Cyber Security for Europe

D9.2

Dissemination Material: Brochures, Posters

Document Identification	
Due date	31 May 2019
Submission date	
Revision	0.02

Related WP	WP9	Dissemination Level	PU
Lead Participant	UMA	Lead Author	Carmen Fernández (UMA) Javier Lopez (UMA)
Contributing Beneficiaries	UMA, TDL	Related Deliverables	D9.1

Abstract:

This deliverable describes the initial dissemination material that we have created for the purpose of communication and dissemination of CyberSec4Europe. In particular, we describe here the posters created at the beginning of the project, as well as the brochure and two different types of presentations.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

This deliverable describes the dissemination material created in the context of CyberSec4Europe for the purpose of communication and dissemination. The material described comes in different formats targeting different audiences and purposes: brochures, posters and presentations.

Document information

Contributors

Name	Partner
Carmen Fernández	UMA
Javier Lopez	UMA

Reviewers

Name	Partner
Alberto Lluch Lafuente	DTU
David Goodman	TDL

History

0.01	2019-05-15	Carmen Fernández, Javier Lopez	1st Draft and ToC
0.02	2019-05-27	Carmen Fernández, Javier Lopez	All sections contents completed

List of Contents

List of Acronyms

Glossary of Terms

1 Introduction

The communication strategy is one of the key building blocks of CyberSec4Europe. Thus, as a first stage of the communication process we have delivered some dissemination material that targets different audiences and fullfils different objectives in terms of communication and dissemination.
The first material we designed for CyberSec4Europe are the following:

- A brochure.
- A flyer
- Posters: a general poster, a poster for "Open Tools and Infrastructures for Certification and Validation", which corresponds to WP7 of the project, and seven posters, one for each of the demonstration use cases.
- Presentations: a short one to give an overview on CyberSec4Europe and a long one where we provide detailed information on the building blocks of the project and the demonstration use cases.

These three types of communication and dissemination material fulfil different purposes in terms of desired impact and audience. For this reason, we first identified the target audience for each of them.

2 Target Audience

The dissemination material described in this deliverable is going to be used at different venues and will be targeting different audiences.

In general, the brochure and the posters provide general information and, therefore, can be distributed at ICT and cybersecurity events to a technically-literate audience. The posters are aimed to be also used at specialized events devoted to the vertical domains of the respective demonstration demonstration cases they describe.

We have also created two presentations to be used with for different purposes and audiences – the one short and general whereas the other is customisable and potentially available to a more specialized audience interested in deep-diving into the project's technical details.

3 Dissemination Material

For the purpose of dissemination we created specific material to be used at events promoting the CS4E project. The first opportunity to make such material available was at the project kick-off meeting held in Brussels, 28 February and 1 March 2019. Going forward, we will provide both general and tailored material for both internal and external events, where the CyberSec4Europe partners are presenting either the whole or part of the project.

3.1 Brochure

The main purpose of the brochure is to inform a broad range of delegates at ICT- and, more specifically, cybersecurity-related events. In a leaflet format (i.e., folded A4), the brochure contains high-level information about the project that is intended to stimulate further interest and a desire to discover more, both about cybersecurity issues as well as about the project itself. The first page contains the project objectives and logo. The two central pages describe the main building blocks of CyberSec4Europe and the connections

between them. These building blocks are Governance design, from research to demonstration cases, where the demonstration cases are presented together with the research provided by them. Then, there are transversal building blocks such as Dissemination and communication and community building or Education and training that lays on all the other blocks. Finally, the last page includes contact information.

3.2 Flyer

The project created an A4 flyer on request for a project partner who had the specific requirement of having to impress upon a local administrative official of the importance of both CyberSec4Europe and the other three pilots for the purposes of getting his endorsement of a outward-facingproject concertation event. Hence, particular emphasis was put on highlighting the collaboration between the four pilots: Concordia, Echo and Sparta (see Annex II).

3.3 Posters

We created nine large (1.5m x 1m) posters for the initial purpose of introducing the project to the audience attending the public event during the project kick-off meeting. The intention was to attract interest in the project from specialists and non-specialists alike, from industry, local and national government, cybersecurity bodies and others, across a wide-range of subject material. The posters were designed in very large format to fit on whiteboards and to be visible at a distance, even across a crowded room, with appropriate project representatives standing in front of them.

The posters, which share a common design and format with the project logo at the top and the main contents below, are:

- One that captures the main objectives of CyberSec4Europe with a graphic overview of the relationships between the work packages (see Annex I).
- One that describes WP7, “Open Tools and Infrastructures for Certification and Validation”.
- One for each of the seven WP5 demonstration use cases: open banking, supply chain security assurance, privacy-preserving identity management, incident reporting, maritime transport, medical data exchange, smart cities.

For further use in other scenarios, the posters can be reduced in size, typically to A3.

3.3.1 Poster for Open Tools and Infrastructures for Certification and Validation

This poster contains basic information about the WP7 devoted to “Open Tools and Infrastructures for Certification and Validation”. The top right of the poster provides information related to timeline, leadership and partners involved. Then, the main body of the paper includes the distribution of the WP in tasks and the main objectives of the work to be done in this WP.

3.3.2 Posters for CyberSec4Europe Demonstration Use Cases

The posters for each of the seven demonstration use cases share some common features such as timeline, leadership and partners involved.

