D6.8 Exploitation, dissemination and commercialisation report V3.4 January 2021 (M36 – revision after the final project review)

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)	Judi Blackmur, Peracton Ltd. Thomas Schaberreiter, University of Vienna
Internal reviewers:	Alex Papanikolau, Innosec John Forrester, Cesviter
Document version:	V3.4

Table of Contents

Revision History

Version	Changes
3.0	Original draft sent to internal review 24.08.2020
3.1	Submitted to the Commission 31.08.2020
3.2	Revised version submitted to the Commission following received feedback 24/12/2020
3.3	Minor intermediary revisions 18/01/2021
3.4	Greek market cybersecurity update added and final version submitted to the Commission on 21/01/2021

Executive Summary

This deliverable is the final update of the 'Exploitation, dissemination and commercialization report' covering the period March 2019-August 2020 and the developments during this period. It consists of four chapters that have been developed in the past versions and now they are being actualized: a final update of the dissemination plan and actions, a final update of the commercialization and exploitation plan (focusing on the spin-out as well as individual commercialization), final IPR management update and future work.

1 Introduction

Cybersecurity global market is one of ever-growing focus and importance as all private and governmental actors and entities require protection from increasing sophistication of cyber threats and attacks. In the same time, according with 'Research and Markets, April 2020' [1] the impact of COVID-19 on the market is forecasted to reduce the cybersecurity market growth 'at a slower average rate of 6.2% per year until 2023. Still, with such impact, there will be solid growth as the market forces stimulants will keep driving the growth. However, reaching out to this market in current market and COVID-19 safety conditions render additional challenges at all pre-sales and sales levels.

Following the CS-AWARE EU LPAs market focus as well as the feedback received during the previous reporting periods, the consortium worked during the final reporting period on identifying how to reach out to EU based LPAs, what are their features, what are the communication channels, their particularities, having a special focus on Italy and Greece. It was very obvious from early on that the market we are addressing is not a B2C (business to consumer) one but a B2B (business to business) type, where the end users are organizations having various but specific procurement channels, rules and required steps within the whole EU space.

Given the B2B market focus, the consortium decided that the most appropriate (main) commercialization path of the CS-AWARE project to be via a new spin-out commercial vehicle.

While the spin-out wasn't explicitly a deliverable in the original project description of work., the consortium decided to go beyond the original plan and invest consistent effort in preparing and setting up a spin-out, in spite the unexpected COVID-19 situation that apparently may induce an economic recession at least as strong as the 2008-2012 one with extra risks on top of the inherent ones when establishing a new company.

Also, in parallel, three partners of the consortium (3rdPlace, Peracton and Cesviter) have the intention to pursue individual commercialization actions independent and not competing the spin-out initiative as it will be detailed below.

2 Dissemination plan and actions

2.1 Dissemination Plan

We continued our dissemination effort via various channels such as partners' direct contact with LPAs in Italy and Greece, via blogs, newsletters, scientific publications and social media channels. The original dissemination plan had no major deviation. The only notable mention is that given the B2B (business to business) focus and not B2C (business to consumer), the dissemination effort via social media was deemed by the consortium to have less impact at this stage and rather, focus in particular on the effort on the spin-out preparations and set-up. The advantage of this approach is that 1) it has been ensured a continuation of social media presence of the CS-AWARE effort beyond the project life-span given that all social media channels will be taken over by the new spin-out and 2) social media efforts will continue in very targeted commercial ways for the spin-out needs as the spin-out will develop. We consider this balanced approach has been the most appropriate for the long-term development of the CS-AWARE platform.

2.2 Website presence

During the last year of the project a new newsletter section was created, where the newsletters written by partners were uploaded and available for download: https://cs-aware.eu/newsletters/ The website remained stable with no major changes and was updated continuously. The next Figure 1 shows the project website number of users, new users and sessions recorded by google analytics, with the caveat that due to GDPR regulations, some users may have chosen not to be tracked by cookies and therefore were not recorded as website hits.

