D6.7 Exploitation, dissemination and commercialisation report February 2019

Grant Agreement number:	740723
Project acronym:	CS-AWARE
Project title:	A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis
Principal author:	Christian Wieser, University of Oulu Contact: christian.wieser@oulu.fi
Additional Authors	Laurentiu Vasiliu (Peracton Ltd), Judi Blackmur (Peracton Ltd) John Forrester (CesViter),
Document version:	1.0

Table of Contents

Executive Summary

This deliverable of the CS-AWARE project is the second in an iterative series of three deliverables regarding the dissemination, exploitation and commercialization actions during the project lifetime. The following deliverable will constitute updated versions of the first iteration. Based upon the ongoing technology challenges and future market findings, the last version will be updated accordingly and commercialisation plans may be subject to variations or changes, depending on market needs and respective requirements.

The current deliverable consists of four principle chapters: An update of the dissemination plan & relevant actions, a commercialization & exploitation analysis updated, followed by considerations on future work.. It also provides an update on the various social media accounts the project is using, to assist with dissemination. With regards to exploitation and dissemination, this deliverable looks into the developed technology, then into the cyber-security industry and the market opportunity, examines practices of IP Policy and Strategies, and finally proposes the best licensing, revenue and commercialization path approaches. This part will be significantly enhanced during the second and third year of the project, while during the first year, will consolidate the main trajectory and approach.

1 Introduction

As we mentioned in the first version of this deliverable, cybersecurity is a challenging practice that impacts individuals and organizations. Cyber attacks have profound consequences for the business industry, whether organizations are the target, or the victim is the end user

CS-AWARE is an initiative to manage cybersecurity more effectively. The CS-AWARE solution entails a *situational awareness solution* that is meant for any size IT infrastructures of local public administrations (LPAs), (but also for other different markets such finance or health) in both technological realisation and business/market strategy. Advanced features like *information sharing*, *cyber-incident detection* or *self-healing* capabilities are being designd as part of the CS-AWARE offering.

To achieve the aforementioned goals of the project, we continue the dissemination plan we started at the beginning of the project and documented in the first version of this deliverable. The dissemination plan continues to run throughout the lifecycle of the project and will continue to be developeds concurrently with the commercialisation and exploitation plan..

2 Dissemination Plan and Actions

2.1 Dissemination Plan

The dissemination plan of CS-AWARE is has three bases: The first is associated with online dissemination and presence, the second with the development and production of classic marketing materials such as documents, posters and fliers and the third is related to direct marketing, by

presenting and organizing specific events such as seminars and workshops. Within the first 18 months of the project, all three bases have been developed and applied.

2.2 Website presence

The CS-AWARE website is online since November 2017 at https://cs-aware.eu/
We have received very good comments with regard to the web design and the clear message of the website. Since our last deliverables, there weren't made any major changes, except the blogs that have been continuously added since.

Figure 1. Landing page CS-AWARE website https://cs-aware.eu/

Figure 2. CS-AWARE project objectives

2.3 Social media presence

The Social media tools associated with the project were created and consolidated from the very first day.CS-AWARE has now an active presence on social media,.

1. Facebook account can be found at https://www.facebook.com/H2020.CSAWARE.CyberS3curity.Situational.Awareness/
2. Twitter account can be found at https://twitter.com/H2020EU_CSAWARE
3. You-tube account https://www.youtube.com/channel/UCQbnu8tb4zIW9u4_bKYAyMg

During the last year, as the technology has been in the process of design, we have tweeted and posted Facebook notes regularly, on matter of interest for our project and cyber-security community in particular. There were several project partners that had common access to the social media accounts and so, the inputs were varied and the contribution balanced.

