D6.2 Exploitation, dissemination and commercialisation report February 2018

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:	Laurentiu Vasiliu, Peracton Ltd, Contact: laurentiu.vasiliu@peracton.com
Additional Authors	John Forrester (Ancitel), Giuseppe Clementino (Ancitel) George Apostolopoulos (OTS)
Document version:	1.0

Table of Contents

Executive Summary

This deliverable of the CS-AWARE project is the first in an iterative series of three deliverables regarding the dissemination, exploitation and commercialization actions during the project lifetime. The following two deliverables will constitute updated versions of this first iteration and will be produced at month 18 (version 2) and month 36 (version 3) of the project's lifecycle. Based upon the technology challenges and future market findings this 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: A short introduction, a dissemination plan & relevant actions, a commercialization & exploitation analysis, followed lastly by some suggestions on future work. The document begins by presenting some early on dissemination activities (project website, social media presence and training materials for the CS-AWARE project) and then focuses on designing and consolidating the commercialization and exploitation analysis. On the dissemination side, it outlines the project website updates, the rationale and the type of information content that can be found on it, with selected screenshots of some pages illustrating the changes. 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 strongly developed during the second and third year of the project, while during the first year, will consolidate the main trajectory and approach.

1 Introduction

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 as the end user. Security controls such as usernames and passwords have become quickly outdated because they are widely used and exposed. Information on any type of storage, such as credit card data and health records, can turn into sources of exposure and stress for individuals upon malicious use, while in the case of organizations cybersecurity can have multiple repercussions such as loss of reputation, legal fines, sales and revenue decrease among others. Cybersecurity is such a hot topic that attracted the attention of European Union (EU) which caused the introduction of the Network and Information Security (NIS) directive that obliges member states to get in line with the EU cybersecurity efforts.

As an initiative to manage cybersecurity more effectively, the CS-AWARE project entails a *situational awareness solution* that is meant for small and medium-sized IT infrastructures of local public administrations (LPAs), in both technological realisation and business/market strategy. Advanced features like *information sharing*, *cyber-incident detection* or *self-healing* capabilities are within reach of this project.

To achieve the aforementioned project directions, we build upon the dissemination plan and actions that entail the communication channels selection to promote the existence and purpose of the

project. The dissemination plan that will run throughout the lifecycle of the project will be in parallel development with the commercialisation and exploitation plan. This type of plan aims to boost the visibility and practicality of the project deliverables and justify the purpose towards cybersecurity management.

2 Dissemination Plan and Actions

2.1 Dissemination Plan

The dissemination plan of CS-AWARE is based on 3 pillars: The first one is associated with online dissemination and presence, the second one with classic marketing materials such as documentation, posters and fliers and the third pillar is related to public impact, by presenting and organizing specific events such as seminars and workshops. Within the first 6 months of the project, all 3 pillars have been covered.

2.2 Website presence

The CS-AWARE website represents the main channel of displaying the project's progress. It was launched at the end of November 2017, after being approved by all consortium members. It can be accessed through https://cs-aware.eu/ , a domain specifically purchased for the CS-AWARE project.

