Dissemination Activities Report v3

WP8– Dissemination, sustainability and exploitation

Version: 1.00

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

Disclaimer

Any dissemination of results reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Copyright message

© SPHINX Consortium, 2019

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

Document information

Grant Agreement Number	826183	Acronym	SPHINX
Full Title	A Universal Cyber Security Toolkit for Health-Care Industry		
Topic	SU-TDS-02-2018 Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures		
Funding scheme	RIA - Research and Innovation action		
Start Date	1st January 2019	**Duration**	36 months
Project URL	http://sphinx-project.eu/		
EU Project Officer	Christos Maramis (HaDEA)		
Project Coordinator	Dimitris Askounis, National Technical University of Athens - NTUA		
Deliverable	D8.6. Dissemination Activities Report v2		
Work Package	WP8 – Dissemination, sustainability and exploitation		
Date of Delivery	**Contractual** 36	**Actual**	36
Nature	R - Report	**Dissemination Level**	P - Public
Lead Beneficiary	ViLabs		
Responsible Author	Vasileios Voulgarakis	**Email**	vmvoulga@vilabs.eu
		Phone	
Reviewer(s):	Polaris Medical, HESE		
Keywords	Dissemination, Communication, Cybersecurity, Healthcare		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Document History

Version	Issue Date	Stage	Changes	Contributor
0.10	01/11/2021	Draft	ToC	Vasileios Voulgarakis (VIL)
0.20	05/11/2021	Draft	First Iteration	Vasileios Voulgarakis (VIL)
0.30	18/12/2021	Draft	Deliverable Preparation	Vasileios Voulgarakis (VIL)
0.40	22/03/2022	Draft	Deliverable Ready for Review	Vasileios Voulgarakis (VIL)
0.50	23/03/2022	Draft	Review 1	Sergiu Marin (Polaris Medical)
0.60	24/03/2022	Draft	Review 2	Ricardo Cabecinha (HESE)
0.70	28/03/2022	Pre-Final	Deliverable updated & Ready for QC	Vasileios Voulgarakis (VIL)
0.80	28/03/2022	Pre-Final	Quality Control	Michael Kontoulis (NTUA)
1.00	29/03/2022	Final	Final	Christos Ntanos (NTUA)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Executive Summary

SPHINX aims to introduce a Universal Cyber Security Toolkit, to enhance the cyber protection of Health IT Ecosystem and ensure the privacy and integrity of patients' data. The dissemination and communication of the project constitute a pivotal aspect of its overall planning, due to their role on promoting SPHINX's intentions, scope and contributions to the field of cybersecurity. Hence, the project adopted a multifaceted and detailed dissemination plan from the very beginning in order to:

- Create awareness about the SPHINX Solution benefits and opportunities.
- Increase engagement and encourage involvement of the target groups in the project activities.
- Ensure sustainability of the SPHINX targeted audience after the project's completion.

The present deliverable describes the progress and provides statistics of the dissemination and communication activities, both online and offline, during the entire lifecycle of the Project (M1-M36). This is the third and final version of the Dissemination Activities Report, a deliverable that was conducted in an annual basis.

D8.8 takes into account the input of the two previous reports and concludes on an overview of the Consortium's efforts to promote SPHINX scope and its results to the appropriate target audiences and engage them with the project.

The chapters below present the aggregated information and data regarding the visual branding of the Project, the website and the social media channels created for SPHINX, the networking activities of Consortium Members and the scientific publications of Project as well as the press releases, newsletters, videos, and blog entries produced.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Contents

1 Introduction 8
1.1 Purpose & Scope 8
1.2 Structure of the deliverable 8
2 Reporting Overview 9
2.1 Project Branding 9
2.1.1 Logo 9
2.1.2 Templates 9
2.1.3 Brochure 9
2.1.4 Infographic 10
2.1.5 SPHINX Flyer (Greek Version) 10
2.1.6 Videos 10
2.2 Online Metrics 10
2.2.1 Project Website 10
2.2.2 Social Media Accounts 12
2.3 Networking Activities 15
2.3.1 SPHINX Workshops 16
2.3.2 Synergies 18
2.3.3 Events organised by 3rd parties 20
2.4 Project Publications 21
2.4.1 Deliverable Reports 21
2.4.2 Scientific Publications 21
2.5 Media Content 23
2.5.1 Promo video for Pilot Cases (Greece) 23
2.5.2 SPHINX Toolkit Components Demos 23
2.5.1 Workshop Recordings 24
2.5.2 Pilots' execution Videos 24
2.5.3 Press Releases 24
2.5.4 Newsletters 24
2.5.5 Blog entries 24
2.5.6 Interviews 25
3 Summary Table M13 – M24 26
4 SPHINX dissemination and communication after the project's end 27
Annex I: Project Materials 28
I.1 Deliverable Template 28

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

I.2 Standardised Presentation 30
I.3 SPHINX Brochure 31
I.4 SPHINX Infographic 32
I.5 SPHINX Flyer (Greek version) 33

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

List of Figures

Figure 1. SPHINX Logo 9
Figure 2. SPHINX Symbol 9
Figure 3. SPHINX Website – Audience Overview 11
Figure 4. SPHINX Website - Audience Countries 12
Figure 5. SPHINX Facebook page 12
Figure 6. SPHINX Facebook Page - Followers Demographics 13
Figure 7. SPHINX Facebook Page - Followers Countries 13
Figure 8. SPHINX Twitter Account 14
Figure 9. SPHINX Twitter Account - Analytics Summary 14
Figure 10. SPHINX LinkedIn Profile 15
Figure 11. SPHINX LinkedIn Profile - Followers per Industry 15
Figure 12. SPHINX Workshop - CyberSec4Health 16
Figure 13. SPHINX Worlshop - CYBERAWARE4HEALTH 17
Figure 14. SPHINX Workshop - SPHINX4HEALTH 17
Figure 15. Article in Kathimerini newspaper 25

List of Tables

Table 1. SPHINX Total Events ..... **Error! Bookmark not defined.**
Table 2. SPHINX Total Scientific Publicaiotns 23

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

1 Introduction

1.1 Purpose & Scope

The present deliverable is the third annual report of the activities implemented by Consortium Members to disseminate and communicate SPHINX. This is the final version that entails descriptions and data regarding the progress of the defined dissemination and communication planning. Also, it critically analyses relative results throughout the whole project duration.

1.2 Structure of the deliverable

The Dissemination Activities Report v3, likewise the two previous versions, is structured to provide feedback on the dissemination and communication planning as it has been elaborated on the SPHINX's Dissemination Plan. Hence, the following sections are based on the content of D8.2. In this way, the current report aims to produce an accurate form of reporting which will be clearly aligned with the approach of the dissemination strategy of the Project. Below, the dissemination and communication activities of the Project are clustered in respective sections to assess their efficiency to meet the objectives of the dissemination strategy. This main part of the report is titled Reporting Overview. The deliverable concludes with a display of an aggregate table in which the objectives of SPHINX's dissemination strategy, as they have been derived from Project's Grant Agreement, are summarised, and presented.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2 Reporting Overview

2.1 Project Branding

This section is directly related to the plans made for the visual identity of SPHINX. The following actions have been carried out to create the visual cues of the project which would render SPHINX recognizable and promote a brand awareness about it.

2.1.1 Logo

ViLabs has delivered a logo version, on which the Consortium has agreed after majority voting to trademark project's work in any electronic and/or print material. Below there is the final version of the logo:

Figure 1. SPHINX Logo

Figure 2. SPHINX Symbol

2.1.2 Templates

Drawing from SPHINX's logo, a set of graphical templates have been developed to ensure a professional level of quality in terms of design and presentation in all project documents and communications. That is, Microsoft Word and PowerPoint templates have been designed and shared among the Consortium. These templates were used for all project's deliverables, reports, minutes etc. and whenever project partners needed to share specific information of the project in external events, such synergy workshops and/or conferences.

Those templates are presented in Annex I.

2.1.3 Brochure

A brochure was created for the first year of SPHINX as a complementary material to dissemination and communication activities of project partners. This offline material has been shared to stakeholders during varying occasions, where partners represented SPHINX. The brochure is also available for download at the project's website.

The brochure is available in Annex I.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2.1.4 Infographic

In order to deliver a comprehensive and well-rounded overview of SPHINX for the needs of multiple presentations, an infographic was crafted. The design depicts SPHINX's ID information such as project description, objectives, the pilot sites, consortium members, the proper declaration of EU funding by Horizon 2020 Research and Innovation programme and its duration. Moreover, the infographic depicts an easy-to-grasp design of the architecture of SPHINX Toolkit.

The full-size infographic is available in Annex I.

2.1.5 SPHINX Flyer (Greek Version)

During the first trimester of project's second year, a Greek version of an informative and awareness raising flyer was printed. The flyer was shared in the Greek pilot sites of SPHINX, that is, the premises of 5th Regional Health Authority of Thessaly and Sterea, the University Hospital of Larissa and the General Hospital of Volos in March 2020.

The action aimed at informing the medical and, even more, the administrative staff of the organisations about the day-to-day activities that they need to keep in mind to maintain a cybersafe work routine. Due to the Covid-19 pandemic and the overload of Healthcare Organisations, the action was not replicated at Romanian and Portuguese pilot sites as it was initially intended.

The full-size flyer is available in Annex I.

2.1.6 Videos

According to the Grant Agreement, the Project has had to create an initial video/slideshow during its first year, and the objective has been addressed by uploading SPHINX's first slideshow on the dedicated YouTube channel of the project. More information about videos produced by SPHINX is provided in the Media Content sub-chapter.

2.2 Online Metrics

The online dissemination and communication of SPHINX was based on two streams. On the one hand, project's website has been set as a point of reference and a source of information about SPHINX. On the other hand, the social media accounts of SPHINX have been drawing content from project's development and the activities of partners and promote it to varying audiences in a direct and engaging fashion.

2.2.1 Project Website

The project's website went live on March 2019, the third month of the project. It has been the major source about project's identity, goals and actions, from which every stakeholder category can be informed. In other words, SPHINX website has operated as a central dissemination and communication tool of the project providing the main results of the SPHINX research and outcomes. In particular, the SPHINX website has been used to:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

- Provide information about the project, its main objective, description of the produced toolkit and knowledge, publications, latest news and upcoming events in which SPHINX will participate, information about project partners and descriptions of related projects with a link to their websites, subscription to project's newsletter, social networks and contact info.
- Present information to stakeholders so that they will understand the reasons to get involved and how they can participate in the Project's activities.
- Provide a common reference for interested Stakeholders to all the produced content, including the SPHINX Solution, details of activities, etc.

During the lifecycle of the project, emphasis was put on creating diverse content to enrich the created pages and feature enough information for the multiple aspects of SPHINX. Notably, there were weekly blog entries on SPHINX's website, whose content derived from original work of project partners in their respective deliverable reports or from their dissemination activities (more information is provided in the Media Content sub-chapter).

The website is available at: https://sphinx-project.eu/

PROJECT LIFECYCLE ANALYTICS

The following data have been sourced from Google Analytics to assess the progress of the website throughout the project duration.