2.4 Blog presence

The blog presence has been very dynamic. Since the beginning of the project, a goal has been set amongst consortium partners, to produce on a weekly basis a blog Currently, this goal stands and our latest blogs can be found on: https://cs-aware.eu/blog/

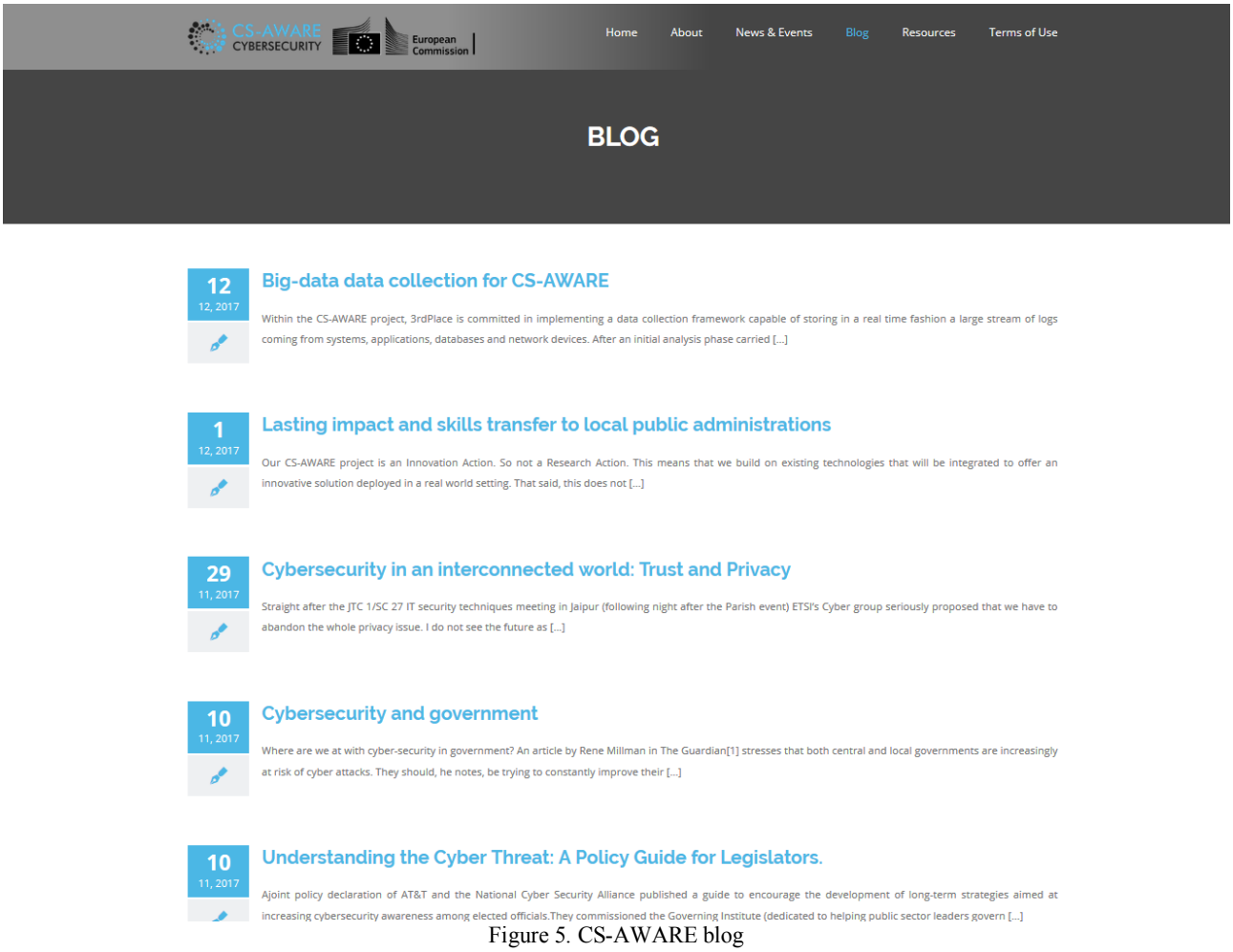

Figure 5. CS-AWARE blog

2.5 Leaflet and poster

A leaflet and poster were created describing the essence of CS-AWARE and are available for downloading on the CS-AWARE project website https://cs-aware.eu/documentation/ There has been no updates to the original produced material. Once a prototype is running we'll update the materials to reflect the progress.

