our interviewees had with implementing some form of mandatory training was that healthcare workers generally have a high workload and could 'mentally check out', as is the case in Robin's experience. If staff are uninterested or do not have time, they will not participate and thus not benefit from the training. Trainers should weigh the options regarding how mandatory a training should be together with the healthcare organisation.

3.4.2 Addressing awareness and alternative approaches

Alternative approaches to raising awareness may not be effective as standalone interventions. Most of these interventions have no mandatory element, so participation cannot be enforced. There is no guarantee that healthcare staff will engage with the awareness campaign and generally, response rates are relatively low, putting the effectiveness of these strategies into question. However, awareness campaigns may peak interest in the topic, creating a momentum that the healthcare organisation or trainer can use for additional interventions.

> *"On average, around 40% of the 500 approached employees responded to the survey [per round]. Because, if you don't care about security, you are not going to answer the questionnaire you're getting."* Albert

> *"It is almost impossible to create an awareness campaign with lasting effect. It helps as a way to provide an impulse, but then you have to do something more to hold the momentum, and that is a step that is often forgotten."* Gemma

The lack of response to awareness campaigns may stem from a lack of interest in the topic, according to Albert. And even if there is some success in engaging target audiences, awareness campaigns are not sufficient strategies on their own, explains Gemma. Trainers who want to implement an awareness campaign should think about methods to make use of the momentum such a campaign may create.

Physical communication materials are more successful than online and/or digital communication materials. For various reasons, online materials are not viewed or read often. Physical materials can be placed at strategic points in the working environment of healthcare staff, increasing visibility. However, the strategy behind these materials should be well thought out.

> *"Reaching employees is a challenge for all communication professionals, because they don't read messages on intranet and they don't read emails. Physical means of communication and live meetings are necessary."* Daphne

> *"One of the last campaigns we did was an animation movie, in Dutch and in English, because we also have international researchers. What do you think the response rate was? 3%."* Albert

> *"The disadvantage of a poster is that you don't notice it after the first or second time. Objects like paper cups can trigger a moment of realisation with every use. Having a little booklet that staff can carry with them helps to keep the topic tangible."* Gemma

It is a structural problem in organisations to reach and inform their staff members about important news and events, as indicated by Daphne. She states that physical means are still the most successful way to notify staff members. Albert's experience seems to underline this, while Gemma is somewhat critical of this. She states that physical communication materials have their own specific challenges that should not be ignored. Trainers could benefit from taking a mixed approach and use both online and physical ways to communicate with their target audience.

Fundamental knowledge about cybersecurity and auxiliary topics can provide a stronger basis for learning. If healthcare staff is taught about underlying concepts, it is easier for them to apply what they have learned in future situations.

> *"Knowledge about specific applications or programs can become outdated. So we shifted our attention to fundamental knowledge, making sure that learners know of underlying (security) mechanisms."* Edward

> *"I need them to understand and at least get a general understanding of how an attacker thinks, because that will also allow them to be more conscious about the information that they share, leave behind or disclose to people who they don't know that contact them."* Jake

Many of our interviewees consider it a problem that people are unaware of the way technology works. While they use different situations, Edward and Jake both show that knowing underlying mechanisms and concepts will help trainees not only with current situations, but also in future situations when details may have changed, but the mechanics have not.

3.4.3 Types of targeted training audiences

The targeted training audiences is heterogeneous; there is not a typical participant. Gender, age, education level, role in the organisation, these all vary. There is also a distinct difference context and practices of those who work in cure-centred organisations, such as hospitals, and those who work in care-centred organisations, such as elderly care or home care.

> *"I teach nurses, office people, those who work in financial control, and many more. From all levels in the organization, from the basic ground staff so to say up to middle management."* Tim

> *"We split healthcare sector into two categories, care and cure, and they are very different from one another. And the target audience 'the healthcare worker' does not exist. "* Gemma

> *"Each sector in healthcare requires its own jargon and specific cases. For instance, in disabled care, employees are responsible for the social media use of clients, in the elderly care this the responsibility of relatives."* Daphne

The target audiences of cybersecurity in healthcare organisations can vary in many ways. The pre-existing knowledge, experiences and practices depend on each trainee's role in the organisation. Additionally, the type of organisation and which type of patients or clients they serve greatly influences which cases are relevant for training audiences. Trainers need to be aware of these variations in order to tailor their training as much as possible. This way they can relate most effectively to their target audiences and create effective learning opportunities.