Overall, 11.128 users visited SPHINX website, while their majority were new visitors. Regarding their activity on the website, users engaged with SPHINX's content in a total of 14.588 sessions. Analytics define sessions as the period time a user is actively engaged with a website, app, etc. All usage data (Screen Views, Events, Ecommerce, etc.) is associated with a session. In this respect, each user averaged nearly one and a half sessions (1.31) and they viewed approximately 2 pages (2.19) per session, which lasted on an average of 2 minutes and 9 seconds. In sum, users who visited SPHINX website have recorded 31.958 pageviews.

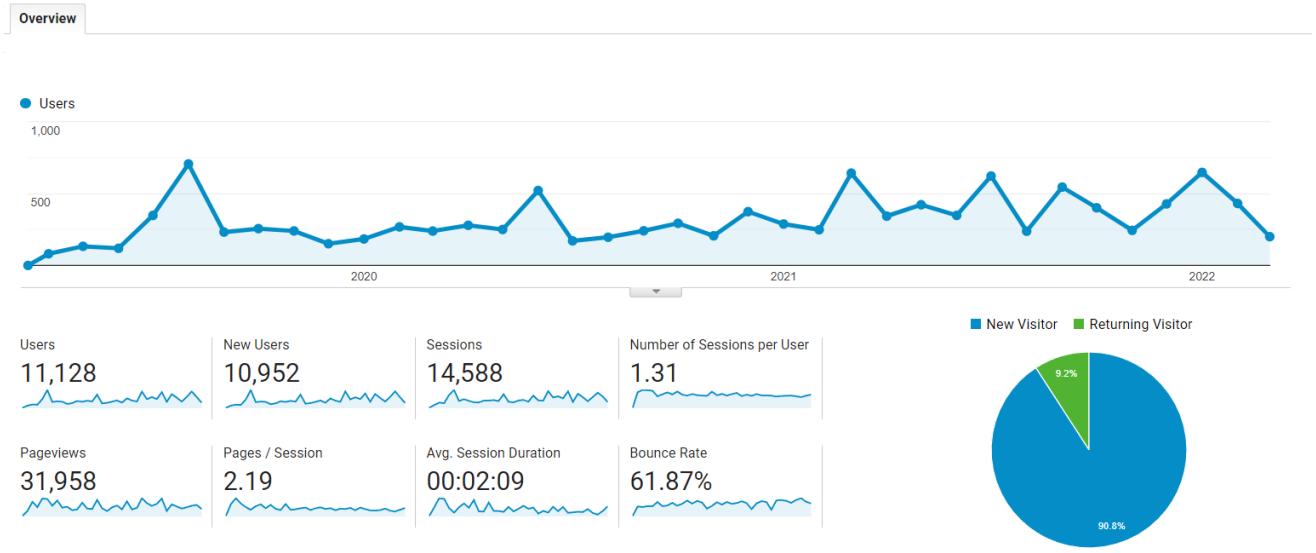


Figure 3. SPHINX Website – Audience Overview

Tracing SPHINX website audiences, Greece and USA are the two prominent countries from which users visited the project website, while users from additional EU countries, like Romania, Germany, Netherlands, Portugal and France are also identified.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

	Country	Users	% Users
1.	Greece	2,022	18.42%
2.	United States	1,956	17.82%
3.	Romania	546	4.97%
4.	Germany	434	3.95%
5.	Netherlands	421	3.84%
6.	United Kingdom	420	3.83%
7.	China	404	3.68%
8.	France	350	3.19%
9.	Portugal	341	3.11%
10.	Switzerland	309	2.82%

Figure 4. SPHINX Website - Audience Countries

2.2.2 Social Media Accounts

According to the dissemination strategy of the project, three social media accounts were set up, that is, a Facebook page, Twitter and LinkedIn profiles, as well as a complimentary YouTube channel. Using content that matches the structural affordances of each platform and features SEO characteristics (e.g., relevant hashtags) combined with the partners' already existing accounts, SPHINX accounts were leveraged to increase project's visibility in social networking sites.

ViLabs managed the social media accounts that were created for SPHINX project. Their content came mainly from project's website updates (i.e., a new blog entry posted every week in website and then promoted to all social media accounts) and from news about cybersecurity in healthcare. What is more, the social media accounts were used to promote further dissemination activities of SPHINX and other Synergy projects (i.e., newsletters, events, publications, etc.).

PROJECT LIFECYCLE ANALYTICS

Facebook

Figure 5. SPHINX Facebook page

The Facebook page of SPHINX, Sphinx-project.eu, has accumulated 737 followers. The daily activity of the page helped to increase the overall followership and grow a dedicated audience.

To understand the nature of the audience of SPHINX, additional data from 'Facebook Insights' tool were examined.

As a result, purposeful statistics about the project's Facebook page are elaborated.

Over the three years of SPHINX, the audience remained gender balanced within all the age cohorts (see Figure 4), while more than half of the followership came from Greece (See Figure 5).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

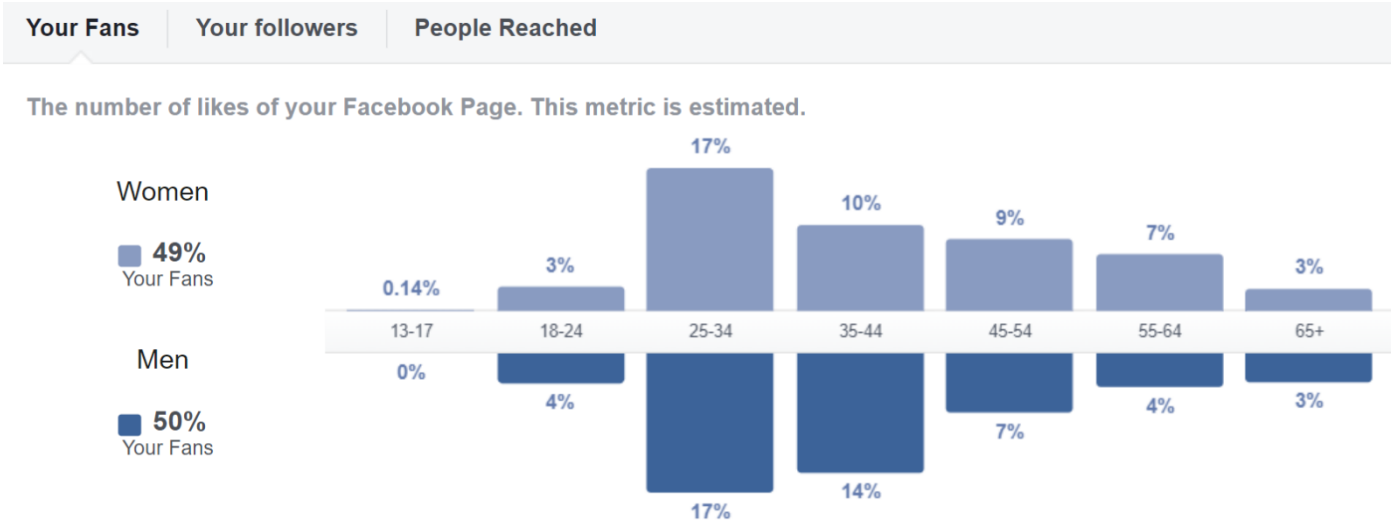


Figure 6. SPHINX Facebook Page - Followers Demographics

Country	Your Fans
Greece	435
Romania	40
Bulgaria	31
Albania	24
Ukraine	21
Serbia	19
Portugal	18
Kosovo	16
Germany	11
Bosnia & Herzegovina	10

Figure 7. SPHINX Facebook Page - Followers Countries

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Twitter

The @ProjectSphinx is the project's account on Twitter and stands as the most followed social media channel SPHINX with 809 followers.

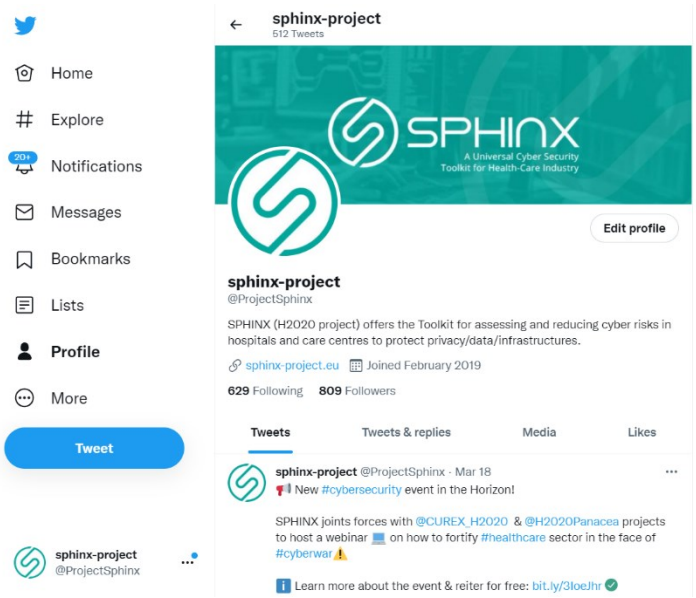


Figure 8. SPHINX Twitter Account

According to the Analytics service of the platform, the account has accumulated near to 280 thousand impressions and approximately 3 and a half thousand users visited SPHINX profile (see Figure 9). Hence the above, the daily update of the account with cybersecurity news and project's developments, likewise Facebook, resulted to a significant visibility of the project on this social network.

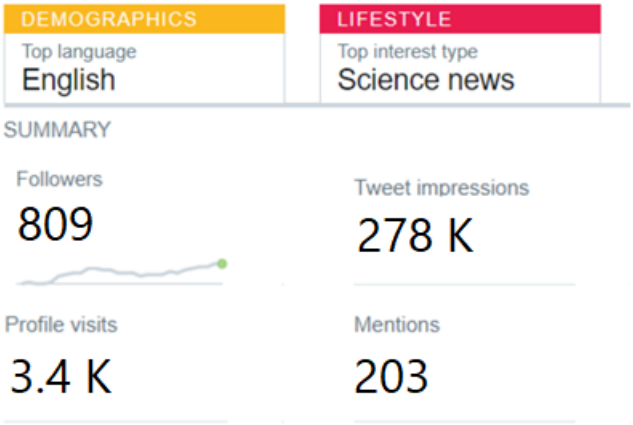


Figure 9. SPHINX Twitter Account - Analytics Summary

LinkedIn

The LinkedIn profile of SPHINX, titled sphinx-project, is the third social media account that the project has utilised. The scope of the LinkedIn profile is to address a smaller audience, yet more familiar with SPHINX's purpose. The reason is that the followers' background is more related to the cybersecurity domain due to their job functions. Overall, the followership of LinkedIn profile has progressed a small increase through year Two, reaching the 189 users.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

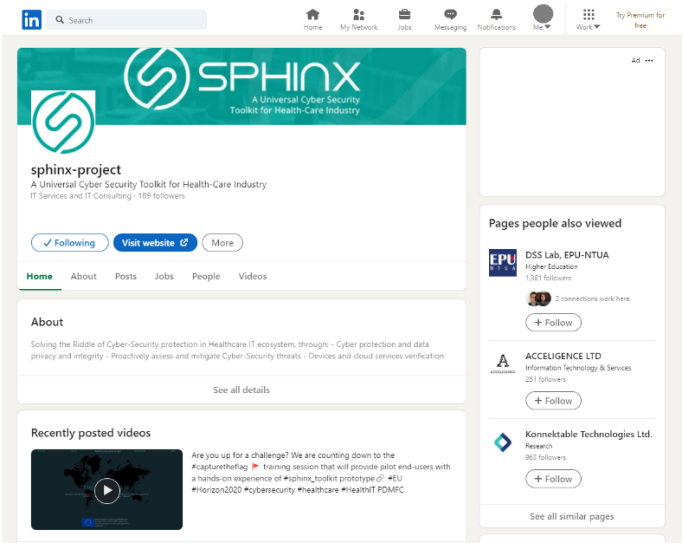


Figure 10. SPHINX LinkedIn Profile

What is more, the significant element of SPHINX's LinkedIn audience, lies, as argued above, to the professional domains, from which the followers come. As depicted in the Figure 11 below, many LinkedIn users that follow SPHINX project are employed in IT Services and/or Research domains. These statistics ensure that the cybersecurity updates and the posts about SPHINX development reached adequate stakeholder audiences.