2.6 Seminars and training

The list of seminars and training events (both past and future) in which our project has or will be involved for the period March 2018 – February 2019 are presented in the next table:

Name	Date	Link	Description
IPICS '18	2.7.2018 - 13.7.2018	https://summer-schools.aegean.gr/IPICS2018	The Intensive Programme on Information and Communication Systems Security (IPICS) academic summer school is a two-week course for undergraduate students in their final year, MSc Students, PhD students and IT professionals interested in a comprehensive overview and broad coverage of recent developments in "Information and Communication Security" . A workshop entitled "Soft Systems methodology in Action; CS-Aware a Cyber Security Awareness System" was presented on the second day of the programme. IPICS runs every year and has been hosted by a number of European universities (1998: Vienna, 1999: Uni Aegean - Chios, 2000: Stockholm, 2001: Uni Aegean - Samos, 2002: Samos, 2003: Malaga, 2004: Graz, 2005: Uni Aegean - Chios, 2006: Leuven, 2007: Glamorgan, 2008: Regensburg, 2009: Vienna, 2010: Uni Aegean - Samos, 2011: Uni Ionian - Corfu, 2012: Vienna, 2013: Uni Aegean Samos, 2014: Lesvos, 2015: Lesvos, 2016 Leuven, 2017: Uni Ionian - Corfu
CyberSec2018	15-17.5 2018	TBD	A dissemination event of the Erasmus+ strategic partnership project SecTech, which will be held in Vienna. The event will be organized in conjunction with CS-AWARE.
Dissemination events	2018.02.16 and 2018.03.08	TBD	Some dissemination events are being held in Roma Capitale, in order to train the internal employees on cyber security issues. The events are organized by the stable team of CS-AWARE

			project, that will be mentioned and described during the session.
Cyber Security Summit	2018.07.05	http://www.cybersecurityconference.co.uk/ http://www.cybersecurityconference.co.uk/presentations	Chaired by Baroness Kishwer Falkner was held in St Pauls London. Around 300 delegates, some from local and regional government, some from the security industry, heard thought-provoking presentations from Peter Yapp, Deputy Director of the UK's National Cyber Security Centre and Jon Ashton, Director of Cyber Security at Her Majesty's Revenue & Customs.
FOSSCOMM 2018	2018.10.13 - 2018.10.14	https://fosscomm2018.gr/index.php/front-page-en/	FOSSCOMM (Free and Open Source Software Communities Meeting) is the pan-Hellenic conference of free and open source software communities. It is addressed at programmers, students and anyone else interested in the open source movement, despite their background. Participating communities include the Hellenic Linux User Group (HELLUG), contributors of open source projects such as Mozilla, Fedora, OpenSuse, KDE and more. The content of the conference includes a wide variety of topics ranging from technical issues and workshops to translations, legal issues, political issues concerning open source software/hardware, etc. The attendance of the conference is *free of charge*.
10th OTS Forum	2018.11.29 - 2018.12.01	https://otsforum.gr/%CF%80%CF%81%CF%8C%CE%B3%CF%81%CE%B1%CE%BC%CE%BC%CE%B1/	The 10th annual OTS Greek Forum took place in Leptokarya, Katerini, where hundreds of representatives from Greek public organisations attended it (approximately 370 representatives, from over 90 public organisations, such as ministries, municipalities, regions, water utilities, legal public entities and academic institutions). The main agenda of the Forum was focused around innovative products and services that could improve the operation of public organisations. InnoSec and the Municipality of Larissa gave a joint presentation about the core functionality of CS-AWARE and the latest project developments. Emphasis was given on the added value it will have for LPAs IT staff, by giving examples of real issues faced on a regular basis by the Municipality of Larissa IT staff. It was

