SECUREHOSPITALS.EU

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

D3.4 Cybersecurity in hospitals Knowledge Baseline 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:	**D3.4**
Title:	**Cybersecurity in hospitals Knowledge Baseline Report**
Lead beneficiary:	**EUR**
Work package:	WP3
Dissemination level:	Confidential (CO)
Type	Report (R)
Due date:	31.08.2019
Submission date:	01.10.2019

Authors: **Tessa Oomen,** EUR
Jason Pridmore, EUR

Contributors: **Stela Shiroka**, INSP
All partners

Reviewers: **Yung Shin van Der Sype**, TLX

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

TABLE OF CONTENT

TABLE OF TABLES

EXECUTIVE SUMMARY

This report provides a baseline description and understanding of the Online Information and Awareness Hub (OIAH) developed by the Secure Hospitals.eu project. It details the connection to the larger project and the goals and audience of this information hub. The report describes the categorisation of articles into four sections, Policies and Regulations, Handbooks and Guidelines, Risk Assessments and Checklists, and Case Studies. Links to each article the hub are given for further review. The report then briefly details how OIAH will become a part of the other efforts of this project, namely the online course, the summer school and workshops. Finally, it mentions how the resource is intended to be used and developed in the remainder of the project and beyond.

1 Introduction

Cybersecurity is currently one of the leading challenges for healthcare organisations. However, there is at present no centralised online information and solution directory that stakeholders can consult. One of the goals of the SecureHospitals.eu project is to create an Online Information and Awareness Hub (OIAH) for trainers, IT specialists, managers and other stakeholders working in or with healthcare (SecureHospitals.eu, 2019a). As SecureHospitals.eu is a Coordination and Support Action, the OIAH is seen as a key support deliverable for the consortium, and a deliverable that will be accessible beyond the lifetime of this particular project.

A key resource within the OIAH are the knowledge articles and sources for further reading. These articles draw on previously defined work developed in work package 3, specifically the collection of relevant literature and other knowledge sources surrounding cybersecurity challenges and (training) solutions for healthcare organisations. Results from the SecureHospitals.eu survey (D2.2) and the Interview report (D4.2) have guided the process and are incorporated in the articles we have added to the OIAH. This deliverable, D3.4 Cybersecurity in hospitals knowledge baseline report, details the process of creating the articles and the choices made for the OIAH. Furthermore, this report will indicate how the articles will be used for the MOOC, the summer school and the local sessions and webinars. While this deliverable is intended to make accessible the process behind the OIAH development, links to described articles are available in this document.

1.1 Links to other work packages

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

- **WP2 - INVOLVE:** The articles that are written as part of D3.4 will be uploaded on the Online Awareness and Information Hub, which is a part of WP2.
- **WP3 - AGGREGATE:** Previous tasks that are part of WP3 provided the sources that are necessary for the work for the baseline report.
- **WP4 - CREATE:** The interview report (D4.2) has provided relevant insights for the baseline report. Additionally, this report and the articles will provide input for training schemes and curricula that will be developed in WP4. As part of D4.3, this work is referenced specifically to indicate the relationships between the material to be developed and the baseline report.
- **WP5 - BOOST:** The articles that are written as part of this deliverable will be used as (additional) readings for participants in project activities, such as the MOOC, summer school and local workshops and webinars.
- **WP6 - COMMUNICATE:** The articles that are written as part of this deliverable will be uploaded to the OAIH, which then can be used to promote the Hub and project as a whole.

1.2 Structure of the report

As the majority of resources developed for this deliverable are available through the OIAH, this baseline report contains links to these resources and gives an overview of the process behind their development. The further structure of this baseline report is as follows: Chapter 2 describes the choices made for the structure and content of the resources currently added to the OIAH. Chapter 3 describes the further use of these resources and further dissemination options. Chapter 4 concludes the baseline report.

2 Content of the baseline report

The consortium had several discussions about what resources to include in the OIAH and this baseline report. In consultation with our stakeholders and drawing on our previously developed project deliverables and work, we oriented the knowledge and information hub towards specific content choices. These choices were made in relation to the goals for this resource and the audience we defined as most relevant for our work.