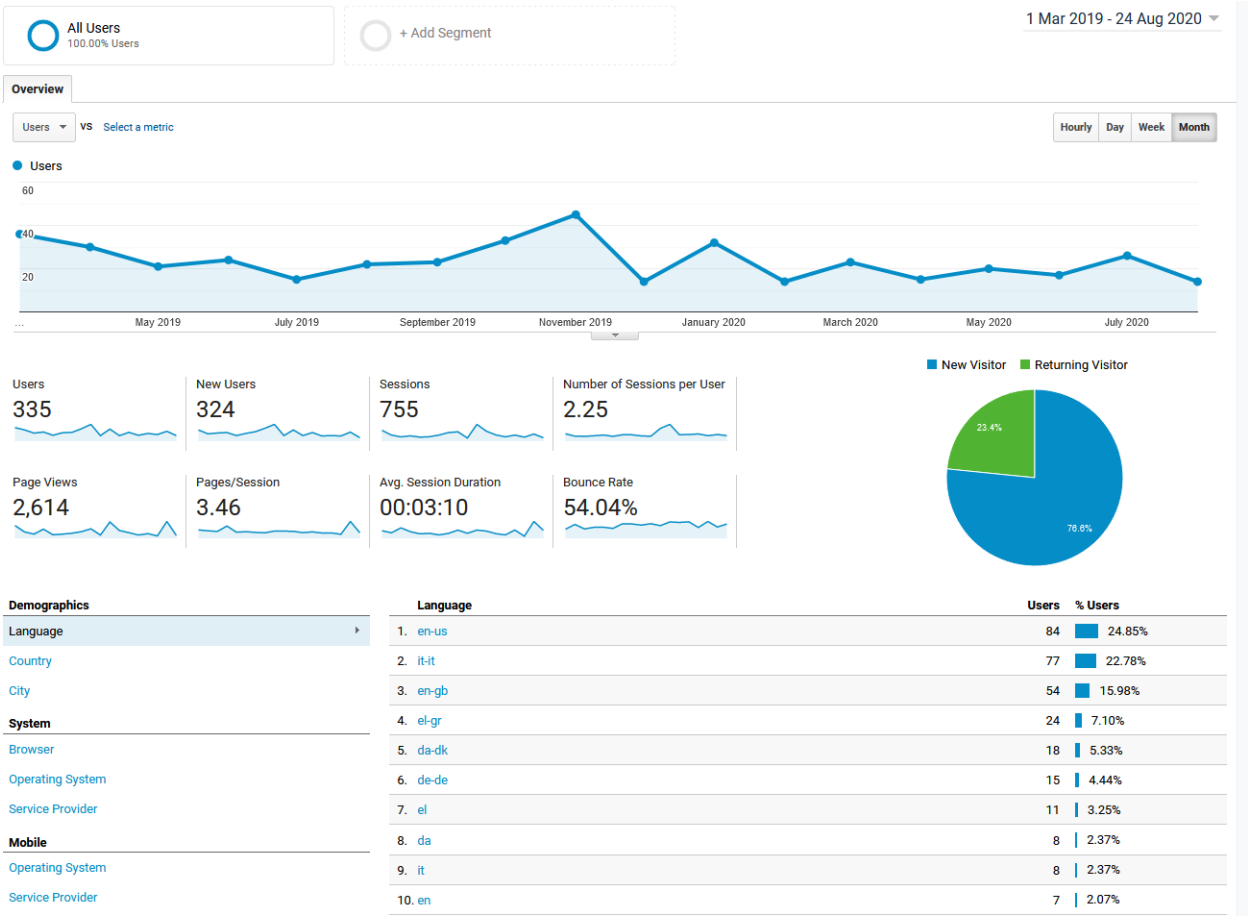

Figure 1 CS-AWARE website users monthly hits and origin languages overview 1 March 2019-24 August 2020

According to the recorded statistics, there were 324 new users, 2,614 page views, with an average of 2.25 sessions per user. The main readers where from English speaking countries (US and UK) followed by Italian, Greek, Danish and German readers.