			then explained how the CS-AWARE system could assist in resolving the aforementioned issues.
Seminar in "Advanced topics in Web Science"	27.11.2018	http://www.fim.uni-passau.de/digital-libraries/studium-und-lehre/lehrveranstaltungen/	Advanced topics in Web Science - dedicated course for MSc students at the University of Passau on the application area of CS-AWARE under the theme "Modern practices for cybersecurity"
CrIM2018	31.10.2018-2.11.2018	https://www.oulu.fi/itee/crim	The international Crisis Management workshop CriM gathers teachers, researchers, experts and students of cyber security annually to study issues of security and privacy of our digital systems. Top international and Finnish lecturers combined with practical workshops bring important insight to students participating in the seminar. In the 2018 edition of the workshop, critical infrastructure and cybercrime will take the spotlight of the seminar: the resilience and security of our critical system, coupled with reporting and forensics systems and both the activity and changing form of cyber-crime cover a significant part of the lecture series. Additionally, the workshop looks on GDPR, on cryptographical solutions and at implications of different scoring systems in a digital society. For the first time, the seminar also contains a CTF competition, which permits the participating students to work on and practice their skills in testing information systems.
21st MDPS/IRIXYS Workshop	10.12.2018-14.12.2019	http://irixys.uni-passau.de	CS-AWARE project infodesk and booth for the participants (Professors, researchers and PhDs students from the INSA Lyon, the Università degli Studi di Milano and the University of Passau, as well as industry representatives).
FinTech Connect 2018	5-6 12 2018	https://www.excel.london/visitor/whats-on/fintech-connect-2018	It is the UK's largest and fastest growing financial trade show. Many companies from banking and finance industry were present there including tech companies, making it a very good environment to discuss the cyber security needs of the industry and see how CS-AWARE approach could fit

2.6.1 Publications policy

The publication policy remains unchanged since the last version. The entire project team will be acknowledged on all presentations and publications.

Authorship credit is based on a number of criteria:

1. Substantial contributions to conception and design, acquisition of data, or analysis and interpretation of data
2. Drafting the article or revising it critically for important intellectual content
3. Final approval of the version to be published.

Authors should meet conditions 1, 2, and 3. Lead and co-authorships will be determined based on the extent to which candidate authors meet the criteria described above. Further to this, lead authors will accept direct responsibility for the manuscript and will fully meet the criteria for authorship / contribution and will complete journal-specific author and conflict-of-interest disclosure forms.

The corresponding author, or for the purpose of presentations the presenting author, will normally be the lead author and will clearly indicate the preferred citation and identify all individual authors as well as the respective universities

Each author should have participated sufficiently in the work to take public responsibility for appropriate portions of the content.

Where a journal requests that one or more authors be identified as the persons who take responsibility for the integrity of the work as a whole, from inception to published article, then this person will be lead author.

The project team will jointly make decisions about contributors / authors before any manuscript is submitted for publication and this will subsequently be submitted to the Steering Committee for approval. The corresponding author / guarantor should be prepared to explain the presence and order of these individuals.

All contributors who do not meet the criteria for authorship should be listed in an acknowledgments section. Written permission must be sought from each individual so acknowledged.

It is a requirement that an acknowledgement of the financial contribution from the European Commission is included in all publications or presentations.

3 Commercialization and Exploitation Plan

3.1 Technology in the context of commercialization

Until recently cyber security was considered an issue primarily for IT. Now it has become an urgent agenda item for entire organizations. What has changed? It’s not only the increased number of reports

concerning cyber security breaches — if anything, these are merely symptomatic of a larger shift underway. Cyber-crime is fuelled by increasingly sophisticated technologies along with new trends in mobility usage, social media, and rapidly expanding connectivity — all very often in the hands of more organized online criminal networks. In this environment, an intelligent and evolutionary approach to cyber security is key to staying ahead of cyber criminals — and the competition.