2.1 Goal and target audience

The OIAH serves as a resource for staff of all types of healthcare organisations. It contains a collection of relevant articles in which information is tailored to the healthcare sector. This resource is not meant to be an exhaustive collection of all relevant topics for cybersecurity in healthcare, but to serve as a starting point for those wanting to learn more about the topic in this particular context.

Central to the creation of OIAH is that its contents should be accessible to all types of staff working in the context of healthcare organisations, as well as to those with little to no experience in cybersecurity (SecureHospitals.eu, 2019b). This broad audience focus means that staff categories such as medical staff, maintenance and upkeep, management and board members, and IT and security staff should find the handbook useful. While this affects the depth of the content for each article, it does not detract from its effectiveness. Each article will be provided with a list of sources for further reading that are relevant to those with more expertise on the topic.

2.2 Content and structure of the OIAH

During the development of the SecureHospitals.eu project, broader categories were previously set out as the focus of this deliverable. Based on the Survey of D2.2 and the trainer interviews of D4.2, we refined the list of categories and defined a subdivision of topics for individual articles (SecureHospitals.eu, 2019b).

Each article contains a description of the topic, the central concerns, and how these concerns should or could be addressed. Each article provides a list of options for further reading for those who would like to learn more about the topic.

The complete list of categories and article titles can be found in Table 1. The hyperlinks to the articles on the OIAH can be found in Appendix I.

2.2.1 Policies and regulations

The first category contains articles that summarise relevant EU-level policies and regulations with regards to privacy and cybersecurity. This collection of articles describe what a specific policy or regulation entails and how it applies to the healthcare sector. In one of the articles, the different national security plans (if available) are described or given direct links. These articles are relevant to all staff member groups in healthcare, but are generally more geared towards security and management level employees.

2.2.2 Handbooks and guidelines

The second category consists of articles about handbooks and guidelines. One set of these articles contain a summary of useful handbooks for management and security professionals in healthcare.

The second set of articles contain guidelines to enhance security. These articles may be useful for all staff member groups in healthcare.

2.2.3 Risk assessment and checklists

The third category provides more insight to the way healthcare organisations could address risk and incident management with regards to cybersecurity. As such, this category is more relevant to security and management level staff members, although it contains relevant knowledge for all members of staff.

2.2.4 Case studies

The fourth category contains case studies of actual events that highlight the importance of cybersecurity in healthcare. The cases include a description of what happened, why it was able to happen and how the incident was resolved. The selection of cases was based on their relevance to the project and the selected topics for the handbook.

2.3 Resources and literature

As part of work package 3, the SecureHospitals.eu project consortium gathered literature and relevant source material that relate to the project. These sources were used in writing the articles if they met the criteria: sources should not be older than 2014, and sources must be authored by reputable organisations or experts.

During the writing of the articles, additional sources were selected to be able to cover the selected topics. The sources for writing the articles stem from relevant EU bodies, academic research, white papers from reputable IT organisations, and blogs by specialists. Other referenced sources are EU funded projects. National resources and cybersecurity initiatives provided specific insight to each member state's individual approach to address cybersecurity.

All the collected sources will be available in a public library facilitated by Zotero and linked to the OIAH (SecureHospitals.eu, 2019a).

Table 1: List of articles published on the OIAH

Category Article No.	Policies & Regulations	Handbooks & Guidelines	Risk Assessment & Checklists	Case Studies
1	NIS Directive	How to create a strong password	How to handle health data	The AMCA case: Hacking and data breaches in healthcare
2	eIDAS Regulation	Habits to be safe online	How to handle personnel information	The WannaCry (UK) and ASP (Italy) cases: Holding medical data hostage through ransomware
3	GDPR	Cybersecurity management guidelines	How to detect a hacker	The Nansh0u campaign: Cryptojacking medical computing power
4	ISO/IEC 27000 family	Ransomware: risks and preventive action	Cyber incident response	The Evilnugget case: The potential for cyberespionage
5	The National Security Plan: Clarification and examples	Good Practice Guide for Incident Management, ENISA	Assessing training needs	Spoofing medical imaging: Highlighting security issues of malware
6	Regulation (EU) 2017/745 on medical devices and regulation (EU) 2017/746 on in vitro diagnosis devices	Incident Handler's Handbook, SANS Institute	How to establish a security culture	The Barbie case (The Netherlands): GDPR and the mishandling of patient information
7	EU Cybersecurity Act	Materials and Resources, European cyber security month (ECSM)	Risk management and assessment	The UnityPoint Health breach: Phishing for sensitive information
8	CSIRT Network and its members	Threat and Thematic Landscapes in interaction, ENISA		Boston Children's Hospital (US): Hacktivism and DDoS attacks
9		Diagnosing cyber threats for smart hospitals, ENISA		