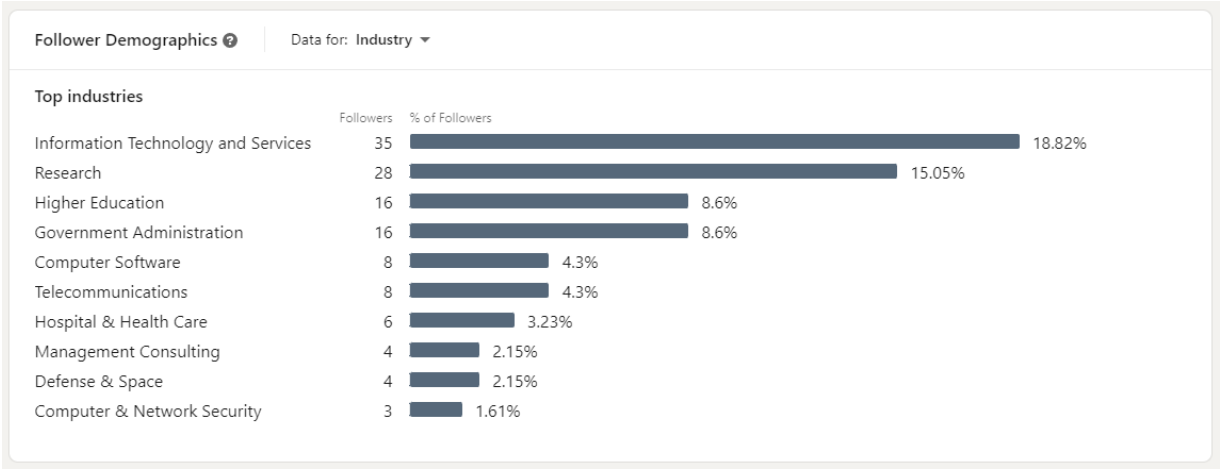


Figure 11. SPHINX LinkedIn Profile - Followers per Industry

2.3 Networking Activities

The networking activities have played a pivotal role on promoting SPHINX, as the participation and the contribution of partners to a series of real-life and virtual events led to fostering awareness among Stakeholder audiences. Despite that networking activities took a toll since several events were taken out of the schedule due to either postponement or cancelation as a result of the global circumstances related to the Covid 19 pandemic, SPHINX partners sought to represent the project on available virtual events. What is more, the project was able to organise its own online workshops and attract audiences consisting of IT experts employed in the broad Healthcare Sector.

Hence the above, SPHINX managed to stay active and in touch with its Stakeholder audiences.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2.3.1 SPHINX Workshops

In its first year, SPHINX organized a workshop on Cyber Security Situation Awareness for Health Organizations titled CyberSec4Health, which took place on 10th of July 2019, in Brussels, Belgium. The event's agenda consisted of four sessions; the first session focused on improving security of Health and Care services, data and infrastructure and featured the presentation of SPHINX scope followed by panel discussion. The next session was focused on a panel discussion about the reducing the risk of data privacy breaches caused by cyberattacks, while the following session actualised a series of training presentations about raising patients' trust and safety through legal and technological toolsets. The last session included a panel of four synergy projects discussing their projects and potential activities for collaboration.

Figure 12. SPHINX Workshop - CyberSec4Health

In the second year, SPHINX Consortium Member DYPE5, the fifth Greek Regional Health Authority, hosted a workshop that was dedicated to IT personnel of healthcare organisations in order to raise their awareness regarding contemporary cybersecurity matters. The workshop was titled CYBERAWARE4HEALTH and took place virtually on Wednesday, 16 December 2020. Partners from NTUA, PDMFC and ViLabs contributed to the event with presentations about information security, risk management, necessary daily actions for a cyber secure routine, firewalls concepts and the Sphinx Toolkit. These presentations were delivered in three sessions.

What is more, Mrs. Dimitra Livery, Network and Information Security expert of the European Union Agency for Cybersecurity (ENISA), gave a keynote speech on procurement guidelines for cybersecurity in hospitals and medical centres. The event gathered more than 100 attendees from several Healthcare Organisations, mainly from Greece, and from other countries of Consortium Members such as Portugal. The audience consisted of IT professionals, middle and high-level managers of IT departments, thus allowing the project to engage with an audience of potential end-users.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

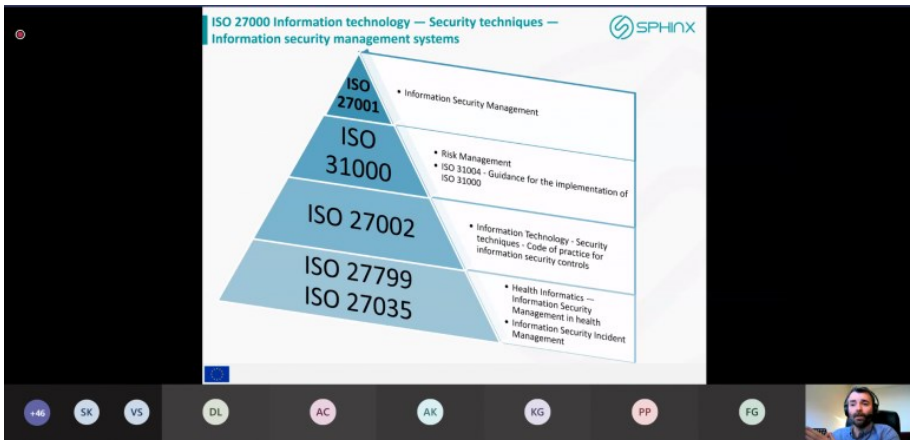


Figure 13. SPHINX Workshop - CYBERAWARE4HEALTH

In the third year, SPHINX partners from Hospital do Espirito Santo in Evora, Portugal (HESE), hosted an online workshop titled "SPHINX4HEALTH: The SPHINX Universal Toolkit for Healthcare Organisations" and featured keynote presentations from other members of the SPHINX Consortium. The event was organised on Wednesday, 6 October 2021, and partners from KT, HMU, SIMAVI, PDMFC, EDGE and Polaris Medical contributed presenting core aspects of SPHINX Toolkit proactive and reactive capabilities. Also, the workshop included presentations that explained SPHINX Toolkit deployment as well as its functional requirements.

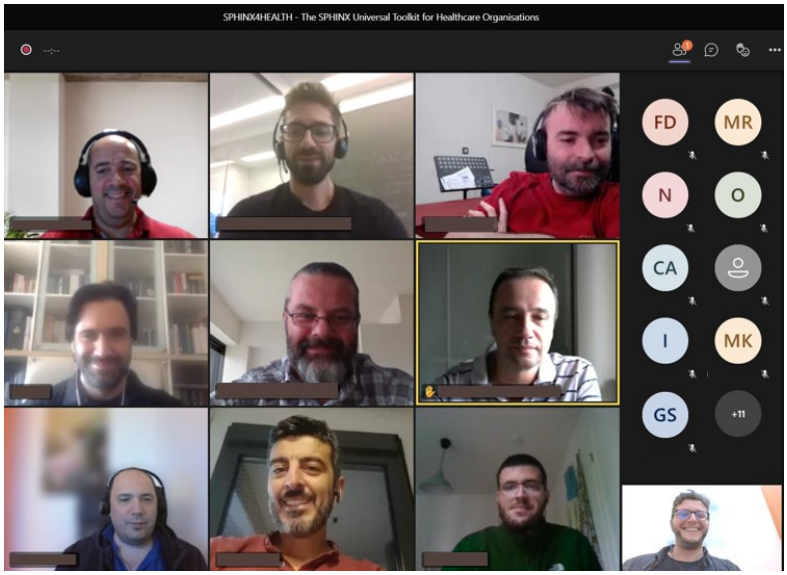


Figure 14. SPHINX Workshop - SPHINX4HEALTH

Finally, the fourth SPHINX workshop was organised early in 2022. The event was hosted by Polaris Medical and it was titled 'SPHINX@HEALTHSECURITY'. The workshop took place virtually on Thursday, 24 February 2022and the context was closely linked to healthcare top management and cybersecurity practitioners and IT experts who work on healthcare organisations. The event was dedicated to the outcomes of the SPHINX prototype testing in the 4 SPHINX pilot sites.

That is, the main part of the workshop included keynote presentations regarding the 3 pilot scenarios in which the components of the developed Toolkit have been deployed and assessed. In this context, the workshop also addressed the perspective of the Healthcare ICT domain regarding the pilot deployment which revolves around the lessons learnt throughout the process, best practices and key recommendations derived, as well as the actions taken in preparation for the pilot deployment like surveys and training for the ICT staff of the pilot sites. Furthermore, SPHINX@HEALTHSECURITY featured an overall technical presentation of the developed Toolkit providing information on its architecture, its components and their functionalities as well as the operating

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

modes of SPHINX. Finally, the workshop entailed a presentation about the exploitation options envisioned for the key results of the SPHINX Toolkit as well as its business model.

2.3.2 Synergies

2.3.2.1 H2020 Synergy

Since its early stages, SPHINX sought to engage with relevant H2020 Project and foster collaboration ties. Thus, SPHINX took part in events held by projects, which now constitute significant members of its network of Stakeholders. In particular, project partners carried through dissemination actions of SPHINX in the synergy projects' workshops listed below:

- Presentation of SPHINX project at the SAFECARE 1st Awareness Event in Leuven, Belgium **by ViLabs.**
- Presentation of how SPHINX is aiming to mitigate current cybersecurity threats at the PANACEA – 1st End users/Stakeholders Workshop in Rome, Italy **by NTUA and HMU**.
- Presentation about the meaning that healthcare carries in legal, ethical and security context and how SPHINX is projected to contribute to the domain of cyber-security of healthcare providers at the CUREX 1st International Workshop on Security and Privacy in Healthcare in Athens, Greece **by VUB.**
- Presentation about cybersecurity awareness among ICT staff in SPHINX pilot healthcare organisations at the synergy (CUREX, PANACEA, ProTego, ASCLEPIOS, and SPHINX) workshop on "Human-Centric Cyber Hygiene in Healthcare" held online, **by DYPE5** and contribution to the panel discussion **by NTUA**.
- SPHINX contribution as part of a projects' synergy to the 19th meeting of the eHealth Network, held online, **by NTUA**.