3.2 Industry analysis

The basic issues of interest, relating to the EU Cybersecurity Market could be summarized as follow:

- **Market fragmentation**. – no update since last deliverable **Innovation influenced heavily by non-EU ICT products**. no update since last deliverable

- **Inconsistent transnational approach.** no update since last deliverable the EU industry to a globally competitive level.
- **Innovation & Finance.** A noticeably weak entrepreneurial culture combined with the overall lack of venture capital and seed money, underlines the need to seek other ways to support innovation. Furthermore, in the academia, there is no standard of minimum entrepreneurial support and spin-out methodologies across EU, as each university has its own particular entrepreneurial support approach to it that can vary widely from one corner to another of the EU. With Brexit, the departure of UK will considerably weaken the entrepreneurial culture in the EU space as UK is one of the most dynamic hubs of start-ups and entrepreneurial idea.

- **Anticipated support from public procurement not yet in place**. no update since last deliverable.

- **EU industrial policies not yet addressing specific cybersecurity issues.** no update since last deliverable **Cybersecurity and cyber defence**. no update since last deliverable **Sovereignty**. no update since last deliverable

- **Strategic autonomy** no update since last deliverable

3.3 Market opportunity

Given that the use of the internet and information and communication technologies (ICTs) is continuing to grow in every aspect of public and private sector activity, special emphasis needs to be placed on the establishment of a safe online environment, infrastructure and services, which will boost citizens' and public organizations trust, leading them to further use of new digital products and services. The economy, commerce and businesses increasingly rely on digital infrastructure for their further development. Public administration expects digital technology to become a means of improving the services provided and to lead to rational use of its information resources. Open and free internet access, and the confidentiality, integrity, availability and resilience of ICT systems are the basis for prosperity, national security but also for the safeguarding of fundamental rights and freedoms.

In the context of the present deliverable, a primary market analysis is been executed, focusing initially on the countries upon which the pilot implementation of the CS-AWARE will take place, those being Italy and Greece. On the second equivalent iteration of the deliverable (month 18), the analysis will be further updated with regards to those two countries, but also extended to the countries of the EU. Lastly, on the third deliverable a more global approach will be attempted.

3.3.1 Greek Market & Cybersecurity

Greece currently does not have a cybersecurity strategy or dedicated cybersecurity legislation. The legal and institutional framework that supports cybersecurity is also limited. According to the European Union Agency for Network and Information Security (ENISA) www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-securitystrategies-ncsss/national-cyber-security-strategy-3, Greece is in the process of preparing a cybersecurity strategy, through which the State's central planning with regard to cyberspace security is being developed.

There is however a Critical Infrastructure Protection (CIP) strategy - (Presidential Decree 39/2011 regarding critical infrastructure protection harmonizes Greek legislation with the European Union Directive 2008/114/EC on the identification, designation, and assessment of critical infrastructure. Furthermore, the Regulation for the Safety and Integrity Network and Electronic Communications Services 2013_addresses network-based and electronic critical infrastructure):

www.adae.gr/fileadmin/docs/enimerosi/sxedio_kanonismou_adae_asfaleia_akeraiotita.pdf

When it comes to accreditation and certification, the Regulation for the Safety and Integrity Network and Electronic Communications Services of 2013, specifically references EU and international standards for security certification and accreditation. It covers all ICT systems, critical infrastructure, and network and electronic communication services in Greece:

www.adae.gr/fileadmin/docs/enimerosi/sxedio_kanonismou_adae_asfaleia_akeraiotita.pdf

With regards to classification of data, Law 3649/2008 on the National Intelligence Service grants responsibility for the classification of government data to the National Intelligence Service (NIS) www.nis.gr . The NIS carries out classification according to a four-tiered system of classification.

As far as operational entities, Greece has established:

- A National Computer Emergency Response Team, responsible for coordinating incident response measures for both government institutions and entities engaged with critical public infrastructure.
- The Assurance Authority for Confidentiality of Communication (ADAE) which acts as the primary body responsible for network and information security.
- The National Intelligence Service of Greece (NIS) handles matters related to information and network security.
- The Directorate of Cyber Defence, responsible for cyber warfare and liaises with the NIS and the Greek police services.

