D6.4 Commercial actions report

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, laurentiu.vasiliu@peracton.com
Co-author(s)	Giusseppe Clementino, John Forrester (Ancitel), Thomas Schaberreiter (University of Vienna), Chris Wills (Caris Research), Jerry Andriessen (Wise & Munro), Alex Papanikolaou (Innosec), Adamantios Koumpis (Passau University), Pierluigi Vacca (3rdPlace)
Document version:	1.0

Table of Contents

Executive Summary

This deliverable outlines the commercialization analysis, plan and action to be pursued by the CS-AWARE consortium members. It covers a brief introduction of the exploitable results, a SWOT analysis, then a market analysis, go-to-market plan, a review of the possible commercial risks and their mitigations, then concrete commercial actions pursued, while taking into account the overall required resources for commercialization before and after the project lifespan.

1 Introduction

The CS-AWARE project consortium partners have acknowledged from the early phases the project set-up that a strong commercial effort is required, so the CS-AWARE platform will get solid market traction. In this respect, a dedicated Work Package (WP6) was designed to handle simultaneously dissemination, exploitation and commercialization as all three are interconnected. This deliverable D6.4 covers the Commercialization analysis, actions and plan and has to be read in conjunction with D6.2 - Exploitation, dissemination and commercialization report that addresses several complementary aspects of the exploitation strategy.

2 Aimed exploitable results

The commercialization challenges faced by an EU type project are multiple given the structure and the very collaborative nature of the project. While the classic commercialization effort involves usually one company that drives, designs and executes the commercial strategy, in an EU consortium no partner can act commercially independent but has to take into consideration the requirements, expectations, internal speed, legal constraints as well as IP specifics of each partner. In the same time, a good coordination and agreement upon expectations, IP and legal matters have to be in place before discussing market strategies, revenue split and specific commercial actions.

While CS-AWARE has a robust industrial component, launching a new product on the market has its own unknowns and setbacks. The consortium may face internal and external market factors to be handled while pitching a novel product. The work in WP6 is synchronized with the bi-weekly Commercial User Group (CUG) conference calls that discusses continuously various challenges and helps design strategies to overcome potential obstacles and prepare the market penetration of the CS-AWARE platform.

The goals of the commercialization are simple in essence, however, require an in-depth preparation and a solid plan execution. By the end of the project, it is anticipated that each industrial partner that commercializes, has a clear understanding of the targeted markets and a plan to approach them as well as how to finance a sustained commercialization effort.

2.1 Goal and features of the solution

The CS-AWARE solution is offering cybersecurity related services and is aimed at organizational systems, where one of the big factors influencing security are the socio-technological relations between technology and its users, as well as the complexity of such organizational set-ups that often neglects to provide an overview of the security situation.

2.1.1 Visualisation and decision support

A main feature of the CS-Aware solution is the visualisation and decision support component. The vision is to provide a system operator (for example, the administrator or security expert of the customer organization) with a mechanism that visualizes current security threats and incidents in the organizational systems, and sets it in context with the cybersecurity situation worldwide, by observing relevant information sources. CS-AWARE provides a decision support system by providing recommendations and potential solutions to solve or mitigate incidents using the additional context gained from external information. The key of the visualization and decision support system is to provide an intuitive way of showing a complex situation to the user of CS-AWARE and making it as easy as possible for the user to come to an informed decision and to choose the best prevention or mitigation strategy.

2.1.2 Situational awareness

Cybersecurity situational awareness is achieved by gaining an understanding of a customer's systems (assets, dependencies and information sources) by conducting soft systems analysis, collecting relevant information from those systems and from relevant external information sources and by detecting anomalies in system behaviour that are classified, enriched with context and presented to the CS-AWARE user.

2.1.3 System self-healing

System self-healing is a feature that can maintain or restore an operational state for a system under attack in such cases where the nature of the attack is well known and clear prevention and mitigation or system recovery policies can be established beforehand. When an incident is detected and classified, and a self-healing policy is available for the incident, the CS-AWARE user will be notified and asked if the self-healing mechanism should be invoked, causing the system to implement the policies without further user interaction.

The main components of CS-AWARE to allow system self-healing are the soft systems analysis and the incident classification. The soft systems methodology includes several steps that allow to define solutions to the problems detected in the analysis phase. In CS-AWARE, we will define policies that will allow to prevent, mitigate or recover critical components/assets in an organizations system from well-known and likely threat scenarios. Based on the policies, the proper mechanisms will be identified or implemented in the organizations systems to allow invoking those prevention, mitigation or recovery policies. The policies can be invoked if the detection component detects one of those anomalies (based on the mechanisms described above for cybersecurity situational awareness) that can be classified to one of the self-healing policies.

2.1.4 Customer's (end user's) perspective

Cybersecurity information exchange is a service of CS-AWARE that is partly transparent to the customer. While the customer might not be particularly interested in sharing information about cybersecurity incidents with the larger community or official authorities, it is still an important aspect of cybersecurity that will gain relevance in the future. So while this service might not have marketing appeal at the moment, it may very well be an asset in the future if information sharing will become the booster for improved cybersecurity that many security researchers and experts are thinking it will be. Once the public opinion about the usefulness of security related information sharing shifts, and the legal framework that supports and protects information sharing efforts stabilizes, a product that offers information sharing may have a market advantage over other solutions that do not.

The part of the information exchange of CS-AWARE that is relevant to the customer is the part where information about security incidents that happened within the customers systems is shared. After an incident is detected and handled, the CS-AWARE operator will have the option to share this information with the community or with relevant authorities in order to be able to develop better protection strategies and help other organizations that are facing the same problem. The information exchange is realized in a separate component that builds upon all the mechanisms that are utilized to provide the cybersecurity situational awareness described above.

2.1.5 An example scenario

To illustrate how the CS-AWARE solution can improve the cybersecurity situation, we would like to give a hypothetical example of how the CS-AWARE could have helped to detect and mitigate one of the large-scale cyberattacks of 2017: The WannaCry scenario. WannaCry was a ransomware attack that targeted a Windows vulnerability to gain access to victims' computers and encrypt their hard drive to ask for ransom. So how could CS-AWARE have helped to stop or mitigate the attack?

- Cyber situational awareness and decision support: While CS-AWARE is not intended to monitor each single end user device that might be affected by malware, the network and service-based monitoring CS-AWARE provides, will allow to detect anomalies in network traffic that may suggest malicious behaviour. For example, WannaCry had a built-in kill switch that was implemented in a way that each newly infected host would try to connect to a specific URL and only continue to infect other hosts if this URL did not exist. CS-AWARE will be designed to pick up anomalies like the sudden increase in connection attempts to a random and previously unknown URL and classify it as suspicious. If enough other sources have been picking up on this behaviour, official sources might give out a recommendation in how to deal with this. CS-AWARE would be able to visualize the extent and real-time growth of the behaviour and propose possible solutions as decision support to the operator who may invoke the proper mechanisms to prevent or mitigate the threat.

- System self-healing: In the case of ransomware attacks one possible solution may be to restore the system or service state to a previous backup. If this is the preferred solution for a customer, a policy and associated mechanisms could be created to automatically restore a system to a previous backup. The policy can then be carried out once CS-AWARE has detected an anomaly and classified it as ransomware.

- Cybersecurity information exchange: if CS-AWARE detects suspicious behaviour that cannot be classified, this information can be reported to relevant authorities. If enough other companies report this kind of behaviour immediately after detection, a fast spreading attack like WannaCry can be detected and analysed by the relevant authorities quickly and possible countermeasures can be proposed in a timely manner, possibly reducing the scope of the incident significantly. Other organizations that are affected by the same attack at a later time will benefit from this.