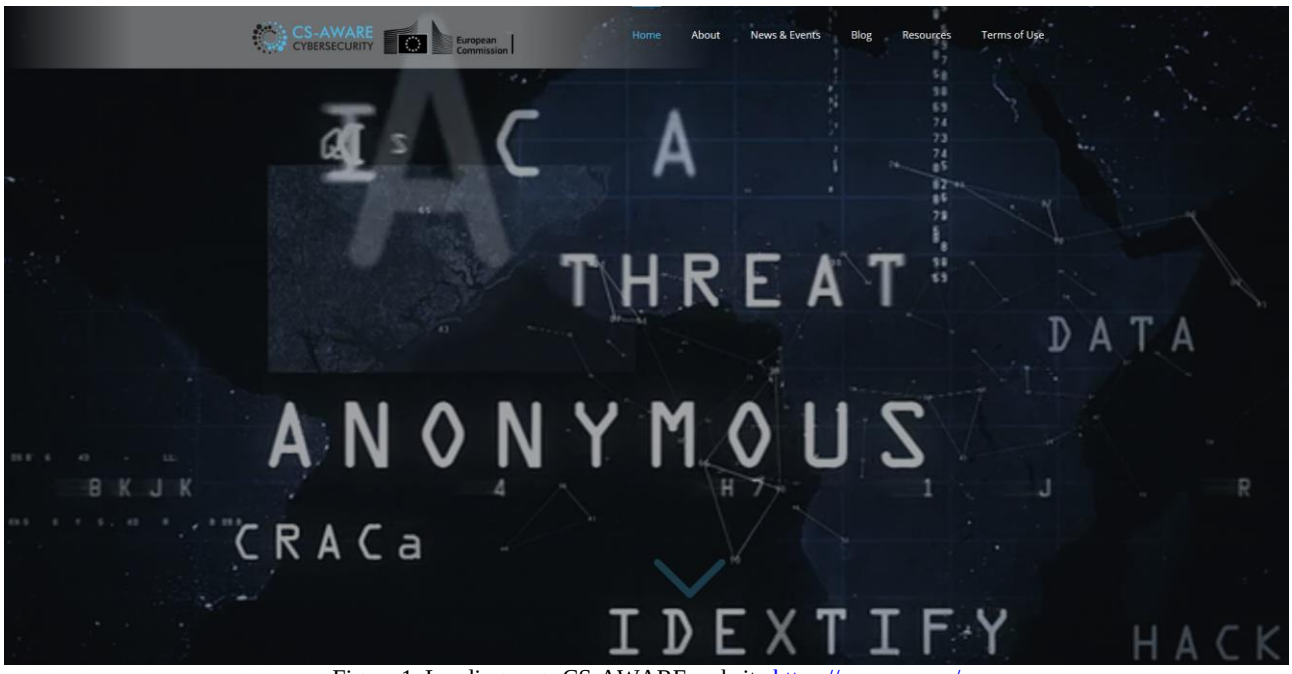

Figure 1. Landing page CS-AWARE website https://cs-aware.eu/

The website has features such as the European Commission logo on all pages, in-build encryption with 'Let's Encrypt' technology, as well as cookies compliance agreement in accordance with EU regulation. In addition, google analytics are installed to monitor the website's traffic and topics of interest.

There are several main sections defined at the top of the website such as 'About', 'New & Events', 'Blog', 'Resources' and 'Terms of Use', that capture all the content related to the website. The project partners are all listed at the bottom of the website by their logos and they can be found with their full description in the About/Partner section, while below there is an open contact form available to anyone