Furthermore, SPHINX has enrolled in the cluster organised by the H2020 Coordination and Support Action (CSA) SecureHospitals. This project constitutes an Open Awareness and Information Hub, whose aim has been to build a 'Community of Practice' platform where healthcare providers would be able to find information, awareness raising materials, training courses, as well as technical solutions and consultancy services dedicated to cybersecurity in healthcare settings, sourced by projects that are developing such products.

Finally, SPHINX collaborated with CUREX and PANACEA projects, as part of a joint initiative facilitated by the Horizon Results Booster platform. As a result, SPHINX co-hosted a webinar with CUREX and PANACEA as the 3 projects were approaching the end of their lifecycle. The event was called 'HSE cyber-attack: a wake-up call for hospitals right across Europe', its scope addressed the ransomware attack on the Irish national health service in May 2021 and elaborated on how CUREX, PANACEA and SPHINX solutions could be used not only to avoid similar attacks but also mitigate their impacts. The event, that featured also keynote speeches from representatives of DG CONNECT, ENISA, as well as the Health Executive Service of Ireland, reached a total of more than 200 participants from healthcare, cybersecurity agencies, government, academia and research domains. The webinar brought into spotlight lessons learnt by the impactful cyberattack in the Irish health sector, as well as the projects' consensus that more dedicated training, structural changes and investment are necessary to cover Healthcare's cybersecurity holistically and effectively.

In the aftermath of this event, the three projects have agreed to another synergy webinar, which is being prepared concurrently with this deliverable. This second synergy event is going to focus on cyber fortification in healthcare against hybrid threats and aims to elaborate on how Europe's critical healthcare infrastructure can be prepared to avoid and mitigate malicious acts of known origin that seek for disruption instead of blackmail.

The event will take place virtually on Thursday, 31 March, and it is directed towards policy makers of EU, top management of health delivery organisations and ICT systems and services providers. Leveraging the support

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

of Horizon Results Booster platform, a joint recommendations document is going to be drafted presenting key takeaways from the pair of webinars, as part of the provided services of the platform in the upcoming period.

2.3.2.2 ECSCI Cluster

Second, SPHINX has joined the cluster "European Cluster for Securing Critical Infrastructures" which is led by FINSEC, a security innovation H2020 project funded by the European Commission. The cluster has been organised to facilitate the relevant H2020 projects to join forces towards exchanging information about their produced results, sharing technologies and common approaches and managing a common dissemination and communication set of actions to reach a wider audience of Stakeholders in their relevant marketplace.

Following the introduction to the Cluster, SPHINX took part in the first online workshop of the Cluster along with ten more Horizon 2020 projects that are active on the broad sector of cyber and physical security of critical infrastructures across Europe. The workshop formally kicked-off the Cluster activities and its context referred to the different approaches on integrated (i.e. cyber and physical) security in seven different industrial sectors, that is finance, healthcare, energy, air transport communications, gas, and water. The peculiarities of critical infrastructure protection in each one of these sectors were discussed and addressed by the different projects of the ECSCI cluster that presented their outcomes, discussing the technical, ethical and societal aspects and the underlying technologies. HMU contributed to this synergy event representing SPHINX project.

Also, the project contributed to another online workshop that was co-organised by the Cluster. The event was titled "The 2nd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2021)" and it was co-located with the ESORICS 2021 conference. The workshop was dedicated to cyber-physical security for protecting critical infrastructures that support finance, energy, health, air transport, communication, gas, and water. The objective of CPS4CIP 2021 was to bring together security researchers and practitioners from the various verticals of critical infrastructures to rethink cyber-physical security in the light of latest technology developments, such as Cloud Computing, Blockchain, Big Data, AI, Internet-of-Things (IoT). PDMFC was the project partner that represented SPHINX in the event.

2.3.2.3 Cyberwatching.eu

SPHINX project established synergy with the **Cyberwatching.eu**, the European observatory of research and innovation in the field of cybersecurity and privacy. Funded under the European Commission's H2020 programme, Cyberwatcing.eu is an online portal that contributes to making the Digital Single Market a safer place by promoting the uptake and understanding of cutting-edge cybersecurity and privacy services which emerge from Research and Innovation initiatives across Europe.

As a result, SPHINX is featured in the research hub of Cyberwatching.eu managing its own dedicated project page. SPHINX page provides an overview of the project and informs the users about the expected impacts and the pilot actions planned. In addition, the page is used as an additional repository of SPHINX deliverables and videos. This way, project's results are visible to a broad community of experts, consisting of cybersecurity researchers, European project managers and Industry Stakeholders.

Additional actions stemmed from this synergy include SPHINX being presented in the Cyberwatching.eu in the special promotional section of 'Project of the Week' to increase its visibility inside the platform. In addition, the project has become member of the Cybersecurity and Privacy Health Cluster maintained by the same platform. Cyberwatching.eu, has clustered **active projects with similar aims** for lightweight synergies. This sub-cluster has been created according to the similarity of projects in their Marketing Readiness Level (MRL) at this point of their execution.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2.3.3 Events organised by 3rd parties

Despite the general slowdown to the organisation of real-life events due to the aforementioned Covid-19 pandemic consequences, SPHINX partners have worked to meet the requirements of the networking activities by representing the project in many virtual events in addition the face-to-face events.

Below, the events organised by third parties, where SPHINX partners participated are enlisted:

- Face 2 face meetings with targeted Stakeholders at the Health IT 2019 conference in Athens, Greece **by FINT and DYPE5.**
- Presentation of the 'Security Assessment as a Service Cross-Layered System for the Adoption of Digital, Personalised and Trusted Healthcare' at the IEEE 5th World Forum IoT in Limerick, Ireland **by EDGE and HMU**.
- Presentation of SPHINX's scope at the Conference, CIBTC Congreso Mundial Blockchain in Granada, Spain **by TECNALIA.**
- Presentation of SPHINX at the Conference, XIII Congreso Internacional de Ciberseguridad Industrial en Europa in Madrid, Spain **by TECNALIA.**
- Booth for the SPHINX project at the Convergence – The Global Blockchain Congress 2019 in Malaga, Spain **by TECHNALIA.**
- Workshop and presentation of SPHINX at the Conference, CIBTC Congreso Internacional Blockchain in Alicante, Spain **by TECNALIA.**
- Presentation of the Blockchain-Based Thread Registry Platform Blockchain at the IoT 2019: IEEE IEMCON 2019 in Vancouver, Canada during the Special Track on Integrating Blockchain and Internet of Things **by TECHNALIA.**
- Participation and Presentation of SPHINX at the Workshop, Social Lab 13: Secure Societies – 2nd Workshop by NewHoRRRizon in Brussels, Belgium **by EDGE**.
- Participation and presentation of SPHINX at the Workshop, Transformación Digital en procesos de Seguridad del Paciente y Seguridad Laboral in Bilbao, Spain **by TECNALIA.**
- Networking between Industry, Research Organisations and Policy-making Stakeholders during the SMI2G Brokerage Event in Brussels, Belgium **by EDGE**.
- Presentation of SPHINX solution to Policy Officers and Medical Sector representatives during the annual Greek HealthIT 2020 Conference held online **by DYPE5**.
- Engagement with Policy-making Stakeholders at Inception Meeting of the EU Health Information Sharing and Analysis Center (ISAC) held online **by DYPE5 and HES.**
- Participation to the XV International Industrial Cybersecurity Experiences Congress held online **by TECNALIA**.
- Networking between Industry, Research Organisations and Policy-making Stakeholders during the three rounds of ICT Verticals and Horizontals for Blockchain Standardisation roundtable discussions held online **by TECNALIA**.
- Promotion of upcoming SPHINX workshop during the Cyberwatching.eu webinar Security and Privacy by Design for Healthcare held online **by ViLabs**.
- Presentation of SPHINX project and the Portuguese pilot case in the 9th Value APAH Conference held online **by EDGE and HESE.**
- Presentation of papers conducted within SPHINX project in the IEEE International Conference on Cyber Security and Resilience (IEEE CSR) 2021 held online **by KT and PDMFC.**
- Paper presentation conducted within SPHINX project in the 25th Pan-Hellenic Conference on Informatics (PCI 2021) held in hybrid format, in Volos, Greece **by NTUA and PDMFC**.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Event	Count	Total
SPHINX Workshops	4	31
Synergy Events	9	
3rd Party Events	18	

Table 1. SPHINX Total Events

2.4 Project Publications

As a Horizon 2020 Research and Innovation Action, SPHINX, put significant effort towards knowledge diffusion. For this purpose, during the project lifecycle, the project has disclosed all the public deliverable reports conducted by the partners in adequate channels. What is more, multiple scientific publications have been elaborated in the context of SPHINX project.

2.4.1 Deliverable Reports

The dedicated SPHINX community in Zenodo was kept updated. That is, public deliverables were uploaded at the platform after their timely submission, to maintain the repository of technical and scientific knowledge produced by SPHINX partners.