2.2 Delineating the CS-AWARE product

The product that CS-AWARE provides can be split into two parts: The individual analysis of a customer's systems that allows to gain an individual understanding of an organizations assets and dependencies among them, and the automatic and tool driven detection and awareness solution. While those two parts form a complete product and one part could not exist without the other, there could still be two separate services that can be offered to customers: The analysis part that requires expertise and manual effort (and could be positioned as cybersecurity consultancy), and the access to the detection and awareness part that could be, amongst other possibilities, a subscription-based service.

In some situations, a company may decide to only need the analysis services of CS-AWARE, just to gain a better understanding of their systems, but decide not to opt for the detection and awareness part. In other situations, a company may decide to perform the analysis part themselves and only subscribe to the detection and awareness solution, providing their own analysis results.

To illustrate the two parts of the product the two figures next (1 and 2) show the interactions of the main players involved in the two parts of the CS-AWARE product: the system operator who will be responsible for controlling the interactions with the tool driven detection and awareness solution, and the analyst who is responsible for providing all the necessary information to correctly set up the tool driven solution for each individual customer organization.

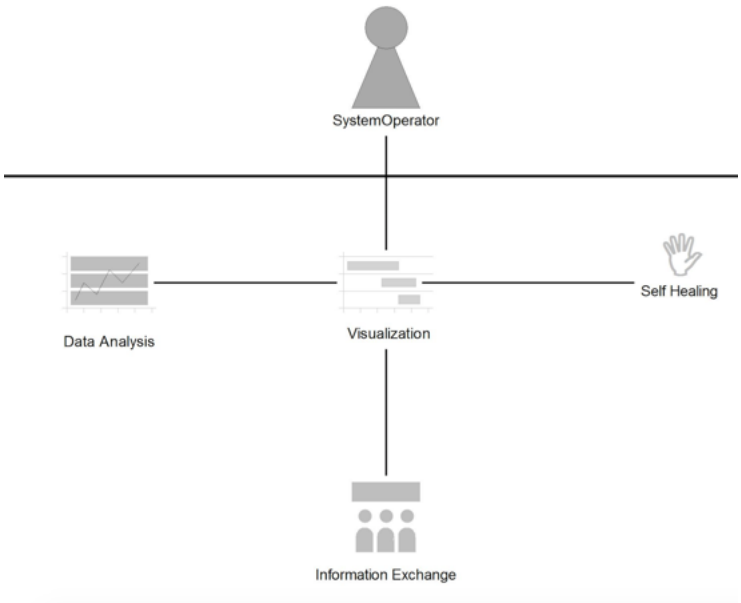

Figure 1 System operator interaction with the CS-AWARE platform

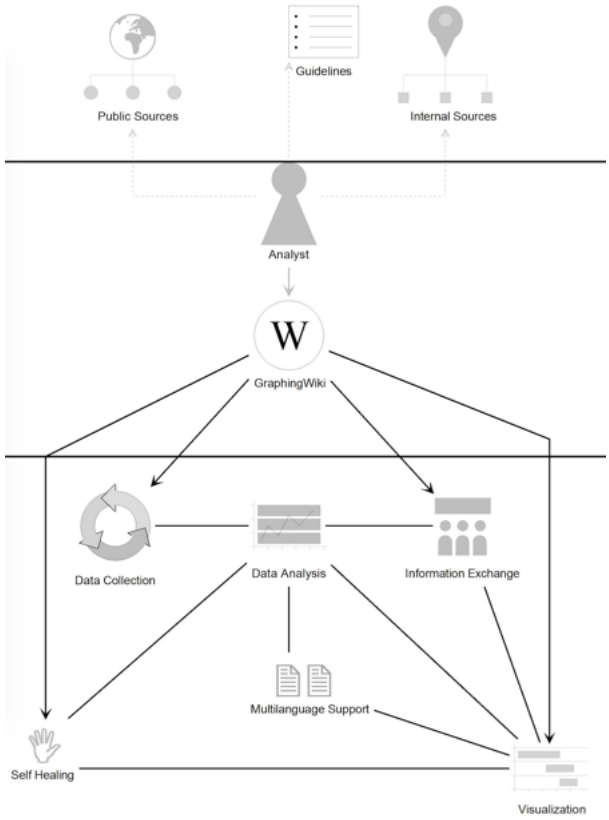

Figure 2 Anlyst interaction with the CS-AWARE platform

The system operators view of the CS-AWARE solution is mainly concerned with the user interface that will present the automatic detection results and will allow control interactions with the main features of situational awareness and decision support (via data analysis, visualization and control interface), system self-healing and cybersecurity information exchange. The analyst is responsible for, on an individual basis, making sense of the customers systems (from both internal and public sources) and provide the required information to configure the CS-AWARE components and get the automatic and tool driven CS-AWARE solution up and running.

In this phase of the project we have been evaluating the feasibility of the chosen analysis methodology, the soft systems methodology, its practical relevance and its exploitation potential by conducting the analysis in both of the projects pilot studies in Larissa and Rome. We have seen that the soft systems methodology is an excellent tool to provide the required information for CS-AWARE, in both the medium sized pilot in Larissa and the large and very complex pilot in Rome. The commercialization prospects of this analysis method (possibly positioned as cybersecurity consultancy) are seen as excellent, since this methodology has been used by one of the commercial

project partners (Caris Research) on many occasions, and the contextual shift to cybersecurity related analysis is working as expected.

The second part of the project, the tool driven analysis and awareness solution, has not been evaluated yet in this project phase.

3 SWOT analysis

Next figures 3 and 4 are presenting the very first SWOT analysis for the CS-AWARE envisioned approach:

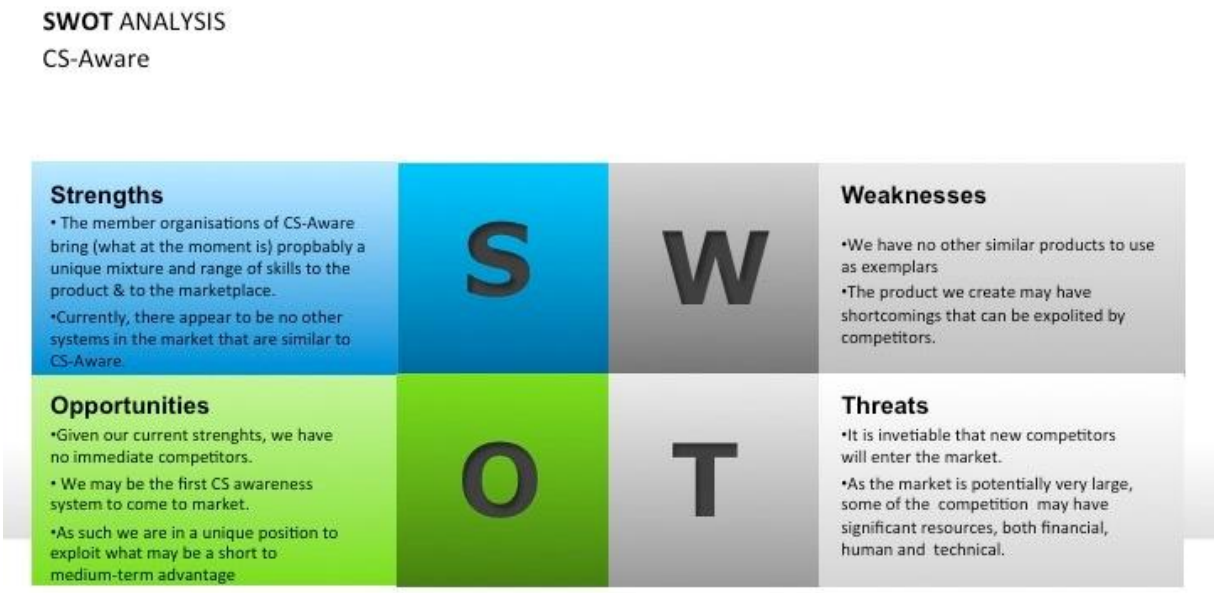

Figure 3 CS-AWARE SWOT analysis

The members of the CS-Aware consortium between them bring a probably unique mixture and range of skills to the product and to the marketplace. It appears that at the moment there are no immediate competitors. The CS-Aware system *may* be the first such system to come to the market. However, if realised, this lead is likely be short-lived, so the advantages of being first to market must be maximised and thoroughly exploited.