Knowledge, awareness, and skill in cybersecurity is unevenly spread among the target audiences. Given that there is not a typical participant of cybersecurity training in healthcare, it should not be surprising that some processes and practices may be considered as easy or basic information for some, it is still unknown or difficult to understand for others.

> *"The eLearning concerns basic information, because many of our employees have not mastered even that level yet. Simple things are in there, such as who do you call when you lose your personnel pass? Because it can also be used to enter many areas of the building."* Frank

> *"A lot is being shared through WhatsApp. There still are a lot of challenges here, and it's not unwillingness, but people honestly don't know how it works. Of course there is the aspect of convenience. A quick email is easier than undertaking several actions [for secure emailing], but I believe it is mostly unawareness."* Daphne

Trainers have to be able to determine the ways in which knowledge acquisition can be complicated by a resistance to participate in cybersecurity training or may be a lack of understanding or motivation for the topic. As such, they have to be able to understand their audiences' attitudes and manage the variety of skill levels their trainees may have.

Training and interventions are often focused on staff working with medical data, while less attention is being given to those with access to other types of sensitive data. Processes that do not directly relate to healthcare provision can be overlooked when thinking about cybersecurity and privacy.

> *"Security and medical incident reports often contain patient data. Personnel files contain person data of staff that should remain private. These are all things that should be considered."* Frank

> *"HR is often overlooked or neglected. They don't get much training in security and privacy during their education. And I often see passport copies etc. lying around, or that they printed something and haven't picked up yet. And the information in these files can be really sensitive."* Gemma

Frank and Gemma both address the issue that staff working in Human Resources can be overlooked when training is implemented. This is a risk to cybersecurity as it weakens a part of the cybersecurity chain. Trainers should inform their organisations whether secondary processes are targeted with training and be able to advocate for additional training for these group of employees.

Working with new technologies seems to be more challenging for older healthcare staff members, while younger workers may be less careful with privacy matters. Older healthcare staff often consider it more difficult to work with new technologies, while younger staff seems to adapt more quickly.

> *"New technologies represent a challenge for older adults. But it appears that this challenge is managed quite well. And future generations will have learned to deal with these technologies, having used them in their active working life."* Martin

> *"It's not the oldest group who scored the lowest [on digital literacy], but the group aged between 40 and 50 years old. People often think that younger people are more skilled than older people. In a way that is true, because they pick up new things quicker. However, older people are more careful about privacy and what they share."* Daphne

As portrayed by Martin and Daphne, each age group has its own specific challenges in relation to cybersecurity issues. Older staff members are not as used to working with technology, while younger staff members are more open with sharing information. This may be valuable for trainers to keep in mind when they design their training.

The level of education seems to influence the ease with which healthcare workers adopt new technologies. Those with a vocational education background seem to struggle more often than those with college or university level education.

> *"There is a lot of complex material with a lot of jargon. And these are mostly employees with a vocational education background who find this difficult."* Daphne

Learning about cybersecurity and privacy is not easy because there are specific concepts and a different kind of language involved. Daphne adds that most of this language is also in English, which can complicate the situation for some even further. Trainers can support their trainees by providing easy to understand examples and using language that audiences may come across and use in their daily practices.

Healthcare staff seem wary of new healthcare technologies, but the acceptance is growing. Generally, trainers indicate that healthcare staff finds that technologies take away from their core responsibility, patient care. However, the level of acceptance is rising, as staff members start to understand that technologies are indispensable and even helpful in modern healthcare settings.