2.4.2 Scientific Publications

Title of publication (Conference papers, peer-reviewed articles, book chapters, etc.)	Date of publication	Authors	Journal Publishing House	Status	Open Access
Security Assessment as a Service Cross-Layered System for the Adoption of Digital, Personalised and Trusted Healthcare	22 Jul 2019	Evangelos K. Markakis; Yannis Nikoloudakis; Evangelos Pallis; Marco Manso	IEEE	Published	Yes
Blockchain-Based Threat Registry Platform	19 Dec 2019	Santiago de Diego; Carlos Gonçalves; Oscar Lage; Jason Mansell; Michael Kontoulis, Serafeim Moustakidis; Barbara Guerra; Angelos Liapis	IEEE	Published	Yes
A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues	06 Jan 2020	Maria Stoyanova; Yannis Nikoloudakis; Spyridon Panagiotakis; Evangelos Pallis; Evangelos K. Markakis	IEEE	Published	Yes
Innovative Toolkit to Assess and Mitigate Cyber Threats in the Healthcare Sector (Book Chapter)	17 Sep 2020	Marco Manso; Barbara Guerra; George Doukas; Vicky Moumtzi	now publishers Inc. Boston - Delft	Published	Yes
A novel feature extraction methodology using Siamese convolutional neural networks for intrusion detection	14 Aug 2020	Serafeim Moustakidis; Patrik Karlsson	Cybersecurity Springer	Published	Yes

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Sandboxing the Cyberspace for Cybersecurity Education and Learning	24 Dec 2020	Stylianos Karagiannis; Emmanouil Magkos; Christoforos; Ntantogian; Luís L. Ribeiro	Springer	Published	Yes
Reference Architectures, Platforms, and Pilots for European Smart and Healthy Living—Analysis and Comparison	6 Jul 2021	Andrej Grguric; Omar Khan; Ana Ortega-Gil; Evangelos K. Markakis; Konstantin Pozdniakov; Christos Kloukinas; Alejandro M. Medrano-Gil; Eugenio Gaeta; Giuseppe Fico; Konstantina Koloutsou	Electronics	Published	Yes
The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular	July 2021	Dimitra Markopoulou; Vagelis Papakonstantinou	Elsevier	Published	Yes
Automated and On-Demand Cybersecurity Certification	6 Sep 2021	Stylianos Karagiannis; Marco Manso; Emmanouil Magkos; Luís L. Ribeiro; Luís Campos	IEEE	Published	Yes
Act Proactively: An Intrusion Prediction Approach for Cyber Security	6 Sep 2021	Panagiotis Panagiotidis; Christos Angelidis; Ioannis Karalis; George Spyropoulos; Angelos Liapis	IEEE	Published	Yes
Consolidated Proceedings of the first ECSCI Workshop on Critical Infrastructure Protection (e-book)	26 Sep 2021	Habtamu Abie, Davide Ferrario, Ernesto Troiano, John Soldatos, Fabrizio Di Peppo, Aleksandar Jovanovic, Ilias Gkotsis, Evangelos Markakis (Eds.)	Steinbeis-Edition	Published	Yes
An Intuitive Distributed Cyber Situational Awareness Framework Within a Healthcare Environment (book chapter)	15 Sep 2021	George Doukas; Michael Kontoulis; Sotiris Pelekis; Christos Ntanos; Dimitris Askounis; Yannis Nikoloudakis; Ioannis Kefaloukos; Evangelos Pallis; Evangelos K. Markakis	now publishers Inc. Boston - Delft	Published	Yes
Hospitals' Cybersecurity Culture during the COVID-19 Crisis	7 Oct 2021	Anna Georgiadou; Ariadni Michalitsi-Psarrou; Fotios Gioulekas; Evangelos Stamatiadis; ,Athanasios Tzikas; Konstantinos Gounaris; Georgios Doukas; Christos Ntanos; Luís Landeiro Ribeiro; Dimitris Askounis	Healthcare	Published	Yes

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

A-DEMO: ATT&CK Documentation, Emulation and Mitigation Operations: Deploying and Documenting Realistic Cyberattack Scenarios - A Rootkit Case Study	Nov 2021	Stylianos Karagiannis; Alexandros Tokatlis; Sotiris Pelekis; Michael Kontoulis; George Doukas; Christos Ntanos; Emmanouil Magkos	PCI 2021: 25th Pan-Hellenic Conference on Informatics	Published	Yes
A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures	Jan 2022	Fotios Gioulekas; Evangelos Stamatiadis; Athanasios Tzikas; Konstantinos Gounaris; Anna Georgiadou; Ariadni Michalitsi-Psarrou; Georgios Doukas; Michael Kontoulis; Yannis Nikoloudakis; Sergiu Marin; Ricardo Cabecinha; Christos Ntanos	Healthcare	Published	Yes

Table 2. SPHINX Total Scientific Publicaiotns

A significant accomplishment in regard to scientific publications has been the contribution of a chapter dedicated to SPHINX Toolkit in the publication of the Open Access book *"Cyber-Physical Threat intelligence"*. The book has been a collaborative outcome of a synergy between several European projects that are active on the board sector of cybersecurity for critical infrastructures. Overall, this synergy book has achieved a significant impact with quite more than 10,000 downloads (approx. 13,500 by the time this report is written).

The success led to the publication of the second volume of the book, titled "*Cyber-Physical Threat Intelligence for Critical Infrastructures Security"* on which SPHINX partners are contributed the chapter *"An Intuitive Distributed Cyber Situational Awareness Framework Within a Healthcare Environment"*, as mentioned in the table above.

2.5 Media Content

For the second year of SPHINX, the dissemination effort regarding media content creation has been placed mainly on the creation of plenty of blog entries to project's website; a task which derives from the target indicators of SPHINX's Grant Agreement.

2.5.1 Promo video for Pilot Cases (Greece)

In order to foster general awareness about SPHINX pilot demonstrations, the project has created a short promotional video. The aim of this activity is to inform medical and administrative staff of the pilot sites, as well as regional stakeholders about SPHINX project and its application, thus facilitating trust and potential uptake after project's completion.

To this end, the first video was created in the premises of University Hospital of Larissa, Greece which is going to be one of the infrastructures that the 5th Regional Health Authority of Thessaly and Sterea will provide for the Toolkit evaluation. The video is available at SPHINX's YouTube channel, and it is also featured at project's website on the Greek pilot page.

2.5.2 SPHINX Toolkit Components Demos

The project has put emphasis on knowledge diffusion and especially on disseminating technical information about what tools and methods are being utilised to set up the SPHINX Toolkit. Hence, after the completion of

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

the first iteration of the components that comprise the envisioned solution, a series of short presentations and demonstrations has been recorded.

Every component inside SPHINX's architecture has been presented in an approximately 5 minutes video by the respective project partner that is leading its development. The videos are accessible through project's website in a dedicated vault and through SPHINX channel on YouTube.

2.5.1 Workshop Recordings

Following the successful organisation of CYBERAWARE4HEALTH, SPHINX4HEALTH and SPHINX@HEALTHSECURITY online workshops, all the presentations have been uploaded at SPHINX YouTube channel into dedicated playlists, so that the content is openly available on demand. All the contributors have previously given their consent for this dissemination option.

2.5.2 Pilots' execution Videos

In order to afford external stakeholders, the opportunity to better grasp the concepts addressed by the pilot executions, 3 videos (1 video per pilot) were created. Each video presents the process flow of the corresponding pilot case explaining the hospitals' preparation. It, also, describes the type of the attack executed and how SPHINX tools were utilised to mitigate such attack. The videos conclude with lessons learnt and testimonials from the pilot end-users who participated. What is more, a complimentary video was created addressing the KPIs measured for each pilot case.

2.5.3 Press Releases

SPHINX has submitted two documents in the form of press release to the Community Research and Development Information Service (CORDIS). After the standardized peer review procedures of CORDIS the two press releases have been published at the platform. The first one, called 'A Universal Cyber Security Toolkit for Health-Care Industry', presents the project's identity and provides information about the Consortium Members. The second, called 'SPHINX project launched - A Universal Cyber Security Toolkit for Health-Care Industry' entails an overview of the objectives and scope of the Project.

In addition to the above, partners were encouraged throughout the project to spread the word about the SPHINX. In this respect, EDGE and SIMAVI published their own press releases after the approval of the dissemination management team. The former released a press release about the commencement of the project (link to EDGE's page) while the latter during its completion (link to SIMAVI's page).

2.5.4 Newsletters

Throughout the SPHINX duration, 5 newsletters were published according to the dissemination plan. The Newsletter subscription form is accessible in SPHINX's website, and it was initially circulated through social media channels of the Project. The Newsletter were sent to its subscribers through the MailChimp platform. The final pair of newsletter issues is going to be published within the next few months of the project's completion. The first one is going to feature the SPHINX's main outcomes at the end of the project, and the second one is going to be dedicated to the synergy with sister Horizon 2020 projects.

2.5.5 Blog entries

SPHINX has put significant effort to enrich the Blog section of its website making it a great resource of information about project's developments. Content was being added in a weekly basis and it was then promoted on project's social media channels. The blog entries mainly provided information from SPHINX public deliverables and, also, referred to SPHINX's presence in various networking events.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

By the time this report is being conducted, there are 95 blog entries on SPHINX's website dedicated page, thus reaching close to the overall expected number by the end of the project.

2.5.6 Interviews

TECNALIA's representative, Jason Mansell, provided an interview for Crypto Birds, a Spanish media platform that focuses on topics of blockchain and publishes a quite successful podcast show in Spanish. The interview was held in the context of the aforementioned Global Blockchain Congress, Convergence 2019, in Málaga, Spain. During this session Jason Mansell explained the particular contribution to cyber-security of Medical Sector that SPHINX is elaborating.

SPHINX Coordinators gave an interview in the Sunday edition of Kathimerini, one of the most prominent nation-wide newspapers in Greece, to promote the project's synergy with CUREX and PANACEA. The article focused on recent cyber-attacks against critical infrastructure and the healthcare sector in particular. The article referred to co-organisation of the synergy webinar focusing on last year's massive cyber-attack against Ireland's HSE. The news item showcased how EU funded research can help tackle one of the most challenging modern-day threats to knowledge, security and health.

Στόχος κυβερνοεπιθέσεων, εν μέσω πανδημίας, τα «ΕΣΥ»

Ευρωπαϊκό πρόγραμμα το οποίο συντονίζει το Εθνικό Μετσόβιο Πολυτεχνείο φιλοδοξεί να αναχαιτίσει τους απανταχού χάκερ

Της **ΙΩΑΝΝΑΣ ΦΩΤΙΑΔΗ**

Πώς θα νιώθατε αν ήσασταν ασθενής και σας ακύρωναν μία κρίσιμη εξέταση λόγω «έκτακτου τεχνικού προβλήματος»; Αν ήσασταν γιατρός και ξαφνικά χάνατε την πρόσβαση στο e-mail σας ή τους φακέλους των ασθενών σας; Τα παραπάνω δεν αποτελούν αποκύημα φαντασίας, αλλά πραγματικά περιστατικά που συνέβησαν σε Μεγάλη Βρετανία και Ιρλανδία έπειτα από κυβερνοεπιθέσεις στα εθνικά συστήματα υγείας. «Όταν οι κυβερνοεπιθέσεις γίνονται οργανωμένα και σε μεγάλη έκταση, στόχος τους είναι συνήθως οι κρίσιμες υποδομές των χωρών, όπως το δίκτυο ηλεκτροδότησης, τηλεπικοινωνίας και οι δομές υγείας», αναφέρει στην «Κ» ο δρ Χρήστος Ντάνος, διευθυντής Ερευνών στο Εργαστήριο Συστημάτων Αποφάσεων και Διοίκησης του ΕΜΠ. Το εν λόγω εργαστήριο συντονίζει το ευρωπαϊκό έργο έρευνας και καινοτομίας «SPHINX - A Universal Cyber Security Toolkit for the Healthcare Industry», το οποίο απαρτίζεται από δεκαεπτά φορείς, πανεπιστήμια, νοσοκομεία και εταιρείες πληροφορικής από εννέα χώρες της Ε.Ε.