Then, in the main body of each poster we included the description of them following a basic structure:

- Objectives.
- Possible use cases that are identified for each of the demonstration cases.
- Expected impact, where we describe how the proposed technologies for each of the demonstration cases will aid to solve current problems.
- Challenges and cyberattacks that are to be overcome by the development of the research tools in WP3 for each of the cases
- And finally, contact information for each of the demonstration use cases.

See Annex III for two example posters.

3.4 Presentations

Given the large number of partners in the CyberSec4Europe consortium, it is particularly important that we deliver a common message no matter which partner goes to which event. For this reason, we have designed two types of Powerpoint presentations, which are to be used by all the CyberSec4Europe partners whenever they present the project or aspects of the project.

The short presentation contains information about the partners, the main building blocks, the main stakeholders and the relationships with the other three pilots: SPARTA, CONCORDIA and ECHO. It is expected that this material will be used to introduce the project to those who are not already familiar with CyberSec4Europe but have some familiarity with cybersecurity issues and the broad objectives of the European Commission in this regard.

In addition to including the material from the short presentation, the long presentation offers more detailed information about the objectives and outline of each of the work packages with detailed descriptions provided for the demonstration use cases as well as the communication and dissemination strategies addressed by CyberSec4Europe. The intention with this material is to provide components or building blocks that can be used and built on by partners from across the ten work packages for specific, technical purposes and delivered to reasonably technical audiences. It is also expected that partners will add new content to this set of materials, particularly as the project starts to deliver results, replacing older material which is largely based on the project proposal and the description of work. Consequently and over time, it may be prudent to break up this longer presentation into smaller components, based on the four general areas of the project.

4 Conclusion

In this deliverable we have described the dissemination and communication material currently in use by CyberSec4Europe partners. We have considered a brochure, a flyer, nine different posters for different purposes and two presentations, a short and a long one.

Over the course of the project, besides dovetailing with any material produced by or on behalf of the four pilots' communications group, we will continue to develop material that reflects both the project as a whole as well as the results and technical intricacies of individual work components, in collaboration with all consortium partners.

5 Annex I: Poster

6 Annex II: Flyer

7 Annex III: Posters

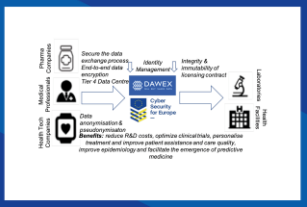
Cyber Security for Europe

[M01–M42] Lead ATOS Involved TUD, CYBER ATOS DAWEX DTU

Task 5.6

Medical Data Exchange

Expected Impact
- To valorise and so increase data exchange in the medical sector.
- To allow health players to minimize data transaction and data management costs.
- To facilitate obtained data to be translated into precise diagnosis, personalized preventive treatment, and ultimately more effective care.
- To allow players from the medical sector to exchange data in full security, compliance and trust.
- To benefit policy makers from insight into the types of systems and services required to support pan-European data markets.
- To provide industry with a blueprint of best cybersecurity and data protection practices and solutions, which different data sharing platforms can adopt (cross-border and cross-sector).



Objectives
Integrate and validate the research outcomes on the security and protection of sensitive and personal data for medical data sharing in a realistic environment (DAWEX Private Data Exchange platform).

Use Cases
- Development and roll out of tools and technology, tokeep up with evolving threats and to strengthen dataprotection in the medical sector, involving a large number of stakeholders and data sets.
- Provision of an environment compliant with the requirements of data regulations (GDPR and NIS) when sharing sensitive data, to remove frictions, obstacles and data exchange costs for users.

Challenges
When exchanging medical data, focus must be put on:
- Security and data protection aspects in the Dawex data marketplace to ensure trust between all parties, by guaranteeing their identities, and providing them legal functionalities and protecting citizen's rights.
- Guarantee the right data management from different sources (smart wearables, hospitals, laboratories, insurance companies, pharma companies, etc)
- Compliance with EU laws and regulations must be ensured (when non-EU companies).

More information
cs4ewp5t6@dlist.server.uni-frankfurt

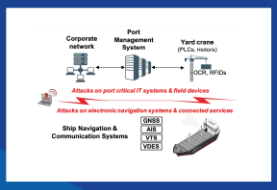
Cyber Security for Europe

[M01–M42] Lead UPRC Involved CYBER SINTEF UCY UPRC

Task 5.5

Maritime Transport

Related Cyberattacks
- Take control of CCTV port system
- Remote/nearby hacking of ship ICT and navigation systems
- Local/nearby attacks against port field devices
- Interception/manipulation of port-to-ship and ship-to-ship communication
- Disruption of the port supply chain
- Use social engineering to maximize the impact of a physical attack



Use Case
- Identify and deploy cybersecurity services for port and ship operators
- Examine system interconnectivity and the interdependencies between various systems both at the ship side and at the shore side
- Model cybersecurity threats and assess their risks.
- Design and develop a threat management system for continuously managing threats against critical maritime cyber infrastructures

Expected Results
- Threat management system capable of continuously managing cybersecurity threats against targeted critical cyber infrastructures at the maritime sector
- Novel threat modelling techniques capturing non-obvious security threats
- Advanced software-hardening techniques for legacy/IoT systems
- PKI services for maritime systems
- Advanced secure communications for maritime systems

More information
cs4ewp5t5@dlist.server.uni-frankfurt