> *"But everyone I spoke with gets that digital skills are (becoming) a part of working in healthcare. They also see the need in their private lives, and it is impossible to go around it."* Daphne

> *"With the development of the smartphone in the last ten years, [healthcare professionals] think: why can't I do this on my phone? They think it's only logical that something is within hands reach."* Chris

> *"I guess – just a guess – they are struggling with their routines. And when their routines are disturbed, they are in stress. And if a new term like cybersecurity comes in, they are stressed even more. BUT – and this is important – if they see that cybersecurity can be part of their routine and makes their life maybe even easier – then you have their attention and their acceptance."* Tim

The acceptance for new technologies and learning to work with them is in transition. Especially because the need in people's private life is also growing, according to Daphne. Chris and Tim add that technologies are generally more accepted if they prove to make their work easier and not harder. Trainers can use this to relate the use of technologies to the private lives of their training audiences, and to approach the topic from the perspective of easing the workload.

A large part of healthcare staff struggles with digital literacy and digital skills. A part of this group struggles with literacy in general as well. This may affect the issues with privacy, as this requires a type of language they struggle to master.

> *"Through my research found out that 1 in 10 healthcare professionals is digitally illiterate [=not highly skilled with digital innovations]. And in elderly care, we estimate that number to be higher, to at least 2 in 10. ... I think low literacy rates and a lack of digital skills are at the basis of many problems with privacy … They have a hard time with difficult words and computer-related words."* Daphne

> *"It's the workarounds they make up because they do not have digital skills. Some people are sometimes so happy the computer works that they won't lock their screen. Others have very large fonts on their phone that you can read from a mile away. And some nurses have a 'shadow administration' on paper. This causes substantial risks."* Gemma

Daphne's own research helped her determine that low literacy rates and a lack of digital skills are a big concern for cybersecurity and privacy issues in her organisation. Gemma agreed and added examples of what this looks like in practice and that it increases risks to cybersecurity and information security. What can be considered basic skills to some, may prove to be challenging to others. As such, trainers will come across different skill levels in their training audiences, and must be able to notice this and adjust their training accordingly.

Digital skills are either not a part of vocational or university education of healthcare staff, or the addressed skills and technologies do not often match what is being used in reality. There exists a great disconnect between current education programs and the needs that exist in the healthcare sector.

> *"Digital skills are optional courses in nursing programmes. If students do not choose these courses, they will not learn to work with healthcare technologies. Also, the content of these courses are also not aligned to which technologies are actually being used in healthcare … Existing learning materials mostly focus on cognitive aspects and mostly 'send' knowledge to students."* Daphne

Trainers have to be aware that experience in and knowledge of working with healthcare specific technologies can vary greatly among their target audiences. Even recently graduated nurses may not have had the preparation to work with innovations in healthcare that may be expected from others. This limited experience and knowledge will significantly impact the readiness of an organisation to develop a good cybersecure staff culture and mentality.

3.4.4 Emotions and responses of trainees

Cybersecurity can evoke a range of emotions in trainees. These emotions can be tied into trainees' disinterest in the topic, the resistance to work with technology as opposed to working with people, or even fear to make a mistake. However, not all responses are negative.

> *"They are afraid to update their devices, because they depend on them, and what if something goes wrong and they don't work anymore?"* Gemma

> *"There's a taboo to talk about it, there is shame. Of course, there is also resistance to learn. People say that they chose to work with people, not machines. Or the fear that robots will take over their jobs… I think that in most instances of resistance [from employees] there is fear, lack of knowledge, thinking it is complex and scary."* Daphne

As explained by Gemma and Daphne, negative emotions may hold trainees back in developing their digital skills and performing their jobs. For this reason, it is important trainers learn to address these emotions if they come up during training sessions.

Trainees may not show interest in the training during training sessions, or even actively resist participating. Sometimes trainers find it challenging to create a positive learning experience for all participants.

> *"In general, medical doctors are a special sort of people. They historically underwent a complex and long formal education in their field and they often see the cybersecurity trainings as forced upon them. They sometimes say 'I am a doctor, I am not interested in these things. There are professionals, the DPOs that should do this. I treat people and am not interested in these things'."* Alex

> *"It can be difficult to engage people who are not actively participating. I try sometimes to engage them, but mostly I don't want to ruin it for the guys who actually want this type of training. So sometimes I throw out some decoys [jokes or live demonstration] that call the others to sort of get their attention back."* Jake

Alex' and Jake's experiences are not unique; several of the trainers we interviewed have had one or more oppositional trainees. Trainers have to be able to manage these moods and possibly group dynamics. Jake suggests to (shortly) divert from the training and use humour or live demonstrations to reengage trainees.