Στόχος είναι η δημιουργία προηγμένων εργαλείων και μεθόδων προστασίας των νοσοκομείων από κυβερνοεπιθέσεις. «Η πιο συνηθισμένη και επικίνδυνη μορφή επίθεσης πλέον είναι η διασπορά ransomware, δηλαδή κακόβουλου λογισμικού που κρυπτογραφεί τα δεδομένα των συστημάτων και απαιτεί την κατάθεση λύτρων σε κάποιο κρυπτονόμισμα για να αποκρυπτογραφηθούν». Το πρόβλημα είναι πιο επίκαιρο από ποτέ, αφού οι απόπειρες κυβερνοεπίθεσης αυξήθηκαν παγκοσμίως περισσότερο από 50% μέσα στο 2021 – ενώ μόνο στον τομέα της Υγείας, ο οποίος λόγω πανδημίας δοκιμάζει τις αντοχές του, κατά 71%. Η νέα αυτή πραγματικότητα

Οι δράστες είτε εκβιάζουν απαιτώντας λύτρα σε κάποιο κρυπτονόμισμα, είτε «πρόκειται για κρατικούς ή παρακρατικούς φορείς, που συχνά φαίνεται ότι έχουν γεωστρατηγικά κίνητρα».

έρχεται να καταρρίψει τον μύθο του μοναχικού πλην ταλαντούχου εφήβου που πειραματίζεται στον υπολογιστή του. «Πρόκειται πλέον για οργανωμένες συμμορίες και κρατικούς ή παρακρατικούς φορείς, που συχνά φαίνεται ότι έχουν γεωστρατηγικά κίνητρα», διευκρινίζει ο δρ Ντάνος, συντονιστής του SPHINX. Η λεία τους δεν περιορίζεται στην... υποκλοπή του κωδικού στο e-banking μας, αλλά αποσκοπούν στον εκβιασμό, στην κατάρρευση ολόκληρων κρατών, ακόμα και στην πρόκληση θανάτων.

Η επίθεση με την υπαινικτική ονομασία «WannaCry», η οποία κρίθηκε από τις ΗΠΑ ότι προερχόταν από τη Βόρεια Κορέα, μόλυνε κάπου 200.000 υπολογιστικά συστήματα σε 150 χώρες, έπληξε όμως περισσότερο τη Μ. Βρετανία. Εκεί, παρέλυσαν περί τις 70.000 υπολογιστές, διακομιστές και συστήματα, όπως μαγνητικοί τομογράφοι, ψυγεία αίματος, μηχανήματα χειρουργείων στο Εθνικό Σύστημα Υγείας (NHS). Ασθενοφόρα έπρεπε να αλλάξουν προορισμό και νοσοκομεία να ακυρώσουν περίπου 19.000 ραντεβού ασθενών, θέτοντας έτσι σε κίνδυνο την υγεία, ακόμα και την επιβίωσή τους. «Το οικονομικό κόστος για το NHS μόνο από την απώλεια των υπηρεσιών κατά τη διάρκεια της επίθεσης υπολογίστηκε στα 92 εκατ. λίρες (110 εκατ. ευρώ), και αυτό χωρίς να υπολογιστούν τα επιπλέον 150 εκατ. λίρες (180 εκατ. ευρώ) σε επενδύσεις για τη διάσωση και τη θωράκιση των συστημάτων από επόμενες επιθέσεις», επισημαίνει ο δρ Ντάνος.

Η επίθεση στη Μεγάλη Βρετανία παρέλυσε περίπου 70.000 υπολογιστές, διακομιστές και συστήματα, όπως μαγνητικούς τομογράφους, ψυγεία αίματος και μηχανήματα χειρουργείων. Ασθενοφόρα έπρεπε να αλλάξουν προορισμό και νοσοκομεία να ακυρώσουν περίπου 19.000 ραντεβού ασθενών.

Η Ιρλανδία

Τον Μάιο του 2021, παρομοίως, η Αρχή Υπηρεσιών Υγείας της Ιρλανδίας (HSE) δέχτηκε ισχυρή κυβερνοεπίθεση (Conti ransomware), με συνέπεια να κλείσει το σύνολο των υπολογιστικών της συστημάτων και να ακυρώσει χιλιάδες ραντεβού ασθενών. Η επίθεση θεωρείται ότι προέρχεται από την ομάδα Wizard Spider που δρα από την Αγία Πετρούπολη στη Ρωσία. Εκλάπησαν ευαίσθητα προσωπικά δεδομένα ασθενών μαζί με εμπιστευτικά έγγραφα, τα οποία δημοσιεύθηκαν στο Διαδίκτυο για να πέσουν τις Αρχές να πληρώσουν τα «λύτρα». Η χώρα αρνήθηκε να υποκύψει στον εκβιασμό για να μην ενθαρρυνθούν περαιτέρω επιθέσεις στο μέλλον. Το κόστος της ζημίας υπολογίζεται σε πάνω από 500 εκατ. ευρώ.

«Είναι πολλά τα διδάγματα που πήραμε, πολλές είναι οι καλές πρακτικές που πρέπει να εφαρμόσουμε στο μέλλον», σχολιάζει στην «Κ» ο Peter Daly, επικεφαλής διαχείρισης εκτάκτων αναγκών της Αρχής Υπηρεσιών Υγείας της Ιρλανδίας. «Τα διοικητικά συμβούλια και η εκτελεστική ηγεσία των οργανισμών θα πρέπει να κατανοήσουν πόσο πολύ η κάθε μία λειτουργία (από την πιο απλή έως την πιο σύνθετη) εξαρτάται από την τεχνολογία. Θα πρέπει να ορίζεται σε κάθε οργανισμό ένα πρόσωπο επικεφαλής του προγράμματος κυβερνοασφάλειας».

Παραδόξως, η χώρα μας φαίνεται να βρίσκεται σε πλεονεκτική θέση. Με τον Ευρωπαϊκό Οργανισμό για την Κυβερνοασφάλεια (ENISA) να έχει την έδρα του στην Ελλάδα, με γραφεία στην Αθήνα και στο Ηράκλειο Κρήτης, η χώρα τοποθετείται στην κορυφή της παγκόσμιας κατάταξης του Εθνικού Δείκτη Κυβερνοασφάλειας (NCSI) της Ακαδημίας Ηλεκτρονικής Διακυβέρνησης (eGA).

Οι υπεύθυνοι των έργων SPHINX, PANACEA και CUREX καλούν σε συντονισμένη αφύπνιση τους πολιτικούς φορείς και τις διοικήσεις των νοσοκομείων. Τα τρία ευρωπαϊκά έργα, ολοκληρώνοντας τις εργασίες τους, ανακοίνωσαν –μέσω αρμοδίων– προημερών τα συμπεράσματά τους και παρουσίασαν πολλά νέα εργαλεία.

Τα εικονικά δολώματα

Η αυτόματη αξιολόγηση κινδύνου ασφαλείας στα συστήματα των οργανισμών μπορεί, για παράδειγμα, να εντοπίσει κενά ασφαλείας ή ρυθμίσεις που αφήνουν ανοιχτή κάποια «πόρτα» σε επίδοξους χάκερ. Στη φαρέτρα τους οι ερευνητές έχουν ακόμα... εικονικά δολώματα (honeypots) που εκπαιδεύονται με τεχνητή νοημοσύνη και υποδύονται ευπαθή συστήματα. «Εργαλεία, όπως απομονωμένου περιβάλλοντος (Sandbox) και προσομοίωσης δικτύων και επιθέσεων επιτρέπουν την εξοικείωση του προσωπικού ασφαλείας των νοσοκομείων σε περιβάλλοντα παρόμοια με αυτά που εργάζονται», καταλήγει ο δρ Ντάνος, υπενθυμίζοντας ότι εν προκειμένω ο ανθρώπινος παράγοντας παίζει πρωταρχικό ρόλο.

Figure 15. Article in Kathimerini newspaper

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

3 Summary Table M13 – M24

The following table is an aggerate outline of the dissemination and communication actions that were carried throughout SPHINX's lifecycle. This period corresponds to M1 – M36 of SPHINX and the clustering below is organised according to the goals setting included in the Grant Agreement of the project. The table summarises the information and data that are presented in the entire document.

Dissemination & Communication Objectives	Activity	Achievements	Grant Agreement KPIs
Create Project Identity and Branding	Project Logo, Colour Scheme, Templates	Logo and project template documents drafted	Revise Branding and Identity as required by project partners
Design Dissemination Materials	Brochure, Poster	Project Brochure created Infographic designed Flyer created Pilot Case Promo video published	Update materials according to project feedback. Create versions in other languages where possible with project partners.
Create Project Website	Website	Project website updated with further information about SPHINX aspects	Update the website with portal information and open data repository.
Social Media Strategy	Number of Video/Slideshow	33 Videos in Total 22 component demonstration videos, 19 project workshop presentations videos	YouTube - 3 Videos live w. 5000 hits
	Facebook Followers	737	5000 followers
	Twitter Followers	809	5000 followers - 1000 tweets
	LinkedIn Followers	189	N/A
Networking events and workshops	Total:	31	Attend and/or host up to 30 relevant networking events or workshops addressing the target communities, stakeholders and users.
	Organisation of a Workshop	4	
	Participation to 3rd part events (Conferences, Workshops, Exhibitions, Networking events, Symposia, Webinars, etc.)	27	
Generate positive media coverage & releasing project publications	Newsletter	5 Newsletters Published 2 Newsletters in the pipeline	7 Newsletters in Total
	Scientific and peer reviewed publication (article and/or papers and/or presentation)	15	11-23 Project Publications in Total
	Non-scientific and non-peer-reviewed publication (popularised publication) (Blog entries)	95	100 blog entries
Cluster with Relevant Projects & initiatives	Cluster with relevant projects and/or global initiatives	5 Sister H2020 Projects Member of ECSCI Clsuter with 20+ EU funded projects Member of Cyberwatching.eu platform Enrolled in SecureHospitals CSA	Cluster with 7 relevant projects or global initiatives in Total

Table 3 Objectives' KPIs achievements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

4 SPHINX dissemination and communication after the project's end

The current deliverable concludes with short section dedicated to future steps necessary to ensure that SPHINX stays relevant and impactful upon its completion. As the project comes to a full circle, a joint effort has been made by SPHINX partners to exploit and sustain its scope and produced results. In this sense, promoting SPHINX to target audiences and keep carrying out the above-documented activities play an essential role to promote SPHINX solution, as well as render it applicable to future research and innovation around the cybersecurity of the Healthcare sector.