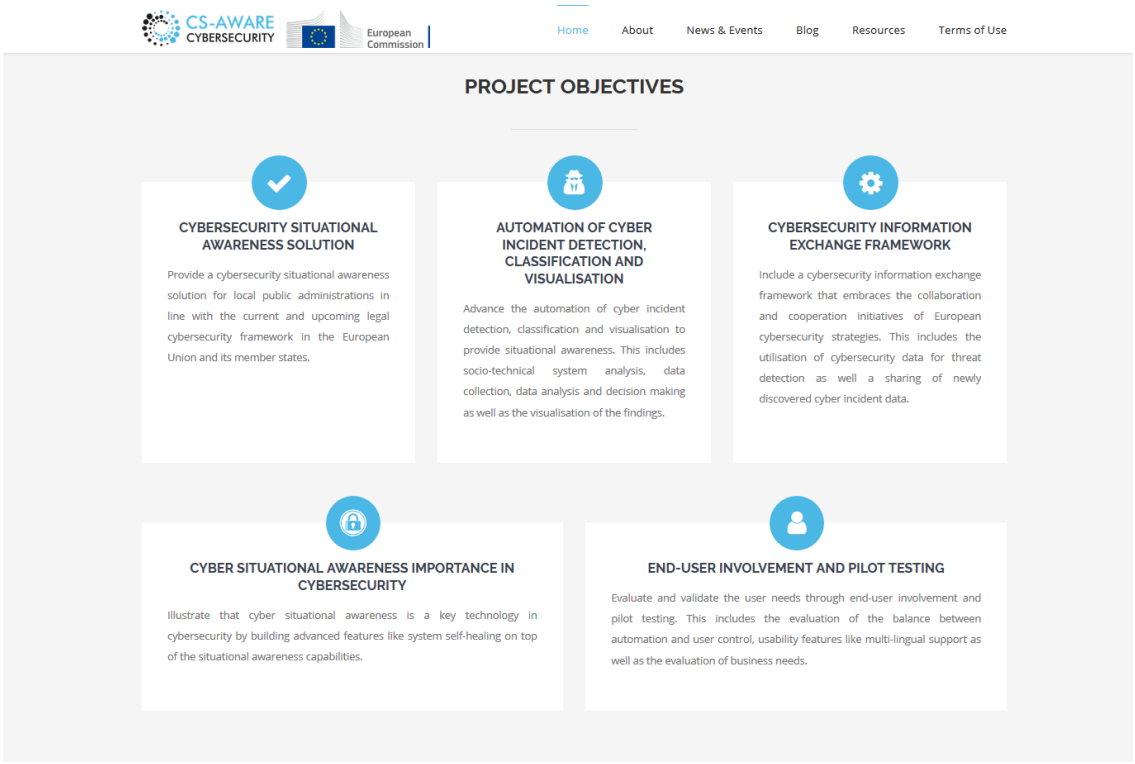

Figure 2. CS-AWARE project objectives

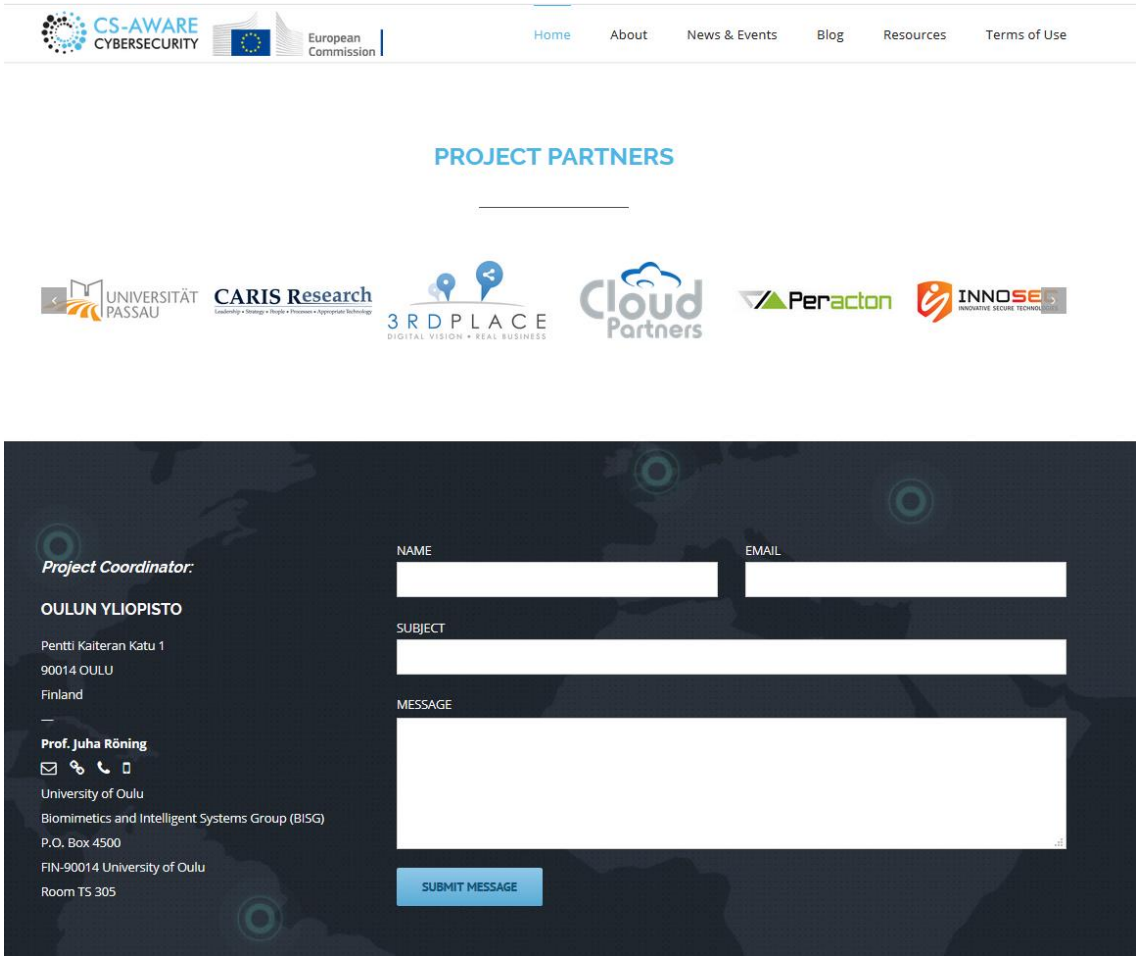

Figure 3. CS-AWARE partners and contact form

Also, there is a dedicated project calendar page, where IT and Cybersecurity related events, conferences, seminars, workshops and trainings can be published:

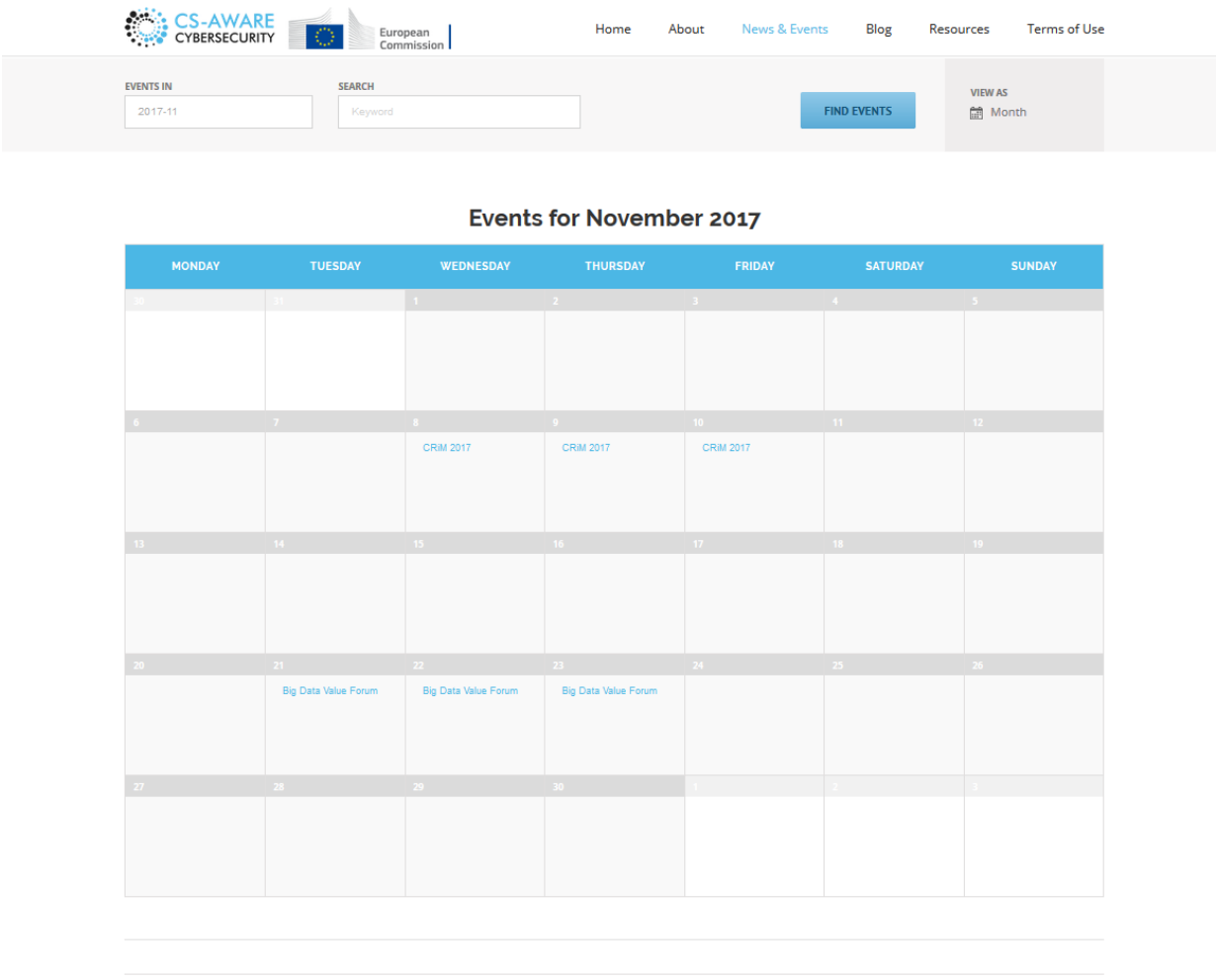

Figure 4. CS-AWARE calendar page

2.3 Social media presence

The Social media tools associated with the project have been created and consolidated from the very first day and now CS-AWARE has a recognizable and distinguishable presence on social media, allowing followers to engage and communicate with the project team, as well as attracting new ones.

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

In particular, a Twitter account and a Facebook profile were created for the CS-AWARE project to help publish news on our activities to attract attention from the LPA and the cybersecurity communities and engage in helpful discussions with them.

We aim to use the combined Klout index for measuring the effectiveness and the impact of those accounts. Furthermore, we aim to carry out targeted campaigns through social media to attract attention of LPA organisations and stakeholder groups early in the project, while during the pilot trials there is the expectation for an increased interaction due to an increase of outcomes coming out from the two pilot sites.

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 has been met and the blogs produced to date can be found on: https://cs-aware.eu/blog/