Cybersecurity becomes a more attractive topic after an incident has occurred. However, this interest does not extend to other cybersecurity related topics.

> *"Usually the trainees have very specific questions about the things they have come across during their work. This is fun, because then you have material you can work with."* Edward

> *"We offer to visit a department meeting after an incident has happened. The first time our offer is rejected. After it happens again, they usually say yes. And these sessions are often the most fun to do. Staff is receptive of new information due to a negative experience, but they are only interested in information about the specific incident that just occurred."* Frank

It is possible that incidents trainees were personally involved in helped them realise what they needed to learn and which questions to ask. To re-create such positive response from their audience, trainers can try and build training sessions around incidents that occurred at the healthcare organisation in question. However, while this can lead to interesting and fun training sessions for both trainers and trainees, limiting training sessions to only real life cases may not provide sufficient material for training healthcare staff and prepare them for future incidents.

3.5 Suggested training content and approaches to communication

From our interviewees, we received the following topics and communication strategies to be the most regularly mentioned.

3.5.1 Relevant topics for training initiatives

- Passwords and password management
- Phishing
- Use and risks of USB drives
- Internet access
- Mobile phones and apps
- Taking, storing, and sharing pictures
- Data protection and practical consequences
- Paper printouts versus electronic documents
- Identifying cybersecurity threats
- What does cybersecurity mean – what does cybercrime mean – what does that mean for my organization?
- Judging sources on credibility
- Social Engineering
- Social Media
- Media competence
- Suspicious cases alert
- Confidentiality
- How to deal with data, lists, mobile phones
- Detailed and understandable explanation of the GDPR
- Insider threats
- Handling personal and organisational data

3.5.2 Tips for training and communicating about cybersecurity

- Focus on the most important points and topics
- Show them what is relevant for their daily work
- Never create fear
- Offer additional learning material or courses
- Encourage the staff come up with suggestions for improvements regarding cybersecurity
- Try to work with storytelling and pictures from everyday life
- Involve the audience
- Give some sort of reward, such as a certificate or accreditation point
- Empower your employees to act conscientiously and responsibly
- Relate to recent incidents and topics currently in the media
- Integrate new perspectives
- Initiate reflection and discussion among participants
- Give participants ample possibilities to experiment and to analyse example cases
- Provide background information and fundamental knowledge
- Gather, evaluate and use feedback
- Get the participants to bring examples from their everyday life, and to ask questions

4 Conclusion

The interviews provided insight into the practices of trainers, the context they work within and how trainees respond to their efforts. This provided valuable insight for the SecureHospitals.eu project and recommendations for European Union policy development.

4.1 Actionable results and quality criteria

Given the insights of our interviewees and analysis of their responses, rather than reiterate the findings detailed above, the focus of these conclusions is on the actionable results that can be determined from the themes that emerged from our interviews. In some cases, these directly translate into 'quality criteria' that need to be integrated into the development of future tasks of the SecureHospitals.eu project. For instance, this report provides direct input for Task 4.3: 'Create novel training curricula on cybersecurity in hospitals topics and define minimum quality standards for training material'. In other cases, further interpretation of how best to use this information from our interviewees will be required.

4.1.1 Supporting trainers

As noted, our interviews focused on the profiles and motivations of trainers and this suggests some important criteria and intentions going forward.

Trainer profiles - Given the multiplicity of trainer profiles evidenced in this report, the SecureHospitals.eu project should determine which persons are best supported through the project deliverables to ensure effective cybersecurity training within healthcare organisations. Based on our interviews, trainers for which cybersecurity training is only a small part of their overall workload may be best suited as a target audience for the SecureHospitals.eu project.

Trainer motivations - We aim to increase accessibility to usable materials for already motivated trainers. This way we provide trainers with the resources they need for their continued work.

4.1.2 Addressing their contexts

Cybersecurity in healthcare organisations - This project seeks to further equip trainers with the tools to communicate the importance of cybersecurity within healthcare organisations. A focus on examples of cybersecurity issues will further demonstrate the motivations and methods of cybercriminals to gather data from healthcare contexts.