Hence, the dissemination and communication of SPHINX will stay active utilising the following legacy options:

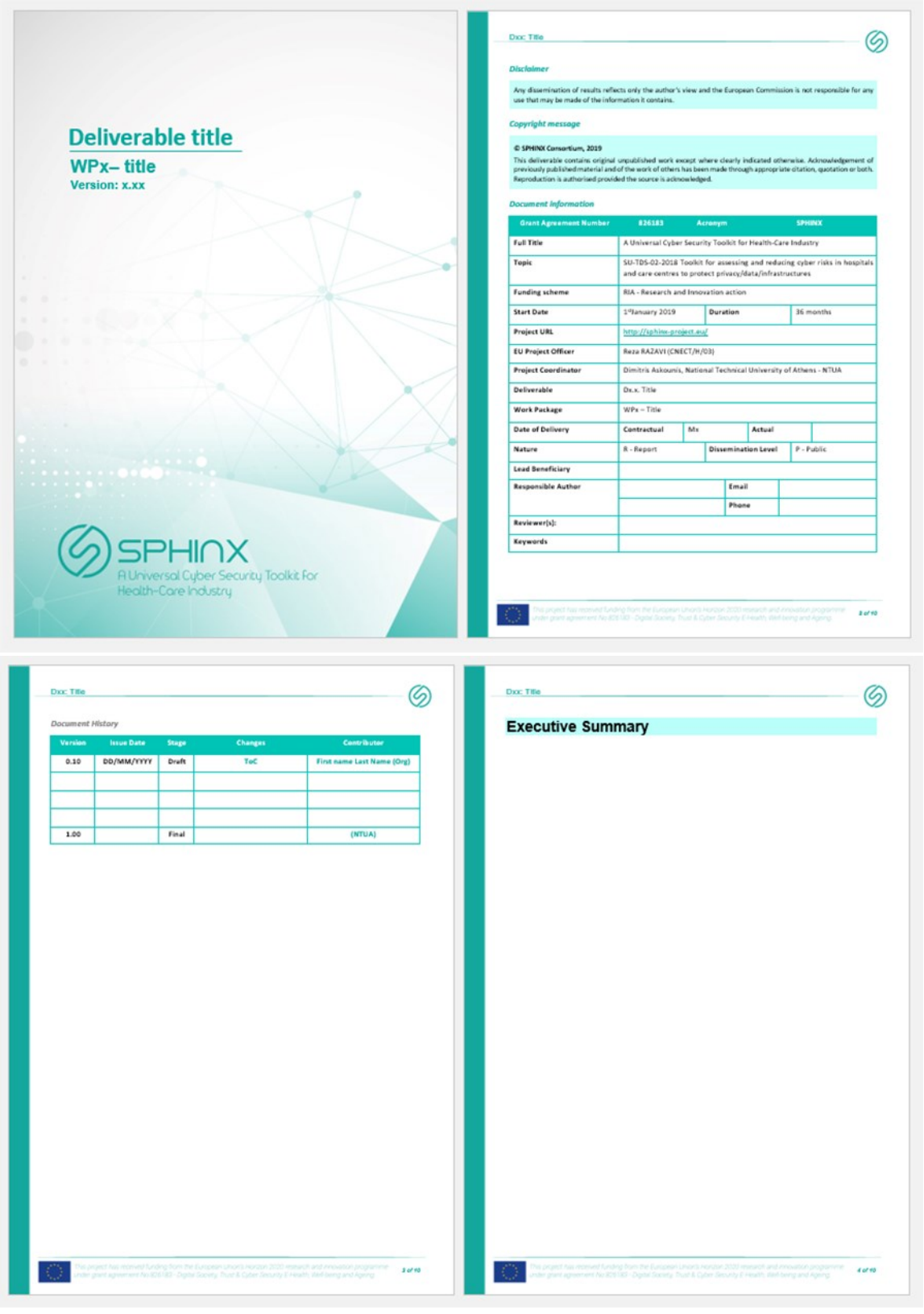
1. **SPHINX website:** The project's website served as the main hub of information and resources of the project. The website will remain online at least 3 years after the project's lifecycle. To do so, the website will be restructured focusing more to the Toolkits set up and offered capabilities. Information sections about SPHINX architecture and components will be further enhanced with the latest developments from technical partners and visitors will be able to easily contact each partner for in depth communications regarding the SPHINX Toolkit and/or individual components. What is more, the landing page will feature testimonials from SPHINX's pilot Healthcare IT end-users to highlight the value and purpose of the developed solution. Updated demo videos showcasing how SPHINX can be used and educational materials (e.g., user manuals) will be uploaded, with the overall goal to make the website more oriented towards the SPHINX Toolkit.
2. **Cybersecurity in Healthcare Working Group (SPHINX WG):** As proposed in D8.10 - Exploitation, Sustainability and Business plans v3, a Working Group can be set up consisting of individuals (under the umbrella of the SPHINX project) that are interested - from a scientific and practical point of view - on the topics that were addressed by the SPHINX. The SPHINX WG will be able to take up the results, continue working in the SPHINX area and focus on sustaining the SPHINX tools, through dissemination of project's results and findings to key stakeholders (e.g., scientific publications, conference contributions, recommendations and white papers), organisation of training programmes and seminars addressed to healthcare professionals (e.g., future SPHINX workshops and capacity building sessions) and transfer the acquired knowledge to future research projects (new proposals relevant to SPHINX's concept). The SPHINX WG will be able to use the project website as its main information hub, thus combining the visibility gained about its activities with the desired promotion of the SPHINX Toolkit solution.

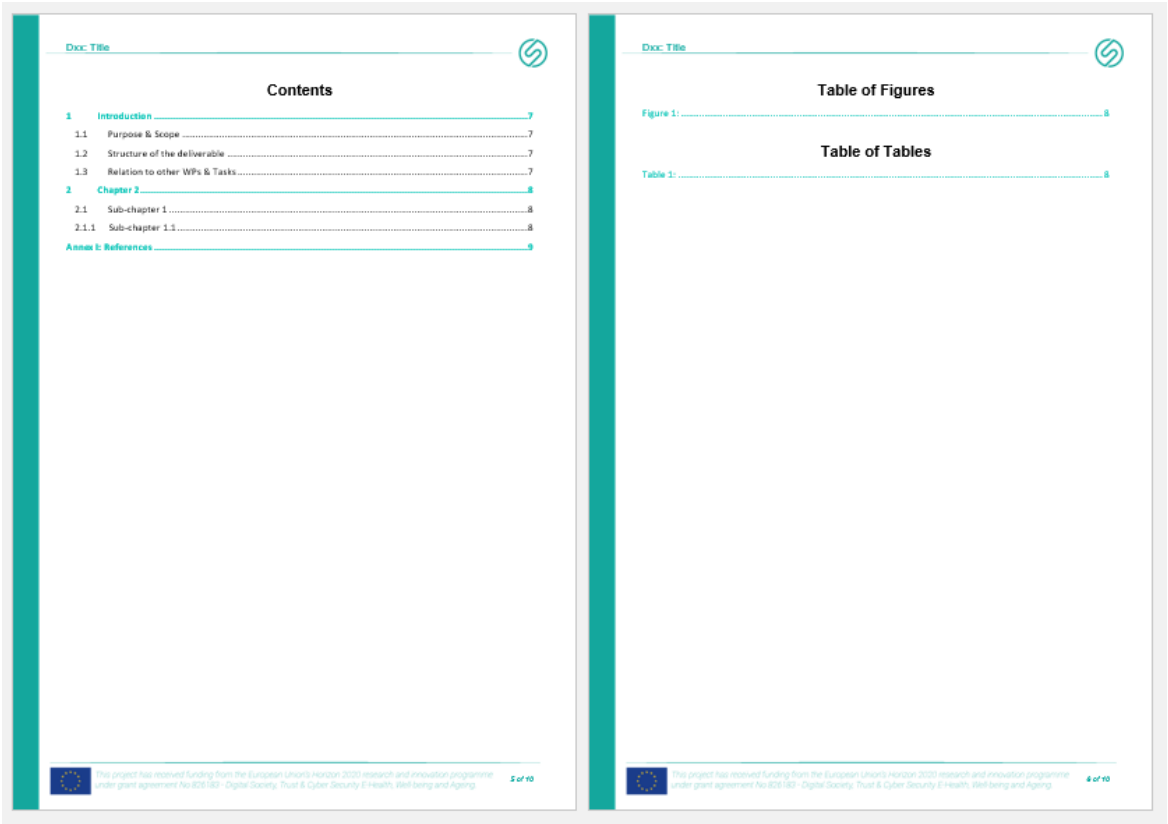
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

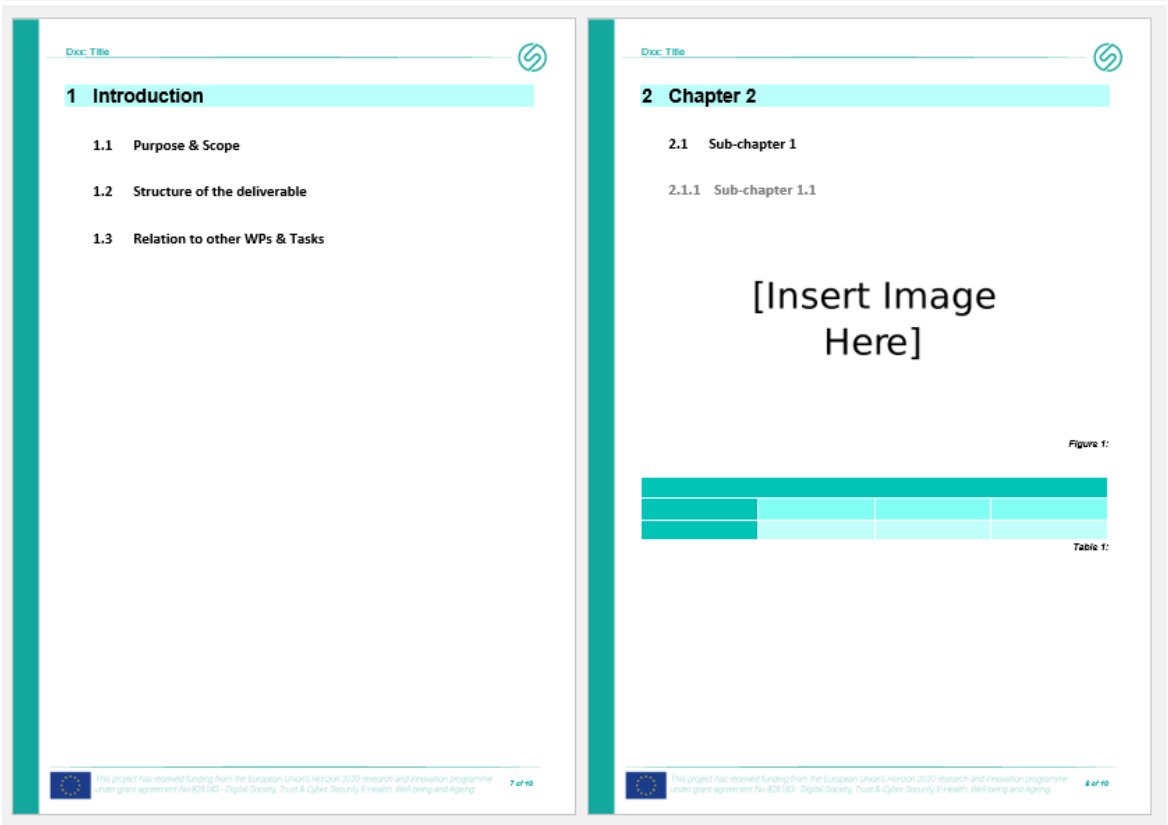
Annex I: Project Materials

I.1 Deliverable Template

Below a standardised format of a SPHINX's deliverable is presented. The captions show the features of the Microsoft Word Template that Project Partners use to conduct their scheduled deliverables.