Figure 4 SWOT analysis primary factors

It follows that time to market is of the essence. The CS-Aware system is under development, so a competitor may enter the market first. A decision may need to be taken as to whether to attempt to create strategic alliances and partnerships with potential collaborators at this stage in order to avoid them becoming potential competitors later.

4 Initial market analysis

This analysis will seek to identify the institutional framework that CS-Aware has to consider. The project certainly has to deal with the current segmentations and needs of the public actors involved in the cybersecurity sector. Another important dimension is related to emerging trends in the PA sector regarding the municipal cooperation. Since municipalities in the European countries, in large part, are quite small and have only limited resources, the municipal cooperation is a must. All the small and medium public administration are obliged to associate their organizations to provide almost any kind of services to the citizens. Understanding how these municipal cooperation is functioning in each country will be critical for the Project.

In other terms, it is important to concentrate the efforts to disseminate the results of the projects directly inside the dynamic development of these municipal cooperation, implemented in each country. Furthermore, the majority of the municipalities are often too small to have (and to pay) the

professional staff and the technological resources to integrate new ideas and innovations. It is necessary to investigate how the municipalities and other local agencies are acting in their real context. Looking at their organizational patterns and commitment, analysing how the actual situation in each country has evolved in recent years, and how their experiences and successes should be integrated in our specific project plans.

The Council of European Municipalities and Regions (CEMR) report on "Local and Regional Government in Europe: Structures and Competences" (sept. 2012) underlines that over 60% of decisions taken at the European level have a direct impact on municipalities, provinces, and regions. Furthermore, the CEMR report estimates that from 70% to 80% of public investments in Europe are managed by local and regional authorities. The future of Europe increasingly lies, as matter of fact, in the hands of local authorities.

The Project will need to develop a deep knowledge of the "terrain". Creating strategies that are truly adaptive, it requires to avoid long-held assumptions in favour of flexibility and deep knowledge of the local administration context. Considering also how the complexity of our changing world is making the world more unpredictable. Average population sizes of municipalities in Europe show that with the exception of the UK, Denmark, the Netherlands, Eire and Greece, large areas of other European countries are dominated by small and medium sized municipalities (Moreno, A et al. 2012).

	Number of Municipalities	**Population (2018)** [1]	**Average Number of Inhabitants per municipality**
United Kingdom	419	65,648,054	156,678
The Netherlands	390	17,064,682	43,755
Ireland [2]	126	4,786,562	37,988
Poland	2,479 [3]	38,131,648	15,382
Italy	7,958	60,589,445	7,614
France	36,658	65,129,822	1,776
Finland	313	5,534,655	17682
Austria	2100	8,745,151	4,164
Germany	11,313	82,220,424	7,267
Greece	325	11,149330	34,305
Denmark	98	5,745,874	58,631

Table 1: Average population sizes in targeted EU countries

[1] Statistics taken from the Eurostat site and Comuniverso site.
[2] 31 municipalities and 95 municipal districts for a total of 126 municipal entities.
[3] Of these 2060 are classified as cities.
[4] 2,060 are classified as cities.

In recent years some national governments in Europe devolved a number of powers and responsibilities to local governments. In addition, there has been in many areas a push for more

unions between local authorities to use the available resources more effectively. Indeed in France, municipal cooperation is a crucial part of the national government strategy, considering the large number of "micro-municipalities". Practically speaking in every country, given the reduction in funding and support, local authorities don't really have any alternative other than collaboration.

This Project will work with interested regional and provincial institutions or with Unions of Municipalities, or at least one of the Metropolitan areas, each in turn would involve their network of institutions. The strategy behind any eventual marketing plan and business models will probably reflect this process of "indirect dissemination", also establishing a cooperation with a selected number of government associations in each country. In other terms, the dissemination models will differ from country to country, depending on both the systems of government and the interests of real stakeholders.

4.1 Selected Country profiles

4.1.1 France

In France, the interests of local and regional governments are handled principally by the following three organizations: ARF(**Association des régions de France**), ADF(Assemblée des départements de France), AMF(**Association des maires de France**). The Association of Regions may be the best to contact not only for suggestions on "early adopters" but also some combination of dissemination action on their part (particularly with their site http://www.lal27regione.fr).

- **The Association of French regions (Association des Régions de France – ARF)**

The AFR lobbies the government about the issues of interest to the regions. The Association also lobbies members of Parliament concerning the opinions of the regions to take into account during the legislative process. ARF also seeks to transmit the regions' viewpoints in a number of state bodies. In addition, the ARF also promotes regional activities, collaboration, and exchange of information in several economic and social spheres, like commerce, industry, and agriculture, as well as legislation on decentralisation and regional administration.

The 27e région (http://www.la27region.fr)

The Association created in 2008 a 27th region calling it a virtual collective ("collectivité virtuelle") – in other words, a laboratory of ideas for the future.

Among their projects are:

- "The Town Hall of Tomorrow"[2]
- "Entrelabs: Immersion in Public Design"

The web sites http://www.la27region.fr and http://superpublic.fr could be platforms to reach local authorities interested in issues like cybersecurity, privacy, and the protection of data.

4.1.2 Ireland

Unlike in other countries one of the key players is the Local Government Management Agency (state agency of the Department of Environment, Community, and Local Government). Web

site: http://www.lgcsb.ie) LGMA. It was established 2012 to provide a range of services to the Local Government Sector. The LGMA is a central resource for the local government sector, providing, procuring and coordinating a range of support services which are most suited to being distributed at national level. It is a shared repository of best practice providing research and specialist expertise for the Local Government sector. At the very least they may be willing to sponsor a workshop to publicize CS-AWARE and to determine whether local authorities might be interested.

The Office for Local Authority Management (OLAM), a division of the Local Government Management Agency (LGMA) provides support and acts as point of contact for the CCMA. OLAM supports the committee structure and influences and implements the Association's work programme through targeted research and identification of best practice. Working with this office could worthwhile on the identification and elaboration of best practices regarding cybersecurity for local government.

In June 2014, the Association of County and City Councils (ACCC) merged with the Association of Municipal Authorities of Ireland (AMAI) to form the AILG (Association of Irish Local Government – web site : http://www.ailg.ie/ . The AILG is a networking, policy development and training resource for the elected members of Ireland's thirty-one County and City Councils. The Association works through delegates in each of the councils to help develop a sense of collegiality among the elected members who serve the public in a variety of local government settings ranging from urban to suburban and rural. Contacts with this group could be important in terms of networking opportunities to identify other local government leaders interested in cybersecurity tools.

The County and City Management Association (CCMA) is known as the "representative voice" of the local government management network. Its members are Chief Executives of the County and City Councils and the Assistant Chief Executives of Dublin City Council. It is a non-statutory body that works to ensure that the influence of local authority Chief Executives is brought to bear on the development and implementation of relevant policy.

The following strategic objectives as listed on the CCMA website point to an interest in innovation and best practice. The results could be applied effectively in promoting "direct engagement with key stakeholders":

• Influence and shape emerging and future policy affecting local government through direct engagement with key stakeholders on a range of diverse subjects;

• Advocate on behalf of the system for necessary resources, identify strategic choices to be made in the allocations of resources and demonstrate the system's capability to ensure the provision of value for money;

• Develop and present an accurate and positive view of the worth of local authorities in the public domain by building an understanding of the broad range of work that local authorities are involved in and the issues that drive and influence it;

The CCMA works in partnership with other agencies to develop and implement legislation. As a representative of the management of local authorities, the CCMA are key stakeholders in the areas of planning, the provision of infrastructure, housing, environment and sanitary services as well as recreational, social inclusion and cultural and tourism services and as such are consulted with by a broad spectrum of organisations.