Cybersecurity mosaic - By understanding cybersecurity as a mosaic, we can support trainers in determining training strategies on how to address cybersecurity in general, its core issues, and solutions, while making sure that the relation between technical and human factors is addressed through training.

Regulatory compliance and GDPR hysteria - The increased concern about data protection and privacy has both improved the visibility of cybersecurity issues and made the work in this area much more complicated. As such, workable understandings and responses to legislation and compliance issues need to be integrated into future project outcomes.

New processes and technologies - The proliferation of new technologies and innovation in healthcare can be a risk, but also provides the opportunity for trainers to reiterate best practices in cybersecurity. By sharing trainer experiences with new process and technology implementation, we can provide a more robust support for trainers in different contexts.

Ownership and responsibilities - A focus on expanding a sense of ownership and participation in cybersecurity practices needs to underlie the orientation and language of the project work.

4.1.3 Responding to their challenges

Organisational complexity - We will determine the level at which resources from the project will be focused and ensure that deliverables maintain a flexible approach for integration and adaptation to contextual factors.

Resource management - Through our project deliverables, we support those trainers with limited resources to develop training to find, create, and share training strategies, content and materials.

4.1.4 Improving audience engagement

Training content and strategies - To increase training effectiveness, we will develop and share training strategies and materials that support trainers in relating to their trainees (interests, motivation, gains). As part of this, we will make sure to include fundamental knowledge in understandable language.

Addressing awareness and alternative approaches - Cybersecurity training and awareness programs are less effective as isolated initiatives, especially when training content and materials are mostly available online. With our project outcomes, we can support trainers in developing a more holistic approach to cybersecurity training.

Types of targeted training audiences - The targeted training audiences vary in many ways; the group is highly heterogeneous. New training programs and materials should address and be suitable for all these different profiles.

Emotions and responses of trainees - Cybersecurity training development has to take a more holistic approach to the potential responses of trainees. This is in recognition that adapting to changes to new technology use requirements can sometimes evoke emotive responses in trainees.

In summary, the above actionable results can be listed as the following:

- Trainers for which cybersecurity training is only a small part of their overall workload are in most need of support
- Increase accessibility to usable materials and include fundamental knowledge in understandable language
- Maintain a flexible approach for integration and adaptation as well as training that addresses a heterogeneous audience
- Focus on relevant examples
- Increase recognition of cybersecurity as a complex set of issues that requires a holistic approach and make this a part of training initiatives
- Create workable understandings and responses to legislation and compliance issues
- Share trainer experiences with new process and technology implementation
- Expand a sense of ownership and participation in cybersecurity practices

- Recognize and respond to the role and impact of emotional responses to all training related to technology

4.2 Recommendations for the European Union

The results highlighted some issues that seemed to be similar experiences of trainers from all over the EU. These shared experiences signal potential topics to address with legislation. The European Union could provide meaningful support in the form of policy and resources.

Promote cybersecurity as part of proper patient care culture - Based on our interviews, cybersecurity is mostly considered ‘other’, ‘extra’, ‘additional’ to healthcare practices. With the current and future adoption of technologies, this perspective is untenable. Promotion of cybersecurity initiatives should reflect the way cybersecurity is inherent to many processes both in and beyond healthcare.

Stimulate and support cooperation on cybersecurity improvement in healthcare in the EU - Healthcare organisations seem to take on cybersecurity challenges individually. The EU could support opportunities for cooperation and collaboration among the organisations in Europe. This way, healthcare organisations can share resources, such as time, finances and expert knowledge, providing even smaller healthcare organisations with the opportunity to address cybersecurity challenges.

Boost the incorporation of digital skill classes as part of medical and/or non-IT education programs - Currently, education programs for medical staff lack courses on digital skills, or existing classes do not match actual practices. This mismatch can undermine cybersecurity efforts, as a lack of digital skills can lead to far-reaching and heavy consequences.

Invest in opportunities and resources for professional training for trainers in the EU - Trainers take the initiative to invest in their professional development. The EU can provide more opportunities for trainers and experts and to connect with their peers across Europe. As discovered through our interviews, trainers encounter the same or similar challenges in their work. Receiving training on EU level allows them to share their experiences, which can help them to push training quality to a new level.