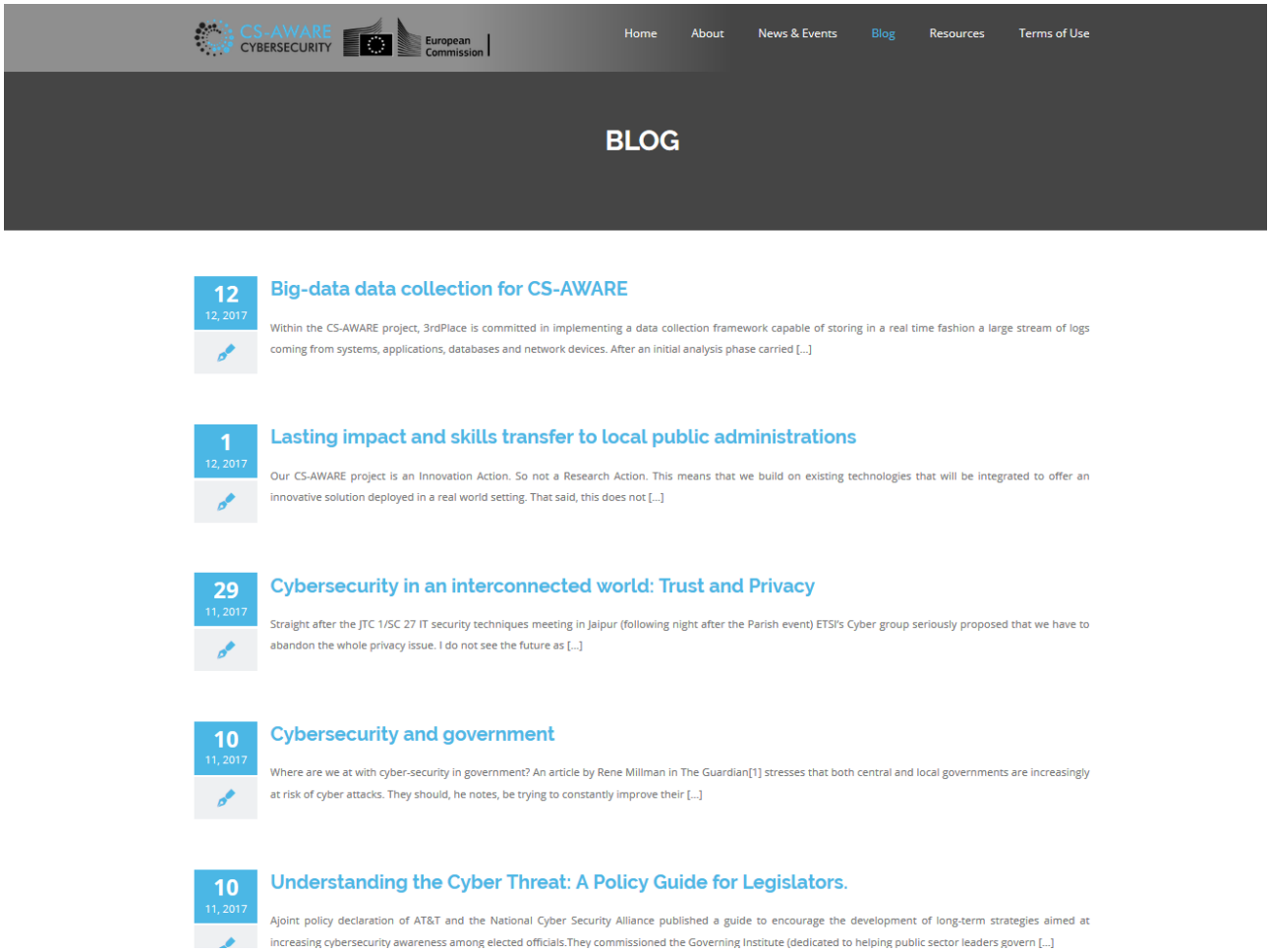

Figure 5. CS-AWARE blog

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/

2.6 Seminars and training

The list of seminars and trainings (past and future ones) where our project is/will be involved are presented in the next table:

Name	Date	Link	Description
CrIM17	8.11.2017-10.11.2017	http://www.oulu.fi/bisg/crim	CrIM17 is a seminar and workshop organized at the University of Oulu on an annual basis and consists of lectures and workshop sessions by security lecturers from all over Europe. It is aimed at students as well as cybersecurity professionals to disseminate the newest developments in security research. CrIM17 was organized as a multiplier event for the Erasmus+ strategic partnership SecTech which aims to establish a European cybersecurity curriculum. For CS-AWARE, we used the synergies between the two European projects where both the University of Oulu and the Unviersity of Vienna are involved in, to promote CS-AWARE at the event, and use the presented content as input for the CS-AWARE system and dependency analysis.
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" will be 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
OTS Forum	16 - 18 Nov 2017	http://otsforum.gr/%CF%80%CF%81%CF%8C%CE%B3%CF%81%CE%B1%CE%BC%CE%BC%CE%B1/	The yearly OTS Greek Forum, organized at the end of November in the city of Katerini - at the Northern part of Greece, traditionally attracts hundreds of delegates from Greek public organizations. The past year (2017) the participants where approximately 300 hundred, representing more than 80 public organizations - amongst them ministries, municipalities, regions, water authorities, legal public entities and academic institutions. The main agenda of the FORUM was focused around innovative products & services that could improve the functionality of public organizations. The CS-AWARE consortium was represented by its Greek partners OTS, Innosec & Municipality of Larisa. OTS & Innosec introduced in a thorough and analytical way the concept of CS-AWARE. The feedback received was quite promising and participants seemed to appreciate the importance and the necessity of a complete product/service such as CS-AWARE. A genuine interest on the project's progress was marked, enhancing the believe that the more familiar public organizations tend to get with the CS-AWARE concept, the more acceptance will receive.
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.