The CCMA may be able to identify for us local authorities interested in issues of cybersecurity, privacy, and data protection.

LGiU Ireland (http://www.lgiuireland.ie)

Their principal mission seems to be help share policy information for local government across Ireland. They aim to develop a schedule of occasional events to help politicians and officers in local government explore and share policy development. The site seems rather small but they may be interested in disseminating information about CS-AWARE and cybersecurity.

Local Government Management Agency - Web site: www.lgma.ie

The Agency seems to be the key, at least in part, to promoting change and innovation on a governmental level. The County Manager, as well as being manager for the county councils, is also manager for all boroughs and town councils within a county. Town clerks (at the local level) work under the guidance of the county manager (intermediate level). Each Regional Authority also has a designated County/City Manager, to assist in guiding the work of the authority and ensure coordination between the local authorities in the region.

4.1.3 Italy

The principal local government association is the following:

National Association of Italian Communes (ANCI)

In cooperation with ANCI Ancitel could create a service for individual municipalities where the installation and management of CS-AWARE would be done by Ancitel as a cloud based service for municipalities interested. There is also an interest in an eventual integration of cybersecurity issues with another service offered by Ancitel concerning Privacy and Data Protection obligations and guidelines. The principal target would be either larger local entities or municipal unions where budgetary issues are not such an issue as in smaller municipalities.

Using the site noted below for demographic statistics (http://www.comuniverso.it) 14 metropolitan areas can be identified in Italy. According to Wikipedia, Metropolitan areas usually refer to a region consisting of densely populated area and its surrounding territories, sharing industry, infrastructure, and housing. As social, economic, and political institutions have evolved over time, these metropolitan areas have become key economic and political regions.

Regione	Città metropolitana	Comuni	Superficie (kmq)	Popolazione (Istat 2017)	Densità demografica (ab/kmq)
Lazio	Roma	121 Comuni	5363,28	4353738	811,77
Lombardia	Milano	134 Comuni	1575,65	3218201	2042,46
Campania	Napoli	92 Comuni	1178,93	3107006	2635,44
Piemonte	Torino	316 Comuni	6827,01	2277857	333,65
Sicilia	Palermo	82 Comuni	5009,28	1268217	253,17
Puglia	Bari	41 Comuni	3862,88	1260142	326,22
Sicilia	Catania	58 Comuni	3573,68	1113303	311,53
Toscana	Firenze	42 Comuni	3513,69	1014423	288,71
Emilia-Romagna	Bologna	55 Comuni	3702,32	1009210	272,59
Veneto	Venezia	44 Comuni	2472,91	854275	345,45
Liguria	Genova	67 Comuni	1833,79	850071	463,56
Sicilia	Messina	108 Comuni	3266,12	636653	194,93
Calabria	Reggio Calabria	97 Comuni	3210,37	553861	172,52
Sardegna	Cagliari	17 Comuni	1248,68	431430	345,51
Totale		**1.274**	**46.639**	**21.948.387**	**470,61**

Table 2 Italian metropolitan areas

Since most metropolitan areas include multiple jurisdiction and municipalities (n.b. 121 municipalities associated with Rome), the Project should consider the metropolitan areas in EU countries as of priority interest in terms of market possibilities.

Aside from metropolitan areas the .comuniverso' site notes that there are 96 municipalities that are provincial capitals. In addition, there are approximately 90 municipalities that are not provincial capitals and have more than 50.000 inhabitants. The municipal unions in Italy are currently 537. Those municipalities with more than 50.000 inhabitants are probably the most likely to have the social and economic resources to be interested in what the Project has to offer. As noted elsewhere the majority of Italian municipalities are small and lack the resources to be able to undertake a cybersecurity project by themselves. The situation is similar in other EU countries. The majority of municipalities in the EU are small and medium sized in population.

4.1.4 The Netherlands

Dutch municipalities are generally dependent on the Central Government. Revenues from local taxes are lower than in many other European countries, but Dutch local authorities are responsible for a wide range of tasks.

The Association of Provinces of the Netherlands (Interprovinciaal Overleg; IPO) (Web site: http://www.ipo.nl/ is the association of the twelve provinces of the Netherlands. The association looks after provincial interests and developed a platform for exchanging knowledge and experience among the twelve Dutch provinces.

On their website they note the following:

Innovation & knowledge

The Association seeks to provide a platform for the provinces to stimulate innovation and the sharing of knowledge. In this way, it hopes to encourage best practices and the sharing of innovations in the implementation of provincial policies. The idea is to contribute to the quality, effectiveness and efficiency of public administration.

It certainly might be possible with the Dutch members of the Consortium to do a number of workshops and training sessions with the Association, that may attract interest for the CS-Aware product.

The Association of Dutch Municipalities (Vereniging van Nederlandse Gemeenten or VNG) http://www.vng.nl/) represents the interests of all 380 Dutch municipalities vis-a-vis central government. In addition, it delivers a variety of services to all Dutch municipalities.

Under the Research and Development programs on the site they outline an outreach program to help municipalities exploit knowledge and research in the social sector. Their interest in the development and diffusion of knowledge – from the bottom towards the top, through workshops on the transformation of local and regional knowledge networks should fit in quite well with our interest with the activities of CS-AWARE.

4.1.5 Poland

Several nationwide organizations of local government have been established since 1990.

Among the organizations of interest in Poland are:

- **Union of Metropolitan Cities (the ten largest cities)** http://www.metropolie.pl/en/ : The resources available to them makes them a likely contact for possible dissemination activities. They would also be important because they would be in a position to help other smaller communities.

- Union of Rural Communes www.zgwrp.pl (Związek Gmin Wiejskich Rzeczypospolitej Polskiej): The Union is very interested in the development of local democracy and local autonomy. They have participated in a number of European organizations and EU projects. With the Consortium partner in Warsaw there could be an opportunity for dissemination here.

- Association of Municipalities of Malopolska and Poviats http://www.sgpm.krakow.pl/index.php They define the Union is the largest of its kind at the regional level in Poland. It includes 100 municipalities and districts. They seem quite interested in promoting democracy on a local level and projects to develop civil society in addition to reinforcing social capital at a local level. This Union would probably be quite interested in discussing possibilities for the Project – particularly in terms of implementing a cloud-based service.

Open data and efforts for more transparency in government have attracted the most interest from local advocacy civil groups. Issues of cybersecurity, privacy, and data protection might well be of great interest.

4.1.6 United Kingdom

The principal local government association in the UK is the Local Government Association (LGA - Web site: www.local.gov.uk). All English councils are members of the LGA* (414 authorities in total).

In addition, there are bodies such as London Councils (formerly the Association of London Government) and other regional bodies to bring together local authorities at the regional level.

Some of the more active regional groupings are the followings:

East Midlands Councils : (http://www.eelga.gov.uk/)

London Councils[6] (http://www.londoncouncils.gov.uk/)

Association of North East Councils (http://www.northeastcouncils.gov.uk/).

South East England Councils (http://www.secouncils.gov.uk/)

South West Councils (http://www.swcouncils.gov.uk/nqcontent.cfm?a_id=1).

It is clear reviewing the activities of these associations there is considerable interest in innovative solutions that would help local administrators develop services that respond more effectively to community needs. Workshops on the activities of CS-AWARE could be developed for their members on not only what the project is about but also what value proposition they may have for local authorities.

4.2 Segmentation of customers

(to be addressed in V2 of this document M18) *

4.3 Competition

(to be addressed in V2 of this document M18) *

4.4 Us versus the competition

(to be addressed in V2 of this document M18) *

*Note: for 4.2, 4.3 and 4.4 sections at this point is too early (M6) to have them defined. They will be addressed by M18 when we'll have a much better view over CS-AWARE platform as well as the specific market we target.