3 Employing the OIAH

The articles that are created as part of this deliverable will be published on the Online Information and Awareness Hub. They will be used as reading material for other outputs of the SecureHospitals.eu project.

During the development of the Massive Open Online Course, the Summer School and the local workshops and webinars, more relevant topics may be identified and added to the list of articles. By doing this, the OIAH will remain up to date and relevant.

3.1 Public resource on the Online Information and Awareness Hub

As mentioned before, the articles of the baseline report will be made available on the OIAH. This way, the knowledge from this project will be publicly accessible for organisations and individuals who are interested in the topic. The OIAH will be promoted through the projects communication channels.

The OIAH will be the first collection of sources, articles and other resources on cybersecurity in the context of healthcare.

3.2 Reading material for the Massive Open Online Course

Alongside additional sources, the articles that are part of the baseline report will serve as reading material for the MOOC that developed as part of task 5.3. Reading the articles will be part of the assignments for participants, and the participants will be encouraged to use the discussion board to discuss cases or specific aspects of these cases in depth. Additionally, quizzes may contain questions that are based on the articles created as part of this deliverable.

3.3 Reference material for Summer School

The articles will be used as initial reading material during the Summer School. As the summer school is aimed at more advanced security professionals, the articles may not contain new information to them. Instead, these readings may open the floor for discussion and allow them to share professional experience and new perspectives. Potentially, new topics for articles may result from these discussions. These can then be developed and published on the OIAH.

3.4 Reference material for local workshops and webinars

The OIAH will be promoted among the participants of the local workshops and webinars. The articles will be referenced as reading material and as a starting point for participants when they would like to find more information.

3.5 Further use and development

The goal of the OIAH is that this becomes a resource for many working in the area of cybersecurity and healthcare. This hub will be available throughout the lifetime of the project and beyond and will be shared extensively through the project's dissemination channels. The 'Community of Practice' module which will be launched at a later project stage, is sought to develop the OIAH from being only a resource, to a space for the community to share additional resources, practices, and developments from the field.

At present, the hub focuses on collected information and information created and developed by SecureHospitals.eu partners. However, as the topic of cybersecurity and healthcare continues to be an ongoing and newsworthy topic, the OIAH will be added to with ongoing news stories on this topic. New information or the publication of new guidelines or handbooks by organisations working on this topic will be included in hub updates. These may come from our own deliverable and engagement work (MOOC, Workshop, and Summer School) or from related project deliverables. With the aim of creating strong synergies with other European projects, the OIAH will provide a space for related projects in the field of cybersecurity for healthcare to publish their results and bring the community together.

4 Conclusion

This report briefly describes the OIAH and its use within the SecureHospitals.eu project. The articles themselves constitute approximately 20.000 words of text within 32 specific articles at the time of this deliverable submission and will grow in the coming months of the project. This resource is particularly timely and pertinent, as there is simply no similar resource to be found online at the moment on this specific topic. As the OIAH both serves as a crucial component of all of the future training activities of the SecureHospitals.eu project and as a key resource that will be available beyond the lifetime of the project, this resource demonstrates critical value for exploitation within the EU and beyond. This report simply serves as a reference point for the larger body of work available at the OIAH.