2.6.1 Publications policy

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. These days 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**. Each EU member has different regulations regarding cybersecurity as well as data privacy concerns. As a consequence, various more national-based solutions have developed over time. In recent years, the EU has encouraged more coordination in requirements, to bring about better interoperability; thus, increasing the market size and creating larger opportunities for industry, while decreasing development costs. The fragmentation of the market in the EU has tended still to favour the dominance of

US players, not only from the competition perspective but also in areas of data protection and cybersecurity.

- **Innovation influenced heavily by non-EU ICT products**. The presence of ICT in different products and services such as electronic banking, e-commerce platforms, big data, cloud computing, e-supply chain, smart devices and internet of things – is often driven by ICT products, that are not designed and manufactured in Europe. The downside to becoming dependent on ICT is that EU countries are increasingly vulnerable to the risks posed by cyber threats.

- **Inconsistent transnational approach.** Innovation is strong in Europe, largely emanating from ICT labs, SMEs and other large players, but not always properly funded due to a lack of a consistent transnational approach. Results of Research and Innovation are not consistently reaching the market. There is still a lack of strategy in EU research: certainly, several current efforts are focusing on identifying technology and societal gaps. Unfortunately, the established research and innovation priorities still tend to fail to consider adequately the economic and industrial perspectives, to bring 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.

- **Anticipated support from public procurement not yet in place**. In its recent assessment of the progress made on the implementation of the EU Cybersecurity Strategy, the Commission acknowledges that little progress has been made, concerning the actions to "develop, by the end of 2013, good practices to use the purchasing power of public administrations in order to stimulate the development and deployment of security features in ICT products and services", . It also states that "such good practices will be developed in the near future". Still, in many EU countries, the pivot towards a coordinated public policy in support of cybersecurity, seems relatively underwhelming.

- **EU industrial policies not yet addressing specific cybersecurity issues.** While the European Cyber Security Organisation (ECSO) noted that European Security Industrial Policy and the Communication for a European Industrial Renaissance, has set out an overall roadmap for the development of a more competitive European security industry, it points out that they did not specifically stress as critical problems in the domain of cybersecurity, the lack of policies in support of European security industry.

- **Cybersecurity and cyber defence**. The ECSO suggests that cyber defence can be considered as a form of cybersecurity dedicated to the protection of military installations and protection of classified information relating to military operations. In some EU countries, cyber defence is considered as the defence of the nation's critical (IT) infrastructure, in particular with the support of defence forces.

- **Sovereignty**. The current market fragmentation is partly due to the fact that security in general and cybersecurity in particular (especially as a component of critical infrastructures) remains, within the context of EU treaties, a national responsibility. Furthermore, cybersecurity cannot be isolated from "cyber defence - in sensitive domains like

cryptography, this would mean to continue developing, at least to a certain extent, country-specific solutions. Hence, there is a strong link between cybersecurity solutions and sovereignty matters for the Member States, which can result in a lack of cooperation and tends to lead to increased market fragmentation.

- **Strategic autonomy** The EU is partially dependent on non-EU technologies in many areas of ICT and the cybersecurity field. While this is not necessarily an issue for hardware and software solutions, it represents a major problem when considering devices manufactured by suppliers outside of Europe's legal frameworks. There is no full confidence that the devices do not include, for instance, built-in backdoors or are applying the same level of quality requirements.

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.

On the context of the present deliverable a primary market analysis is been done, 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 centrale 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 union 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

Open source licensing could be the preferred model of implementation in the case of CS-AWARE, exception being made for the situation where partners' proprietary software is used. In the open source scenario developers generally grant the licensee the right to modify, use, and distribute under certain conditions. Usually the licensee is required to see that any redistributions of software follows the same terms which it was transmitted. This means a distribution in complete form, accompanied by the source code, and without any further restrictions. Failure to follow OSS license terms subjects the user to potential liability for copyright infringement. With regard to any used proprietary licenses there will be followed the commercial licence requirements correspondent to that specific proprietary software modules.