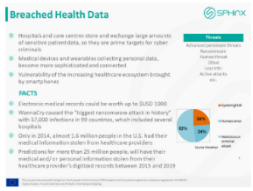


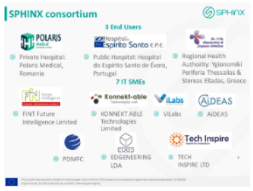

Doc: Title
Contents
1 Introduction 7
1.1 Purpose & Scope 7
1.2 Structure of the deliverable 7
1.3 Relation to other WPs & Tasks 7
2 Chapter 2 8
2.1 Sub-chapter 1 8
2.1.1 Sub-chapter 1.1 8
Annex I: References 9
5 of 10
Doc: Title
Table of Figures
Figure 1: 8
Table of Tables
Table 1: 8
6 of 10


Doc: Title
1 Introduction
1.1 Purpose & Scope
1.2 Structure of the deliverable
1.3 Relation to other WPs & Tasks
7 of 10
Doc: Title
2 Chapter 2
2.1 Sub-chapter 1
2.1.1 Sub-chapter 1.1
[Insert Image Here]
Figure 1:
Table 1:
8 of 10

I.2 Standardised Presentation

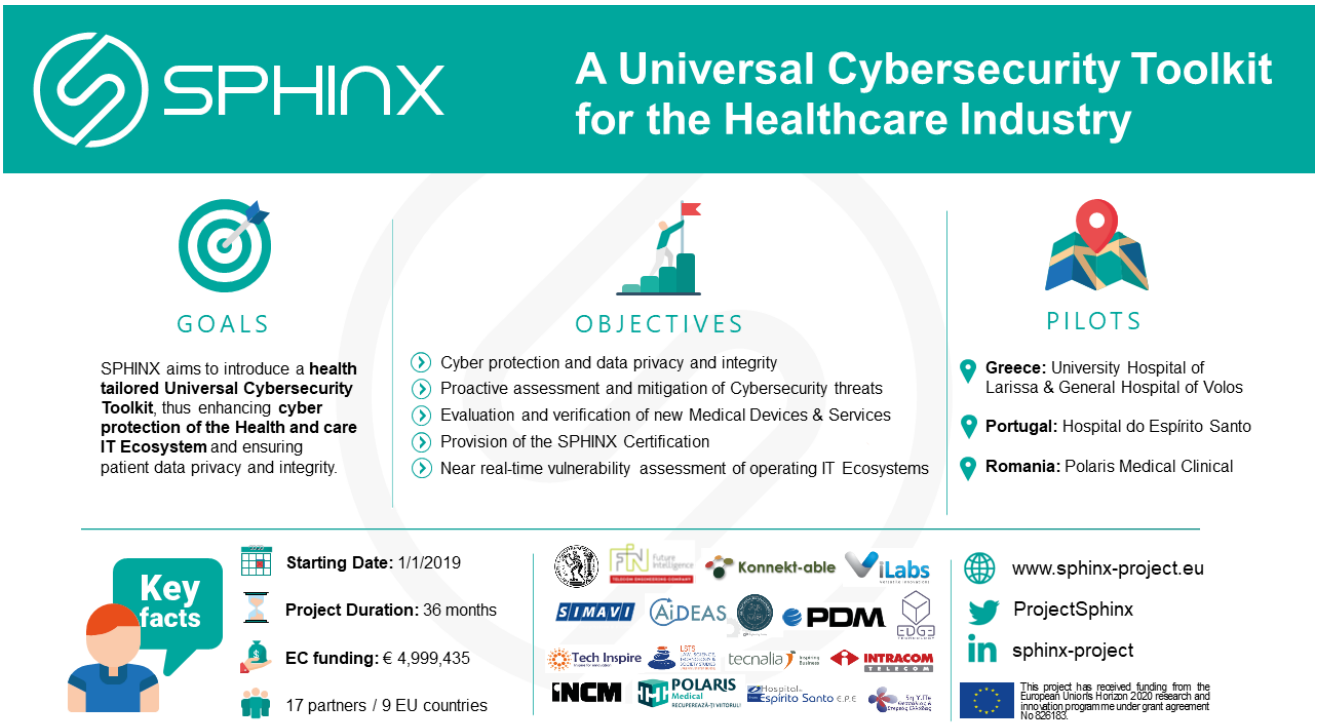
The following figure represents how a SPHINX's Project Presentation on Microsoft PowerPoint is formatted. Project Partners create their respective presentations according to the below format; thus a certain Template is shared.

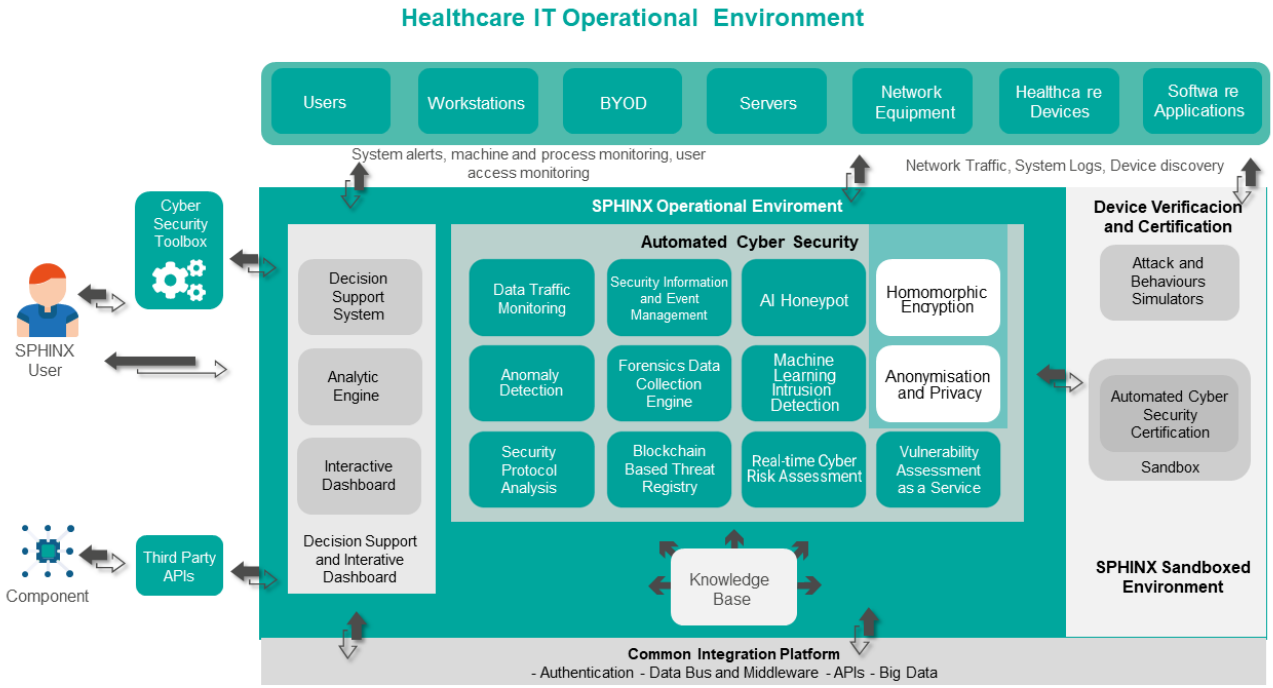
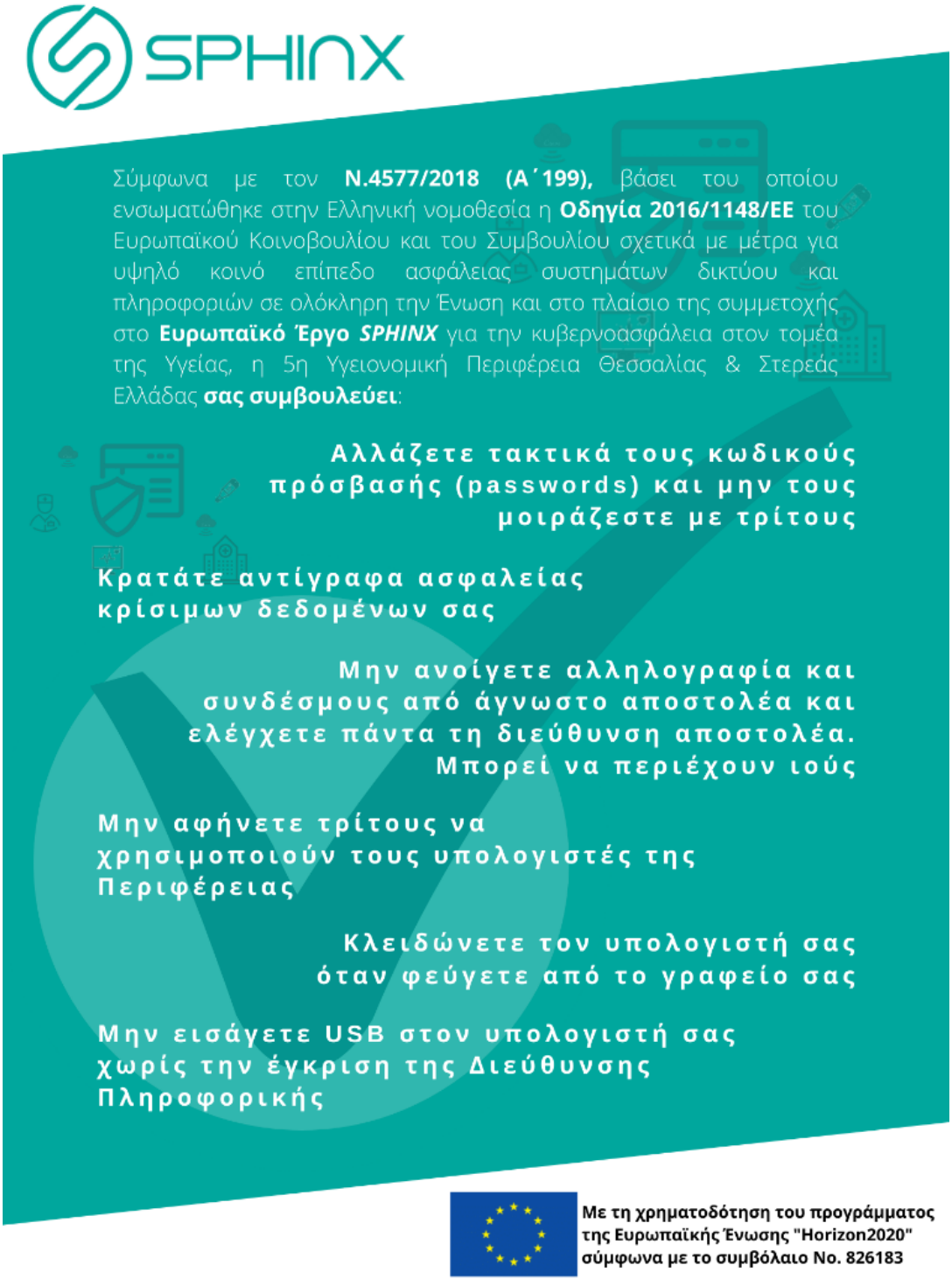




I.3 SPHINX Brochure

I.4 SPHINX Infographic





I.5 SPHINX Flyer (Greek version)