2.3 Social media presence

Activity continued constantly on Twitter, Facebook as our primary channels reflecting specific technical aspects relevant for CS-AWARE or relevant to the cybersecurity space CS-AWARE addresses. The newsletters written by partners were also distributed via Twitter and Facebook as they were released. While below we present the overall social medial statistics for the last reporting period, in Deliverable 1.5 (pages 42 to 48) there is presented a detailed comparison between the originally planned dissemination targets from the description of work and the actually achieved ones by the end of the project.

Table 1 next shows twitter statistics on impressions (the number of times users saw a tweet on their Twitter timeline)

Month	Twitter impressions
August 2020	949
July 2020	2032
June 2020	1008
May 2020	2418
April 2020	763
March 2020	1048
February 2020	1864
January 2020	3884
December 2019	2123
November 2019	2709
October 2019	2888
September 2019	2669
August 2019	2469
July 2019	1155
June 2019	1078
May 2019	714
April 2019	944
March 2019	2673

Table 1: Twitter impressions over the last reporting period

Next screenshots present a sample of the Twitter analytics panel for period April-July 2020 where the twitter impressions are listed:

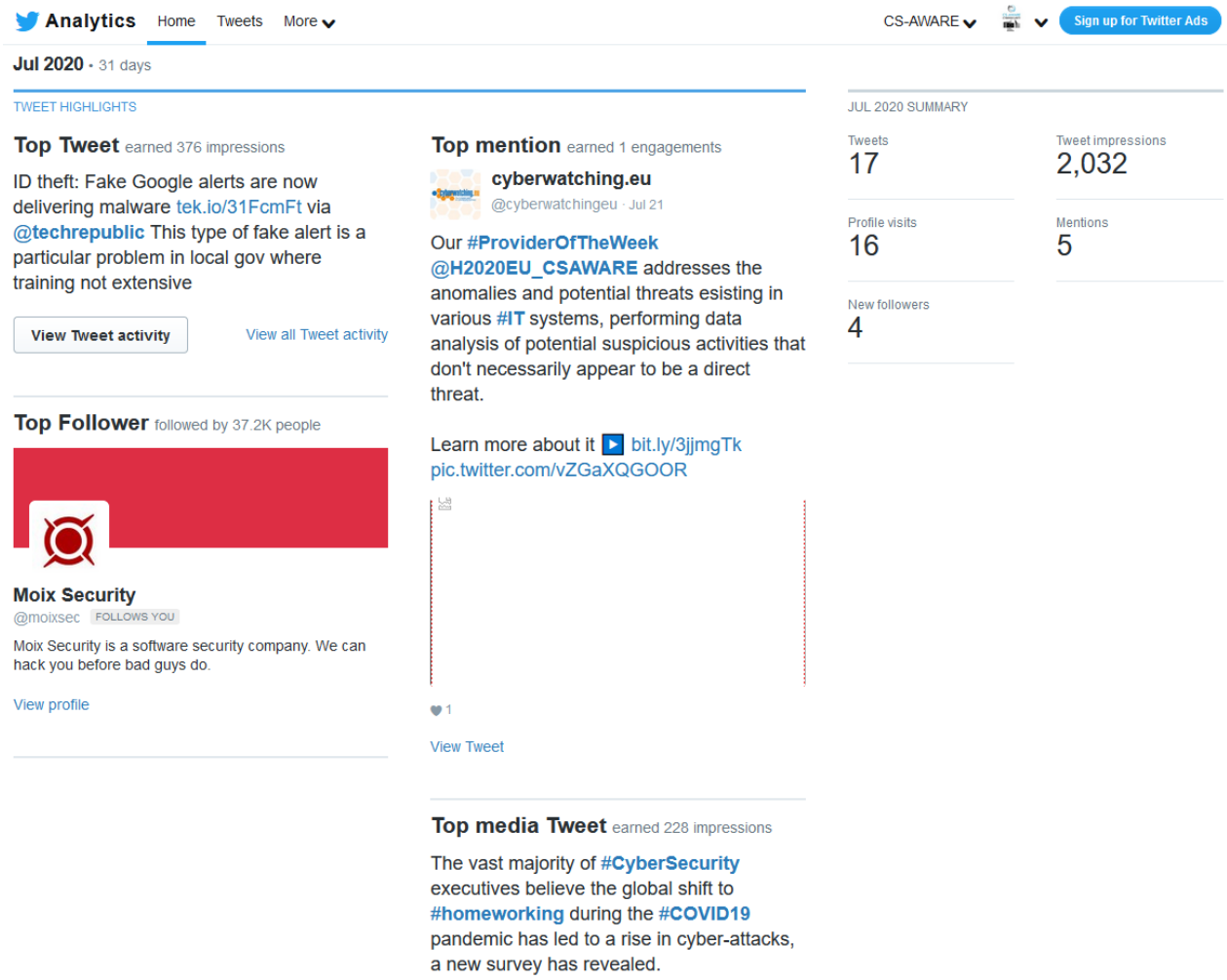

Figure 2: Tweet impressions screenshot from CS-AWARE twitter account analytics – July 2020

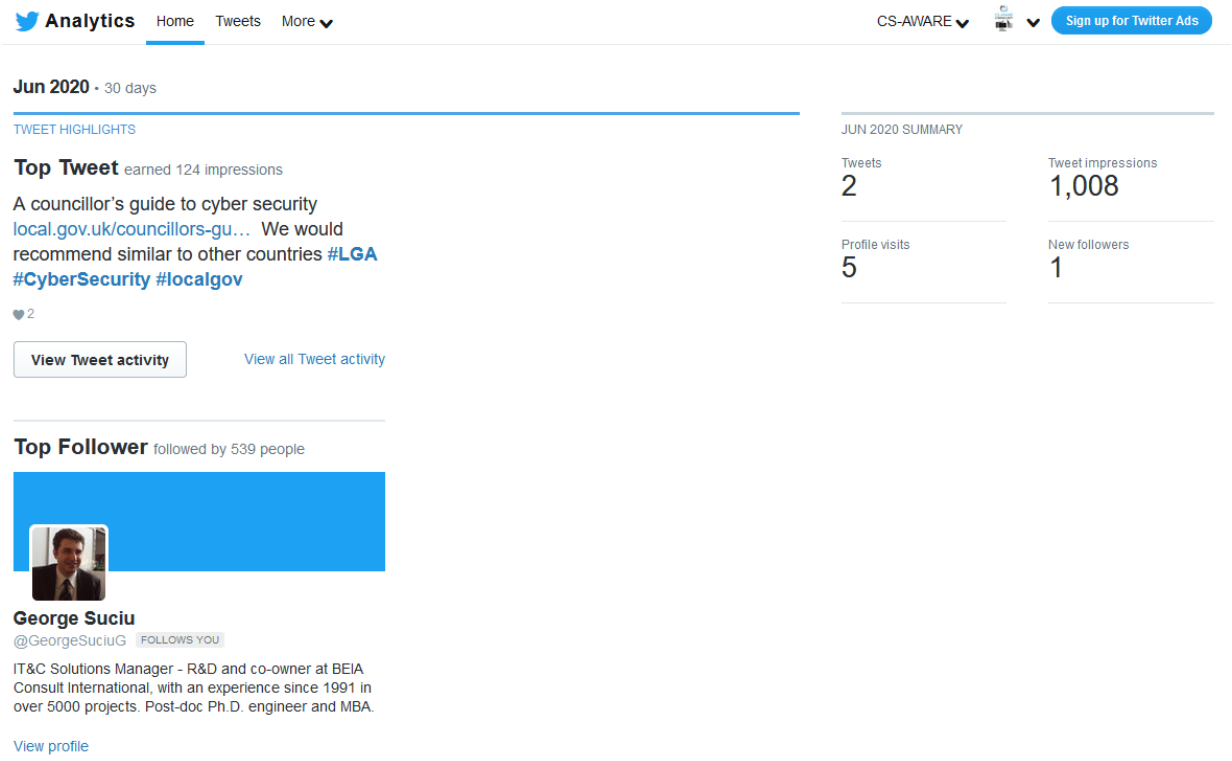

Figure 3: Tweet impressions screenshot from CS-AWARE twitter account analytics – June 2020