5 References

SecureHospitals.eu. (2019a). The Online Information and Awareness Hub. Retrieved 1 October 2019, from SecureHospitals.eu website: http://securehospitals.eu/

SecureHospitals.eu. (2019b). *Trainer interviews report*. Retrieved from https://project.securehospitals.eu/deliverables/

Annex 1: Link to the articles on the OIAH

Policies & Regulations

- Overview: http://securehospitals.eu/knowledge/policies-and-regulations/
- NIS Directive: http://securehospitals.eu/2019/09/30/nis-directive/
- eIDAS Regulation: http://securehospitals.eu/2019/09/30/eidas-regulation/
- General Data Protection Regulation: http://securehospitals.eu/2019/09/30/general-data-protection-regulation/
- ISO/IEC 27000 family: http://securehospitals.eu/2019/09/30/iso-iec-27000-family/
- The National Security Plan: Clarification and examples: http://securehospitals.eu/2019/09/30/the-national-security-plan-clarification-and-examples/
- Regulation (EU) 2017/745 on medical devices and regulation (EU) 2017/746 on in vitro diagnosis devices: http://securehospitals.eu/2019/09/30/regulation-eu-2017-745-on-medical-devices-and-regulation-eu-2017-746-on-in-vitro-diagnosis-devices/
- EU Cybersecurity Act: http://securehospitals.eu/2019/09/30/eu-cybersecurity-act/
- The CSIRTS Network and its members: http://securehospitals.eu/2019/09/30/the-csirts-network-and-its-members/

Handbooks & Guidelines

- Overview: http://securehospitals.eu/knowledge/handbooks-guidelines/)
- How to create strong passwords: http://securehospitals.eu/2019/09/30/how-to-create-strong-passwords/
- Habits to be safe online (cyber hygiene): http://securehospitals.eu/2019/09/30/habits-to-be-safe-online-cyber-hygiene/
- Cybersecurity management guidelines: http://securehospitals.eu/2019/09/30/cybersecurity-management-guidelines/
- Ransomware: risks and preventive actions: http://securehospitals.eu/2019/09/30/ransomware-risks-and-preventive-actions/

Risk Assessment & Checklists

- Overview: http://securehospitals.eu/knowledge/risk-assessment-and-checklists/)
- How to handle health data: http://securehospitals.eu/2019/09/30/how-to-handle-health-data/
- How to handle personnel information: http://securehospitals.eu/2019/09/30/how-to-handle-personnel-information/
- How to detect a hacker: http://securehospitals.eu/2019/09/30/how-to-detect-a-hacker/
- Cyber incident response and management: http://securehospitals.eu/2019/09/30/cyber-incident-response-and-management/
- Assessing training needs: http://securehospitals.eu/2019/09/30/assessing-training-needs/
- How to establish a security culture: http://securehospitals.eu/2019/09/30/how-to-establish-a-cybersecurity-culture/

- Risk management and assessment in healthcare organisations: http://securehospitals.eu/2019/09/30/risk-management-and-assessment-in-healthcare-organisations/

Case Studies

- Overview: http://securehospitals.eu/knowledge/case-studies/
- The AMCA case: Hacking and data breaches in healthcare: http://securehospitals.eu/2019/09/30/the-amca-case-hacking-and-data-breaches-in-healthcare/
- The WannaCry (UK) and ASP (Italy) cases: Holding medical data hostage through ransomware: http://securehospitals.eu/2019/09/30/the-wannacry-and-italy-cases-holding-medical-data-hostage-through-ransomware/
- The Nansh0u campaign: Cryptojacking medical computing power: http://securehospitals.eu/2019/09/30/the-nansh0u-campaign-cryptojacking-medical-computing-power/
- The Evilnugget case: The potential for cyberespionage: http://securehospitals.eu/2019/09/30/the-evilnugget-case-the-potential-for-cyberespionage/
- Spoofing medical imaging: Highlighting security issues of malware: http://securehospitals.eu/2019/09/30/spoofing-medical-imaging-highlighting-security-issues-of-malware/
- The Barbie case (The Netherlands): GDPR and the mishandling of patient information: http://securehospitals.eu/2019/09/30/the-barbie-case-the-netherlands-gdpr-and-the-mishandling-of-patient-information/
- The UnityPoint Health breach: Phishing for sensitive information: http://securehospitals.eu/2019/09/30/the-unitypoint-health-breach-us-phishing-for-sensitive-information/
- Boston Children's Hospital (US): Hacktivism and DDoS attacks: http://securehospitals.eu/2019/09/30/boston-childrens-hospital-us-hacktivism-and-ddos-attacks/