- The Greek Cybercrime Centre, a national project aimed primarily at improving research and education in the area of cyberattacks. It does not handle network and information security at large.
- Lastly Greece has established an incident reporting platform for collecting cybersecurity incident data the NCERT-GR www.nis.gr/portal/page/portal/NIS/NCERT

On the negative side, there are no defined public-private partnerships for cybersecurity in Greece and no significant industry-led platforms for cybersecurity. Greece does not have sector-specific joint public-private plans in place and no sector-specific security priorities have been defined.

The Greek Public Organizations

An attempt of mapping the Greek public administration reveals a rather interesting market, where the services of CS-AWARE could be successfully implemented. Approximately, 965 public organizations constitute the backbone of the Greek administration. These could be categorized as follow:

- 325 Municipalities.
- 13 Regions
- 7 decentralized state administration units
- 18 Ministries
- 25 independent authorities (e.g. Regulatory authority for data protection, National Council of Radio and Television, the Hellenic Telecommunications & Post Commission etc.)
- 38 General Secretariats
- 173 Legal private law entities (e.g. Sports federations, the National Research Institution, Academic Research Institutions, the Institute of Chemical Processes & Energy Resources, the institute of sustainable mobility and transport networks etc.)
- 122 Social Service Providers (e.g. Museums, Cultural Institutions etc.)
- 264 Legal Public Entities (e.g. Hospitals, National Medicines agency, multiple chambers, academic Institutions, Water Authorities etc.)

Out of the totality of the aforementioned Greek public organizations, emphasis will be given to municipalities and regions with regards to promotion of CS-AWARE. Specifically, the Greek partners participating in the consortium, have an active clientele which extends to more than 80 municipalities and 12/13 Regions of Greece, from the upper pool of organizations. As in the case of Italy (described below), most municipalities in Greece are rather small in population and with limited resources. In order to have a rather representative utilization of the service, an initial commercial approach will include 3 small municipalities (with up to 25.000 registered citizens), 3 municipalities with up to 100.000 registered citizens (medium size) and 2 municipalities that are considered to be big in terms of population (more than 100.000 inhabitants). Ideally the approach will be done through the respective municipal unions. A significant factor that will be taken under consideration is the financial situation of the municipalities, without excluding though organizations with less funds, as they represent a rather significant portion of the pie. The purpose is to offer a multimodal solution that will cover the needs of various organizations. Lastly, an initial target will be set to introduce CW-AWARE to the systems of two Greek Regions.

3.3.2 Italian Market & Cyber Security

The Government in Italy has undertaken a number of steps to co-ordinate Cyber-security issues. However, there are not defined public-private partnerships dedicated to cybersecurity. The CERT-PA (at http://www.agid.gov.it/infrastructure-sicurezza/cert-pa) is charged with facilitating public-private information sharing to foster information exchange and the coordination of measures concerning cybersecurity incident prevention.

Currently there is no industry-led dedicated cybersecurity platform in Italy. The Italian Association of Critical Infrastructures' Experts (AIIC - at http://www.infrastrutturecritiche.it/alic-en) does work on providing an "inter-disciplinary approach to developing critical infrastructure strategies, methodologies and technologies" (BSA. Country Report - Italy). Since the AIIC is a non-profit association composed of primarily academic representatives, network provides, and other entities engaged with critical infrastructure, it exerts a limited influence on policy making at a national level. The ANITEC association (at http://www.associazioneanitec.it) is a representative body for information technology companies in Italy. Recently it merged with Assinform to create a unified association for firms in the ICT sector and consumer electronics. At times they deal with issues of cybersecurity but the focus remains broader on ITC firms in general.