5 Go-to-market Analysis

5.1 Business Summary

This project (CS-AWARE Horizon 2020) is a cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis. The key advantages and differentiation are summarized in the following bullets.

- Provide system and dependency analysis based on mature and well-proven system analysis methodologies like the soft systems methodology, in order to capture case specific internal and external socio-technical cybersecurity requirements to refine situational awareness results.
- Use state-of-the-art data collection, analysis and visualisation tools to offer situational awareness in an online fashion, using robust technologies (such as MAARS by Peracton) to detect in real-time cyber incidents based upon multiple threats parameters.
- Provide features like cybersecurity information sharing and self-healing after a cybersecurity incident that builds on the situational awareness capabilities.
- Aim for the right balance between automation and the ability for user interaction, allowing for fully automatic reaction to cyber incidents, or requiring user acknowledgement.

The drivers behind the utilization of this project are summarized as the lack of a) cybersecurity preparedness in local public administrations, b) funding to address cybersecurity in a sustainable manner and c) technical know-how. For this project to be completed, it requires the synergy among 13 participants (list of participants) that include research, technology development and integration, service and user partners.

5.2 Product Strategy

Key objectives for products that will be launched in the context of this project can be summarized like this:

Objective 1: Provide a cybersecurity situational awareness solution for local public administrations in line with the current and upcoming legal cybersecurity framework in the European Union and its member states.

Objective 2: Advance the automation of cybersecurity incident detection, classification and visualisation to provide situational awareness. This includes socio-technical system analysis, data collection, data analysis and decision-making as well as the visualisation of the findings.

Objective 3: Include a cybersecurity information exchange framework that embraces the collaboration and cooperation initiatives of the European cybersecurity strategies. This includes the utilisation of cybersecurity data for threat detection as well as sharing of newly discovered cybersecurity incident data.

Objective 4: Illustrate that cybersecurity situational awareness is a key technology in cybersecurity by building advanced features like system self-healing on top of the situational awareness capabilities.

Objective 5: Evaluate and validate the user needs through end-user involvement and pilot testing. This includes the evaluation of the balance between automation and user control, usability features like multi-lingual support as well as the evaluation of business needs and business models.

Channel Strategy

The primary channels that will be used to disseminate the project's deliverables are presented as two application scenarios. Particularly, the functionality of CS-AWARE, will be demonstrated in the case of small public administrations in Greece (Pilot 1) and a model will be created and tested for local public administrations in the metropolitan area of Rome(Pilot 2). This would provide a

cybersecurity situational awareness solution for several additional municipalities that, apart from the Cybersecurity point of view, could also help show more fully the confidentiality and privacy of citizen data that the project implements by design. Other channels that will support the dissemination of the project's objectives are digital media outlets such as websites, social media and YouTube channels.

5.3 Marketing Strategy

Marketing activities that are selected to drive awareness and generate leads include the following: publications, workshops, conferences, campaigns, social media and blogs, website, end-user involvement and pilot testing, cybersecurity legal expertise in consortium, communication activities with stakeholder groups in cybersecurity and cybersecurity information sharing.

5.4 Customer Experience

The ambition of the CS-AWARE solution is to provide mechanisms that can both benefit from cybersecurity information sharing as well as giving back information to the community to improve cybersecurity for society as a whole. Since in the current situation no information sharing initiative could act as the single point of contact to get all the relevant information, the CS-AWARE approach is to enable information exchange with all relevant sources. Provision of customization and support services will be provided to needs of specific targeted customers. Exploitation prospects per country are available which show the commitment to enhance customer experience and develop a multilingual dimension of the CS-AWARE solutions globally.

5.5 Technical Requirements

This project proposes a situational awareness solution that is meant for small- to medium-sized IT infrastructures of local public administrations (LPAs) in both technological realisation and business/market strategy. The solution proposed in this project is composed of several building blocks consisting of tools and methodologies that consortium partners bring to the project. The main building blocks of this project are system and dependency analysis, data collection and data analysis to achieve the project's goals of cybersecurity situational awareness, cybersecurity information exchange and system self-healing. The system and dependency analysis methodology is expected to be a semi-manual, tool-supported process. System analysis is a task that will always require utilising expertise, but one of the outputs of this project will be the establishment of clear procedures and guidelines that will allow to carry out a quasi-standardised and repeatable system and analysis for the specific contest of local public administrations. Provided with the input from the system and dependency analysis, data collection will be a mainly automatic effort. While data analysis is supposed to be an automatic effort given the data collected in the previous step, it was classified to be a semi-automatic effort because the threat detection might need to be supervised depending on the context. The information sharing and self-healing aspects of the solution are assumed to be semi-automatic efforts, since the end user will retain control over the actions offered by them. Furthermore, in order to deal with the expected language barriers and usability concerns in the context of European local public administrations as the end users of the solution developed in this project, multi-lingual semantics support will be part of this project's solution.

5.6 Evaluation

The table below summarizes and outlines what techniques are being deployed and the relevant evaluation criteria for each one accompanied with means of approval.

Measurement Technique	Evaluation criteria	Means of approval or verification
Project Branding	Level of positive identification of Logo/Branding with the CS-AWARE core functions and aims.	Approved consensually by all partners
Project Website	Google Analytics data to record number of unique visitors per day. Number of users engaged in site activity. Number of through-feeds to CS-AWARE portal.	On an annual basis: Number of visits, number of unique visitors Average visit in minutes Number of page views Number of countries visitors come from
Facebook page	Page activity (posts / comments / likes)	Additional fans since start or per year Number of posts since start or per year Max. people reached in 1 day / 1 week / 1 month
Twitter Page	Follower numbers and interest levels (re-tweets and tags)	Additional tweets since start or per year Number of followers Number of those following
Blog	Entries Reach	Number of blog entries per year Acquired audience
YouTube Channel	Number of Video Views.	Number of videos and respective hits
Newsletter	Number of circulations	Number of readers
Press releases	Rates of coverage and general news interest.	Number of appearances
Publications	Number of articles and/or papers	Number of publications

National and international events attended/activities organized	Events attended/organized.	Number of workshops or other national or international dissemination activities

Table 3 Techniques deployed and evaluation criteria

5.7 Timeline and Execution

This project consists of work packages (WPs) and the picture below shows those WPs as well as the relations among them. Particularly, the task WP1 will ensure the proper coordination and management of CS-AWARE throughout the project's lifetime. Tasks WP2, WP3, WP4 and WP5 are the technical work packages of this project that will ensure that the requirements (e.g. user, legal, organizational requirements) are in line with the project's goals, the building blocks of this solution are properly matured and integrated as well as pilot-tested in real world environments. As illustrated in the following Figure 1, WP3-WP5 will be carried out largely in consecutive order, with the latter WPs relying on the output of the previous ones. However, appropriate feedback mechanisms for refinement will be provided. WP6 covers the dissemination and exploitation of project results throughout the project lifetime, as well as ensuring that steps towards commercialization and market replication are taken.