Care will have to be taken when incorporating products of the Project into very often proprietary systems. Porting open source elements into basically proprietary software platforms might trigger a number of issues with licenses. The Project will work with the Pilots and others that may become involved to identify all instances of open source products and ensure that the conditions of all of the open source licenses have been observed.

Revenue Models

It will be through a large-scale distribution of its products & services that the Project will create revenue opportunities. The most suitable model that could fit the needs of CS-AWARE commercialization aspects is the SaaS model (Software as a Service), which has proven quite

effective for both open source solutions and services. Currently, both Italian and Greek partners utilize SaaS model in their portfolio of products and services.

It is true though, that in more "conservative" markets (the Greek & Italian market of public organizations fall under that category) more conventional models are preferred. Most commercial relations that contain provision of services or software to Greek & Italian public organizations, usually are based on a contractual agreement, renewed on an annual basis. Those types of agreement typically contain full on access of the software/service, support & updates.

A similar model with an annual contract philosophy, that seems to work on both Greek & Italian markets, is the one which contains different annual pricing for accessing different levels of services.

Complementary revenue streams that could be explored and adopted are:

1. **Consulting services**: The Project could offer consulting services to help plan, install, and operate its eventual products.
2. **Charge for additional services**: Either the Project or some combination of its partners could charge for additional services like hosting the platform, or maintenance, or even for implementing additional features.

Sale of additional proprietary modules: The Project could sell additional "closed sourced" additional products that build on its basic open source product. **Paths to Commercialization**

For public organizations - at least in Greece & Italy it is a good practice to offer the service or modules of the service with a free trial contract period (typically 6 months). Considering the bureaucracy that follows any type of procurement in public organizations and further taking into account the factor of limited financial resources, any new product or service that has to be acquired, is been treated with scepticism. It is not enough to justify the obvious benefits as a selling point. A hands-on review & testing by the decision makers and the confirmation that the product "delivers" what promises, is proven to be the most efficient strategy to commercialization.

The networks of local government and other professional associations (IT professionals in local government, for instance) will be an additional alternative. These networks can help decode and appropriate information flows, such as technological change, sources of technical assistance, market requirements, and strategic choices by others, thus strengthening the Project's competitive advantage. Ultimately commercialization performance will be affected by a knowledge of the available markets. Furthermore, these networks may encourage the establishment of relationships with others, to complement each other's resources at various points in the value chain. The usefulness of a national network should, certainly, not be ignored. As one study put it, "Recognizing opportunity and being ready to take advantage of it generally encompasses a temporal element (being in the right place at the right time), a relational element (the unplanned building of networks), and an analytical element (the establishment of connections between actual data and ideas). Further on, descriptions of local government and related associations are given.

Beyond the possible contacts outlined above, the national procurement agencies in each country will play an important role. Over a certain level, municipalities in most countries must go through their national procurement agency when it comes to acquisition of products or services, procedure that differs from country to country. Centralizing acquisitions could allow municipalities significant

savings and more transparency concerning prices, contract options, and maintenance issues Below a certain level (that depends on the country) agencies and local governments do not necessarily have to deal with their national procurement agency. Eventually for large scale acquisitions more formal agreement will be worked out with a number of these agencies. In a number of EU countries, yet to be determined, the Project working in cooperation with a local association or firm will register and develop of commercialization approach for the national procurement agency. While the details of an approach have not been worked out and will depend on the country, an eventual service-oriented agreement involving a cloud-based solution seems probable.

Lastly, when it comes to commercialization it is important to accurately identify those (typically few) entities that will operate as "early adopters", since economies of scale will be critical for the Project. Carefully selected individual municipalities, that maintain a certain "role" or "influence", will be important to find in each country.

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".

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.