No new public-private partnerships are being planned or currently being implemented for cybersecurity. Certainly the National Strategic Framework for Cyberspace Security (sicurezzanazionale.gov.it/sisr.ndf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pfg) focuses on public-private partnerships as occupying a central role in the future direction of cybersecurity in Italy. The Framework maintains that it is the intention of the Italian government to work closely with the private sector sharing information and collaborating in the areas of crisis management. Since there is no joint public-private sector plan concerning cybersecurity, many local governments are not actively involved in cybersecurity activities. The lack of cybersecurity policies and, in particular, public-private partnerships dedicated to cybersecurity has hampered the growth of a cybersecurity market in government.

Italy & Public Entities

The population of Italy is 60,589,445 (2018) and the total number of municipalities in Italy is 7958. Therefore, the average size of an Italian municipality is 7,614. Some 5,541 municipalities have less than 5,000 inhabitants; in other words, around 70% of Italian municipalities are very small in size. Many municipalities are pooling their resources to be able to meet increase public demands for expanded public services. Currently there are 537 municipal unions with 30,095 municipal members, that is, approximately 39% of the total number of municipalities. Only 17 of these unions have more than 100,000 inhabitants. 8 municipal unions have more than 20 municipal members. A target for the Project will be the 12 municipal unions that have more than 16 municipalities as members.

In these initial months of the Project it may be possible to find individual municipalities that are innovative enough to be possibly interested in being "early adopters". Beyond the more traditional role of our pilot projects these municipalities could be useful as further test sites for the Project. Potential markets will be, also, be found in the municipal unions noted above that have more than 16 municipal members. Even more interesting in terms of potential markets will be the metropolitan areas described above.

Going through national public procurement agencies in various EU states may be an additional means of reaching public entities. A summary of the agency in Italy (called Consip) is available at https://www.acquistinretepa.it/opencms/opencms/menu_livello_I/header/Inglese/PROGRAM.

3.3.3 Other markets

Though in the CS-AWARE project we accommodate only two pilots in Greece and Italy, it is obvious that the cybersecurity market is covering all countries of the Union and beyond. To this aim, and after the advice and support of our Project Officer, we are approaching Local Public Administrations in the member countries of the other CS-AWARE partners so that we will be able to broaden the field of applications to cover other pilot needs.

To cope with this challenge, we shall liaise with national or regional ecosystems that may involve also other entities from the public sector or from the industry.

3.4 IP policy and strategy

An underlying theme in any discussion of IP policy and strategy is the issue of open innovation. As an EU project we are expected, in part, to develop an "innovation ecosystem" that allows ideas and knowledge in the project to flow easily across boundaries. In a sense these concepts of open innovation and IP protection seem, as one researcher put, a paradox. Open innovation assumes "a willingness to allow knowledge produced within ..." to overflow to other entities whereas IP protections imply that certain ideas or technologies might excluded from use by others. It should be remembered that some of the world's largest patent holders (IBM, Microsoft, and others) have chosen to adopt "open innovation" models. In recent years IBM changed their corporate policy on the creation and management of patents, particularly relating to software and business methods. IBM established the Open Collaborative Research (OCR) program to support open-source software research between IBM and universities. Many attributes the transformation of Microsoft's IP strategy to the rise of open innovation and open source software. In Microsoft the idea of open innovation focuses on collaboration. Microsoft researchers are actively encouraged to collaborate with academic researchers and scientists, with government and industry partners, and Microsoft business groups across the world. Despite the shift in strategy neither of these 3 firms seems to have reduced its patenting activities.

As outlined in the Grant Agreement the Project will access resources from a range of partners and to ensure the compatibility of the Project's eventual products with others. Managing IP carefully will allow the Project to develop a trade in "technology that accompanies an open innovation strategy without destroying any competitive advantage they might have. Along with this trend towards "open innovation" more "markets for technology" have developed. Firms have become less vertically integrated firms as "specialized producers of technology no longer need to be housed with large vertically integrated firms in order to project and market their assets". While open innovation and an open source model should always be a firm commitment of the Project, the strategic use of IP will be critical for realizing the value of products produced by the Project. The IP strategy will be fashioned to take full advantage of the models of open innovation and open source in converting innovation in the Project in business value.