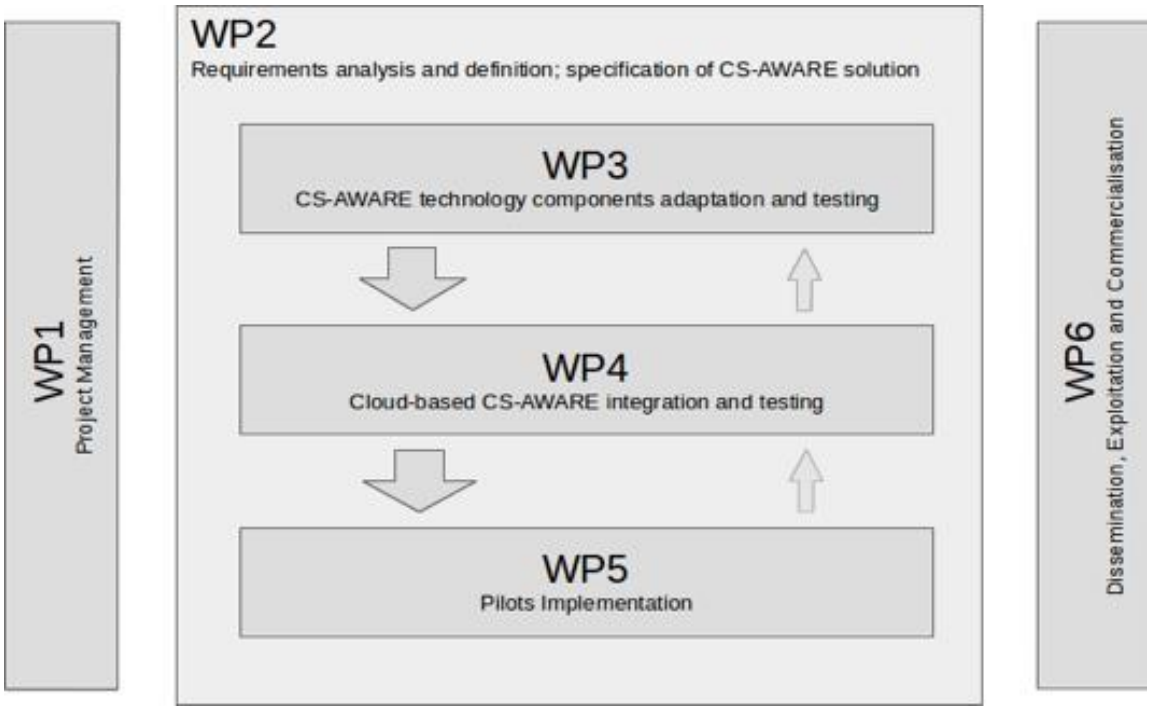

Figure 1: Work package structure and inter-relations.

Moreover, the following Figure 2 is a Gantt chart which shows the work plan as means of work packages, deliverables and milestones.

Figure 2. Work packages, deliverables and milestones.

5.8 Positioning of the CS-AWARE brand

Positioning a brand means emphasizing the distinctive characteristics that make it different from its competitors and appealing to the public (Kapferer, 2004). Positioning is a crucial concept because it lets consumer choices be made on the basis of comparison. The aim of positioning is to identify and take possession of a real advantage. It implies a desire to take up a long-term position and defend it. Moreover, positioning defines a brand's personality and gradually builds its character that is distinct from the rest of the marketplace. Brand positioning is defined by Kotler (2003) as "the act of designing the company's offering and image to occupy a distinctive place in the mind of the target market". In simple words, brand positioning describes how a brand differentiates from its competitors and how it is perceived in customers' minds. Therefore, a brand positioning strategy entails the creation of associations in users' minds to make them consider the brand in a particular way (Fuchs and Diamantopoulos, 2010). In this project, the main objective is to provide a cybersecurity situational awareness solution for small to medium sized IT infrastructures. This solution enables to detect, classify and visualise cybersecurity incidents in real-time, supporting the prevention or mitigation of cyber-attacks. The solution will be a big step towards automation of cybersecurity incident detection, classification and visualisation, and will be based on mature big data analysis tools and methodologies provided by consortium partners. According to a survey conducted for the purpose of this project, it clearly indicates the lack of cybersecurity preparedness in local public administrations. Most notably, the lack of funding to address cybersecurity in a sustainable manner and the lack of technical know-how have been reported. To deal with these facts and to position the project as a brand in user's minds, we selected various techniques such as a) web-site presence, b) social media presence, c) blog presence, d) leaflet and poster and e) seminars and training. Employing such techniques will allow to create and develop a unique impression in user's minds so that the customer associates something specific (e.g. cybersecurity) and desirable (e.g. protection of personal data) with the brand (CS-Aware v2 Horizon 2020). In addition, identification of key stakeholder groups, such as the Focus Group on Cybersecurity or the European

Network and Information Security Agency (for more please see section 1.3.3) allow for a consistent and continuous dissemination of knowledge around the project.

5.9 Communication Channels

Communication channels are defined as the mediums through which a message is transmitted to its intended audience, such as print media or broadcast (electronic) media. The selection of communication channels is of paramount importance for the success of a project because it defines the means through which inputs and outputs of a process are communicated. There are many different communication channels to choose from in today's globalized and high-tech world that each channel comes with its characteristics, pros and cons. Therefore, depending on the message content, scope, audience and timing, there should be a proper selection of communication channels between members of the project. The channels used to reach and engage people should depend on what it needs to be achieved with the communications, the preference of the target audience and the resources and budget available. For the purpose of this project, we use a range of channels to achieve the objectives. In the table below, we identify the communication channels used and link the purpose for their selection.

Communication channels	**Good for**
Group meetings, workshops, conferences	Listening, brainstorming, relationship building, sharing purpose, exchange of complex learning and information, building trust and loyalty, engaging early adopters.
Launch events	Stakeholder awareness, relationship building, provide an opportunity for media coverage, builds up trust and friendship
Social media (e.g. YouTube, Facebook, LinkedIn)	Creating networks with niche specialization or interests, building a profile, directing to other communication channels (website or blog), real-time updates, maintaining relationships, exchange of information, easy to interact, reaching early adopters, accessibility
Website	Demonstrating full range of work, attracting new members/audiences, information exchange
Blogs	Demonstrating expertise, knowledge exchange, interaction with social media, can redirect traffic to website, place for barnstormers
Email	Low cost, wide range of audience, quick transmittance of info and results
Leaflets, brochures, posters	Visual impact, communicating detailed information, wide audience attraction, dissemination of message, longevity
Publications	Scientific approach, attracts specialized audience, connection with libraries and educational institutes, updates of results
Mobile technology / SMS	Quick delivery of short/simple messages, ideal for instant communication
Newsletters	Keeping in touch, news and updates, defined group of interested people

5.10 Sales Channels

Sales channels are means or methods used by an organization to sell or market its product or services to end users (Blakeman, 2015). Selecting the right sales channels can affect directly not only the marketing strategies, but also the business' potential revenue. Sales channels can be two types; direct (e.g. personal sales, email marketing, website) or indirect (e.g. representatives, affiliates, resellers). Both have their own traits that outline their purpose of selection. The direct channels allow for a high level of influence on the customer, knowing exactly how the customer behaves or feels about a product or services due to the direct communication. On the other hand, indirect channels are mostly suitable for expanding geographical reach without having to contact the customer directly (Friedman and Furey, 1999).

For the purpose of this project, we choose to select a mix of both types of sales channels. From the perspective of direct sales, we choose to employ and develop our own website which represents the main channel of displaying the project's features and progress. It was launched at the end of November 2017, after being approved by all consortium members and it can be accessed at https://cs-aware.eu/ that is a domain purchased specially for the CS-AWARE project. In addition, the project partners are all listed at the bottom of the website by their logos and can be found with their full description in About/Partner section while there is an open contact form available to anyone to contact the consortium. By the end of the project, it is anticipated that each industrial partner that commercializes, has a clear understanding of the targeted markets and a plan to approach them as well as how to finance a sustained commercialization effort. Using a direct channel of distribution to connect consumers with our project, especially a Web-based channel, can have several benefits such as low overhead costs and also provides for the project a potentially global reach. Direct distribution via the Internet is convenient for customers and available 24 hours a day.

Considering the fact that we are living increasingly digital lives, the smartphone is perhaps the biggest single influence on consumer change. In this regard, we consider that mobile technology can increase both the penetration rate of the project and the adaption of its purpose, therefore making the m-commerce an important sales and revenue channel. Moreover, the emergence of social media continues to shape the landscape of brand and indirect marketing. In particular, social media, such as Facebook and Twitter, blogging and press coverage allow us to build long lasting relationships with end users by allowing them to contribute to the purpose of this project and by commenting on their experiences.