Provide guidelines and standards for the adoption of new technologies and innovations in healthcare. The trainers we interviewed shared the experience that not all newly adopted technologies supported quality care. Furthermore, healthcare workers reached a point of oversaturation with the amount of new technologies they need to learn how to use. The EU could support with advice and guidelines for healthcare organisations how best to approach this.

References

Boeije, H. (2014). Analyseren in kwalitatief onderzoek: Denken en doen. (2nd ed.). The Hague: Boom Lemma.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Annex 1: Interview Questions

Opening questions

- Please tell me about yourself and your role in this organisation.
  - If external trainer or trainer organisation: What types of healthcare organisations do you normally work for?
  - How does your work differ between the different types of organisations you work for?
- What does a ‘normal’ day (training session, course, other?) look like?
- How do you develop and implement cybersecurity sessions?
  - Do you create training programmes/sessions based on requirements set by the respective organisation for which you will deliver the training?
  - Do training programmes/sessions serve as a promotion for other services or activities you or your organisation offer?
  - Do you arrange sessions to create or maintain professional networks and relationships?

Experiences and knowledge transfer

- What qualifications or knowledge do you need as a cybersecurity trainer and how did you go about acquiring this?
- What do you feel makes you/someone successful as a trainer?
- What do you think is the most relevant content to address in cybersecurity training sessions?
- How do you consider the relationship between humans and technology and how does this show in your training sessions?
- How do you bring your cybersecurity message across to participants, and how do they respond to this?

Training practices and materials

- What materials and teaching strategies do you use?
- What sort of interactions with participants do you find most effective and stimulating for training?
  - What factors is this dependent on?
  - How do you involve less engaged participants?

Personal orientation to work

- How do you view your role as a trainer in cybersecurity?
- How do you facilitate learning and change in participants?
- What are your motivations to work as a trainer in cybersecurity?
- What are significant positive and negative experiences that you had during cybersecurity training sessions?
- Do you gather feedback from participants?
  - If no: is this for a particular reason?
  - If yes: how do you incorporate the feedback you receive in future training sessions?
- What is your most significant memory/lesson (good or bad) in relation to your work as a trainer?

Participant profile and motivations

- Who follows your training?
  - What sort of roles do participants have in their organisation?
  - What are typical characteristics of participants?
- What are the reasons participants take part in training/courses with you/your organisation? (Beyond being required by their employer.)

Experiences with participants

- What do participants struggle within their day-to-day work in relation to cybersecurity and has this changed? If so, how?
- How do you address the concerns participants raise during training activities?
  - For instance, if they do not understand the content.
  - Or if they do not see the added value of the training.
- What do participants communicate about cybersecurity and technology use in their work to you as a trainer?

Annex 2: List of interviewee profiles

This appendix contains the list of interviewees. Names are pseudonyms. A short description of the organisation they work for is included to provide context to interviewee perspectives.

#	Name	Position	EU region
1	Albert	CISO of an academic hospital	Northern Europe
2	Barbara	Education specialist at an information security education company	Northern Europe
3	Chris	Academic medical researcher at an academic hospital	Northern Europe
4	Daphne	Self-employed innovation consultant (with a focus on care sector)	Northern Europe
5	Edward	Clinical IT and data management support at an academic hospital	Northern Europe
6	Frank	Information Security Officer CISM and DPO at a hospital	Northern Europe
7	Gemma	Information security consultant for an IT consultancy firm	Northern Europe
8	Henry	Privacy officer at an academic hospital	Northern Europe
9	Gino	Cybersecurity expert and lecturer	Southern Europe
10	Jake	Cybersecurity expert	Northern Europe
11	Liam	Security expert and trainer	Northern Europe
12	Sophia	Professor in technical cybersecurity	Southern Europe
13	Robin	Trainer cybersecurity for multiple organisations in various sectors	Central Europe
14	Alex	Trainer and DPO for multiple care providers	Central Europe
15	Martin	Head of IT at a care provider	Central Europe
16	Daniel	Deputy CEO and DPO for a care provider	Central Europe
17	Steve	Department head /CEO for a care organisation	Central Europe
18	Jeremy	Department head/designated CEO for a care provider	Central Europe
19	Tim	System architect and trainer	Central Europe