3.5 Licensing, revenue models and path to commercialization

Licensing

no update since last deliverable

Revenue Models

no update since last deliverable

4 Future Work and Next Steps

Given the economies of scale, it will be more efficient for us to select a small number of possible contacts in each country and work with the relevant local government association. Going directly to municipalities and other local governments would not be practical, both in terms of time and resources. It is usually more effective to work with interested associations who could in turn interest their members. The strategy behind any eventual marketing plan and business models should reflect a process of "indirect dissemination". - establishing a dialogue with a selected number of government associations in the countries of each partner. The content in terms of developing concrete business models will differ from country to country depending on the systems of government.

Each country has different systems of local government. Different models of participation in government are at play in each country. As we establish eventual business models, we need to keep in mind the dominant participation models in those countries and develop our models and campaigns in the light of the current dominant model. Over time success will not come from a successful contract or sale but from the impact of the innovations introduced by the Project on the user experience. We will be successful to the extent that we can persuade local government associations that what we are offering will have a positive impact on the experience of all stakeholders involved in local governments.

In the coming months, a list of national procurement procedures will be compiled. In recent years EU law established a number of public procurement rules. These rules are supposed to organize the way pubic authorities purchase goods, works and services. Once the rules are incorporated into national legislation, they apply to tenders whose monetary value exceeds a specified amount. Those tenders of a lesser amount are regulated by national legislation. In the initial phases and as we look for municipalities, associations, & others who may be interested in being "early adopters", we should be well aware of how the procurement rules work in each country. On a practical basis to exploit effectively economies of scale we should look eventually to developing business opportunities with larger public entities or associations. Probably the best place to start with for general information about public procurement in the EU is the survey: "Eu: The comparative Survey on Public Procurement systems across the PPN".

The focus in the following 18 months will be on the Spin-out set-up, commercialisation plan and the overall agreement, shareholding and licencing model between the consortium and Spin-out. Also, the direct sales path will be explored by partners in a parallel set-up that will not conflict with the Spin-out market plans.

We foresee the Spin-Out to be established in Finland. The reason being: Finland has a vibrant Start-Up scene and good support establishing Hi-Tech Start-Ups. Business Finland and Business Oulu – two governmental organizations – are our main supporters when we establish the Spin-Out.

References

Bianchi, Tiziana and Valentina Guidi. "The Comparative Survey on the National Public Procurement Systems Across the PPN". December, 2010. Authority for the Supervision of Public Contracts. Department for the co-ordination of European Union Policies. https://joinup.ec.europa.eu/document/eu-comparative-survey-public-procurement-systems-across-ppn

Bell, Mark. "Why adoption of an open source model is no excuse for ignoring patents", February 21, 2014. https://www.ibm.com/blogs/ip-management/why-adoption-of-an-open-source-model-is-no-excuse-for-ignoring-patents/

EU: The comparative survey on public procurement system acros the PPN, 31/12/2010 https://joinup.ec.europa.eu/document/eu-comparative-survey-public-procurement-systems-across-ppn

Hall, Bronwyn H. "Open Innovation and Intellectual Property Rights - The Two-edged Sword". https://eml.berkeley.edu/~bhhall/papers/BHH09_IPR_openinnovation.pdf

Kurth, Dale R. "Open Source Software: Key Steps to Avoid IP and Licensing Risks", June 27, 2012. http://www.industryweek.com/strategic-planning-amp-execution/open-source-software-key-steps-avoid-ip-and-licensing-risks

Masiyiwa, Tanya and Sunita Grote. "Open Source : Business Model", September 2016. Unicef Office of Innovation. http://www.unicefstories.org/wp-content/uploads/2016/12/Open-source-knowledge-product.pd

Van Hemert, Patricia, Peter Nijkamp, Enno Masurel. "From innovation to commercialization through networks and agglomerations: analysis of sources of innovation, innovation capabilities and performance of Dutch SMEs". The Annuals of Regional Science, April 2013, Volume 50, Issue 2, pp 425-452.