Last but not least, we choose to build an affiliate network that consists of key stakeholder groups, such as ENISA, the Focus Group on Cybersecurity (CSCG, formerly "Cybersecurity Coordination Group") and research and innovation activities such as MICIE and Multimedia Documentation Lab (MDL). This affiliate network will allow us to reach an even wider range of audience and disseminate the project's philosophy, which is an increased resilience to cyber security threats facing SMEs, local public administrations and individuals.

5.11 Anticipating a difficult market entry in times of austerity and cuts in public spending

There is no doubt on the importance of Local Public Administrations all over Europe. However, one may seriously doubt on a number of issues:

First of all, the capacity of the latter to financially support the purchase of a product like ours. A further aspect of this relates also to the existence of the necessary personnel to get trained in the configuration and operation of such a system.
Secondly, the capacity of LPAs to maintain a solution like ours both in terms of its financial cost but also of the needs it incurs for its management by specialized personnel.

While it might seem that the situation in Italy and Greece is to a degree rather unique in terms of local governments than in other countries of the EU there are some common aspects that are similar in almost all EU countries. More specifically, austerity programs have left many local public administrations with ever decreasing budgets while demand for public services may be, paradoxically, increasing. And while local public administrations have acquired more autonomy over the years, they have not been necessarily granted more financial resources. We may well be able to take advantage of initiatives encouraging local governments to pool their resources with others. Typically local governments (not just in Italy and Greece) don't have the resources to deal adequately with cybersecurity issues – this issue may either not appear in their agendas or appear with only a very low priority. Either grouping their resources together or working with a larger governmental entity (whether a larger city, province, or region) might well be the best way for many local public administrations to proceed. However, we see this rather unattractive picture as a challenge from our side to discuss, explore and experiment with a variety of potential approaches like:

- Offer the CS-AWARE product as a solution (infrastructure, application or service) over the cloud and offer it for free with only costs incurred these of hosting and of initial configuration / customization / adaptation.
- Offer the CS-AWARE product as mainly an open source, to be governed by a not for profit entity that may be administered by our Coordinator who is a non-profit entity, and with only costs those of the hosting and of the initial configuration / customization / adaptation. Additional costs may relate to support services and other types of services like training, specialised development, add on modules and components, etc.

In the next months, we shall aim to quantify the different approaches, starting from the cases of Italy and Greece and then extending to the other markets in Europe. Such a quantification will result to different scenarios that will help us proceed with the necessary decisions at the consortium level.

6 Risk analysis and mitigation

This section is identifying the various risks related to the usage of CS-AWARE platform and technology. Further it builds the basis for potential solutions and/or mitigation strategies.

6.1 Technological Risks

	Technological Risk	Mitigation Strategy
1	Corporate policies	We identify the required policies and we make sure we are compliant
2	Noisy content	Robust data filtering methods in place, including focused visualisations
3	Content length - challenge for statistical NLP(Natural Language Processing) approaches	Use the adequate NLP technique to handle the content length variety and use filtering of content that does not need NLP
4	Pilots data access limitations	Ensuring a minimal required set of data for meaningful testing. Good coordination with the legal entities of the Pilot projects and with focus from the ethics part of the project, will ensure correct and meaningful data access.

6.2 Commercial Risks

	Commercial Risk	Mitigation Strategy
5	Sales cycles longer than initially thought	Focus on very specific pre-qualified targets, identify possible sale opportunities during the project.
6	Getting entrance to decision makers difficult	Go early after external partnerships and identify decision makers early in sales opportunities
7	Not enough sales experience within the consortium	Identify by M12 specific commercial weaknesses and have a dedicated plan in place; diversify the commercialization approach such as going simultaneously for other type of actions such as licensing and setting up a spin-out company

6.3 IPR/Legal/Ethical risks

	Legal Risk	Mitigation Strategy
8	place of jurisdiction - data collection	be compliant with each jurisdiction, and avoid collection of Person Identifiable Information(PII)-data using anonymization tools when possible.
9	location of CS-AWARE service	choose the most data protective/friendly location
10	data protection	Host critical security data in locations that are protected by the adequate legislation with service providers with

		full compliance to, among others GDPR, ISO 27018, ISO 27002, etc.

6.4 Regulatory Risks

(to be addressed in V2 of this document M18) *

*Note: for 6.4 section at this point in time is too early (M6) to have them defined. They will be addressed by M18 when we'll have a much better view over CS-AWARE platform as well as the specific market we target.

7 Commercial actions

Two of the main business goals of CS-AWARE are:

- Start selling and increase the sales of the CS-AWARE product and
- increase the number of cybersecurity threats that may be avoided by using the CS-AWARE product by engaging 3rd parties into information sharing, in order to build a stronger European cybersecurity network that will again strengthen the position of CS-aware.

In this chapter, some initial ideas for relevant strategies to achieve both of these goals are presented.

7.1 Marketing

Marketing is the management of creating, keeping and satisfying the customer. From this point of view the strategy will break the activities in 2 macro-categories:

- **Product life-cycle management (PLM)** - the main goals are to:
  - Identify buyer personas (target to reach)
  - Evaluate the CS-Aware solution unique strengths/weaknesses as well as opportunities/threats (SWOT Analysis)
  - Analyse the competition (Market landscape Analysis)
  - Creating and updating a sales strategy
  - Identify potential sales opportunities and revenue contributions,
  - Improve product quality,
  - Reduce time to market (creation of presentation material, sales decks, proposal framework, etc.)
- **Product promotion & communication** - the main goals are to:
  - Generate awareness around cyber security threats and challenges,
  - Position the CS-Aware brand in the mind of the target market (small to medium sized IT infrastructures) as a unique opportunity to face cybersecurity threats and challenges
  - Generate leads: stimulate users interested in CS-Aware Brand to leave their personal info (name, email, phone number, etc.) for future sales contacts

In order to reach the goals described above, we will develop a marketing strategy based on 4 main pillars:

- **PR**: this activity consists in the production and dissemination of articles, press releases as well as press conferences, roundtables aimed to address the challenge of cybersecurity

for small to medium sized IT infrastructures as well as to raise visibility for the CS-Aware Brand

- **Inbound Marketing**: is a technique for drawing customers to products and services via content marketing, search engine optimization and branding. In particular the project partners will produce and disseminate content around the web about cyber security from different perspective (general, technical, legal, ethical, etc.) in order to attract users in every single phase of the buying cycle (awareness, consideration, conversion)
- **Online advertisin**g also called online marketing or Internet advertising or web advertising, is a form of marketing which uses the Internet to deliver promotional marketing messages to consumers. It includes:
    - ***Email marketing***: is the act of sending a commercial message, typically to a a selected group of people that matches the target market criteria
    - ***Display advertising*** is an online form of advertising that the company's promotional messages appear on third party sites such as publishers or social networks. The main purpose of display advertising is to support a brand awareness (Robinson et al., 2007).[6] and it also helps to increase a purchase intention of consumers.
    - ***Social Media marketing***: is the use of social media platforms to promote a product or service. In particular social media can play a strategic role to increase visibility to particular posts, contents that drive high engagement with potential customers (eg. number of likes, shares, etc.)
    - ***Search engine marketing (SEM)*** is a form of internet marketing that involves the promotion of websites by increasing their visibility in search engine result pages (SERPs). This activity is particularly strategic to drive visits on the website from users that may be already in a "consideration" phase of their buying cycle
- **Events & Workshops**: given the complexity and the poor awareness both related to cyber security, we believe that specific workshops, events, roundtables will be one of the the key driver to attract potential buyers, generate a database of prospective clients and start the sales activity. The feedbacks/questions collected during these events will be also helpful to support the pre-sales phase

7.2 Pre-sales

Pre-sales is a process or a set of activities normally carried out before a customer is acquired. These activities can be described as follows:

- **Qualifying new leads**: the project partners will evaluate every single prospect in order to make sure that it fits the CS-Aware offering and consequently its worth to invest time and resources
- **Identifying needs**: once the lead is qualified, the project partners will start the initial contact with the prospect to figure out its needs, problems, goals as well as to analyze specific requirements in order to develop an initial picture of the solution the potential customer needs
- **Proposal Building**: the knowledge of the prospect ecosystem will help the project partners putting together a proposal that matches its needs. The proposal may trigger the following elements:
    - Presentation
    - Market scenario (drive awareness about cyber security)

  - What is CS-Aware and the opportunity connected to the project
  - Eventual Case Histories
  - Project Details/Workflow
- **Product Demo (features)**
- **Proof of Concept**
- **Economic figures**

7.3 Sales

Sales is a process of turning prospects into customers. The activities can be described as follows:

- **Sales Presentation**: the project will be described in detail to the prospect, providing eventual demos, proofs of concepts and/or details about the required workflows to express the CS-Aware solution's full potentials
- **Follow up**: the project partners in charge of sales will keep an open communication flow with the prospective clients in order to provide any additional information, support, clarifications that may influence the buying decision process
- **Negotiation**: it's an open process for two parties to find a mutual satisfaction in a business agreement. The project partners in charge of sale will evaluate the opportunity to review the economics in order to close the deals

The strategy outlined to boost and enhance CS-AWARE sales will be based in two main approaches: a direct and an indirect channel.

- Direct channel: the mains sales point will be the CS-AWARE platform that will offer features and functionality of an online marketplace
- Indirect channel: alliances and partnerships with LPA software vendors and value-added re-sellers, in a commission basis. This is the way that both partners Ancitel and OTS operate in Italy and Greece respectively.

- Direct channel

Direct channel needs may be addressed by a portal that will be created and promoted in the form of the CS-AWARE marketplace. There, the description of the offerings can follow the structure of the items listed in Section 2.1 of Deliverable 2.1 where the list of all relevant cybersecurity threats as they appear in the ENISA report are presented. The development of such a portal would have in consideration the following aspects: the simplification of contents, the simplification of the purchasing process, the utilization of cloud services as these can be defined and offered by the partner CloudPartners and the optimization of the trial process so that LPAs will be able to see and experience practically the value of the CS-AWARE offerings.

- Indirect Channel

This approach will consist in the development of strategic alliances and partnerships with resellers and vendors who are active in the market of LPAs, which will allow the opening of additional sales

channels through a joint go-to-market model in strategic geographies (e.g. same as partner Ancitel is expected to dominate the Italian market for CS-AWARE relevant services and partner OTS the Greek market).

To achieve this, a CS-AWARE Partner Program will be created, in order to train and certify resellers and vendors. Only members of this program will have permission to sell the CS-AWARE product in the respective geographies.

Channel partners will bring actual value for the sales process by introducing their clients and by playing the role of advisor, being an important vehicle to increase market share.

In order to guarantee an adequate performance of indirect sales force, training and targeted sessions will be performed. The following aspects will be taken into consideration within the training plan:

- Development of simpler and practical support materials to support the sales process
- Development of tools and contents to support sales force
- Development of commercial videos and tutorials 'Fast & Simple' about the CS-AWARE offer
- Simplification of purchasing process
- Periodic training courses on key products
- Development of short training initiatives, with business partner groups organized in different countries.

7.4 Post-sales

“Post-sales” is a process or a set of activities normally carried out after a customer is acquired. These activities can be described as follows:

- **In-House Training**: the customer will identify the key personas in its organization be fully trained in order to generate/share “value" from the CS-Aware solution and fill the lack of cybersecurity preparedness in local public administrations
- **Customer Service and Support** in order to find solutions to the eventual technical problems, bugs, etc.
- **Customer Relationship Management**: maximizing customers retention building long-time relationships with the customers, whose feedbacks will be crucial to improve the solution as well as the level of assistance

As the project will evolve, this section will document the commercial actions undertaken by the consortium members. This will be updated in V2 of this document.

8 Conclusions and future work

This first version of the commercial actions report has two aims: one is to create the format that will guide us in our path towards commercialization and provide a structure that will help us in the next months until the second version of this report (M18) that has to include a report on the progress of the already planned activities as well as the plan for the activities till the conclusion of the project.

While the first part of the report is devoted to the presentation of the main features of the CS-AWARE platform and what we consider as the core CS-AWARE 'product', comprising also functionalities related or assigned to respective services and / or Apps, as well as to a SWOT Analysis of what we consider as our strengths, weaknesses, opportunities and threats that we expect to face in view of the commercialization, it is the second part that contains more market- and business-critical content as it reflects our current understanding of the market (section on Market Analysis), the customers (section on Segmentation of customers), the competition (section: Competition) and how we expect us to position ourselves with respect to it.

The Go-to-Market Plan is in this respect the most important part that is complemented by what we perceive as the positioning of CS-AWARE brand i.e. in other words how we understand the branding of CS-AWARE.

All relevant parts to this like the Communication or the Sales Channels, as well as the analysis of technological or commercial risks, or risks related to IP or regulatory / legal aspects can be regarded as resulting from the perspective we have for the addressed field and how we envision to address the opportunities as well as the challenges that are implied.

References

Blakeman, R., 2015, The Hybrid Sales Channel: How to Ignite Growth by Bridging the Gap Between Direct and Indirect Sales, McGraw Hill Professional

Comuniverso (Source: Ancitel) http://www.comuniverso.it

Eurostat. http://ec.europa.eu/eurostat/statistics-explained/index.php/Main_Page

Felix, R., Rauschnabel, P.A.; Hinsch, C. (2016). "Elements of Strategic Social Media Marketing: A Holistic Framework". Journal of Business Research. doi:10.1016/j.jbusres.2016.05.001. ADIKESAVAN, T. MANAGEMENT INFORMATION SYSTEMS BEST PRACTICES AND APPLICATIONS IN BUSINESS. ISBN 8120348966. Retrieved July 10, 2015.

Friedman, L., Furey, T., 1999, The Channel Advantage, Reed Educational and Professional Publishing Ltd.

Fuchs, C. & Diamantopoulos, A., 2010. Evaluating the Effectiveness of Brand-Positioning Strategies from a Consumer Perspective. European Journal of Marketing, 44(11/12), pp. 1763-1786.

Kapferer, J.-N., 2004, The new strategic brand management. Creating and sustaining brand equity long term. 3rd edition, Kogan Page Limited.

Kotler, P., 2003. Marketing Management. 11th ed ed. Englewoods Cliffs,NJ: Prentice-Hall.

Kresl, Peter Karl and Daniele Ietri. Regional Studies Association: The Global Forum for City and Regional Research, Development and Policy. Regions and Cities. Routledge, New York, 2016

MECLABS, content: MarketingSherpa, design: Scott McDaniel, code: Steve Beger, (January 21, 2009). "New Survey Data: Email's ROI Makes Tactic Key for Marketers in 2009".
"IAB internet advertising revenue report: 2016 full year results" (PDF). PricewaterhouseCoopers, Internet Advertising Bureau. April 2017. Retrieved 6 February 2018.
"The State of Search Engine Marketing 2006". Search Engine Land. February 8, 2007. Retrieved 2007-06-07.

Moreno, Á. M. (Ed.). (2012). *Local government in the member states of the European Union: A comparative legal perspective*. Madrid: INAP, Lithuania Had an average of 50,876 inhabitants pr. Municipality (2011) www.tandfonline.com/doi/full/10.1080/17445647.2015.1060181

Robinson et al. (2007) 'Marketing communications using digital media channels', in Chaffey, D. and Chadwick, F. E. (2016) Digital Marketing: Strategy, Implementation, and Practice. Edinburgh Gate: Pearson Education Limited, pp. 515-522.