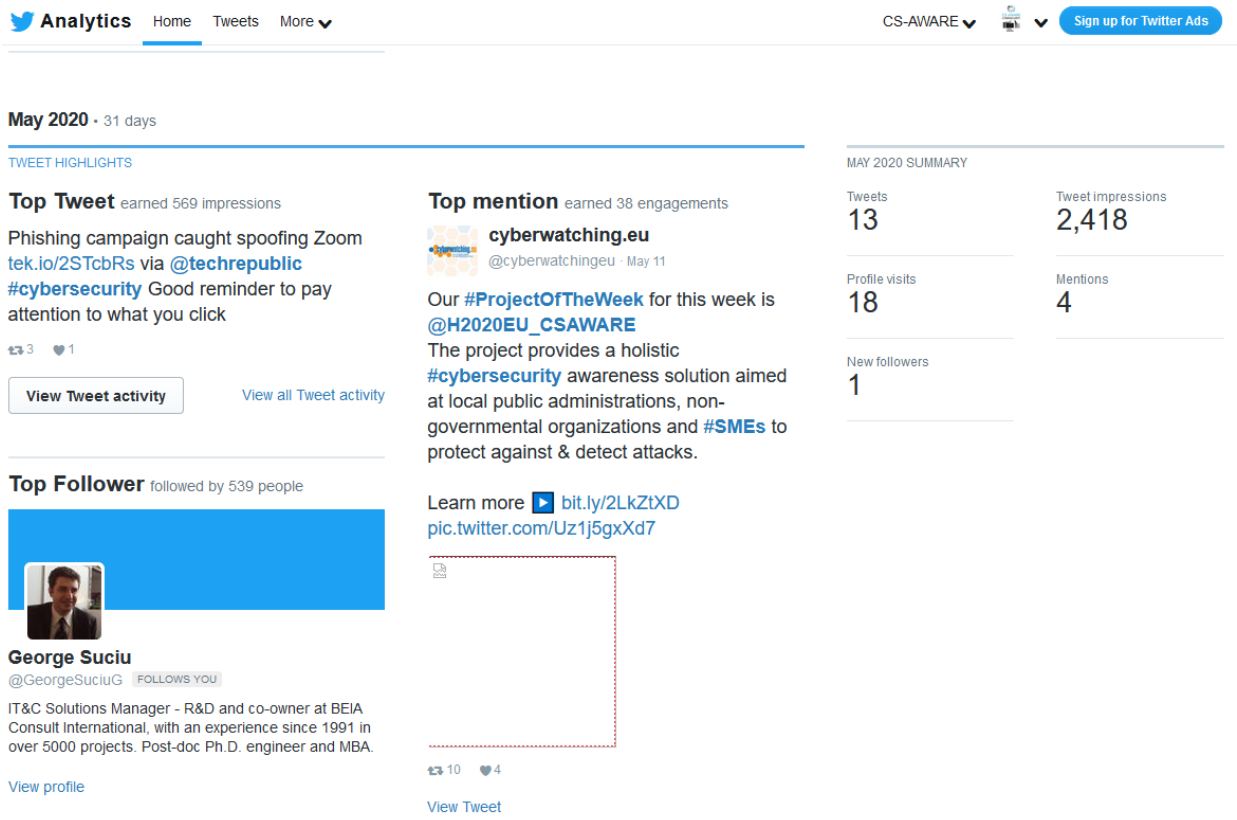

Figure 4: Tweet impressions screenshot from CS-AWARE twitter account analytics – May 2020

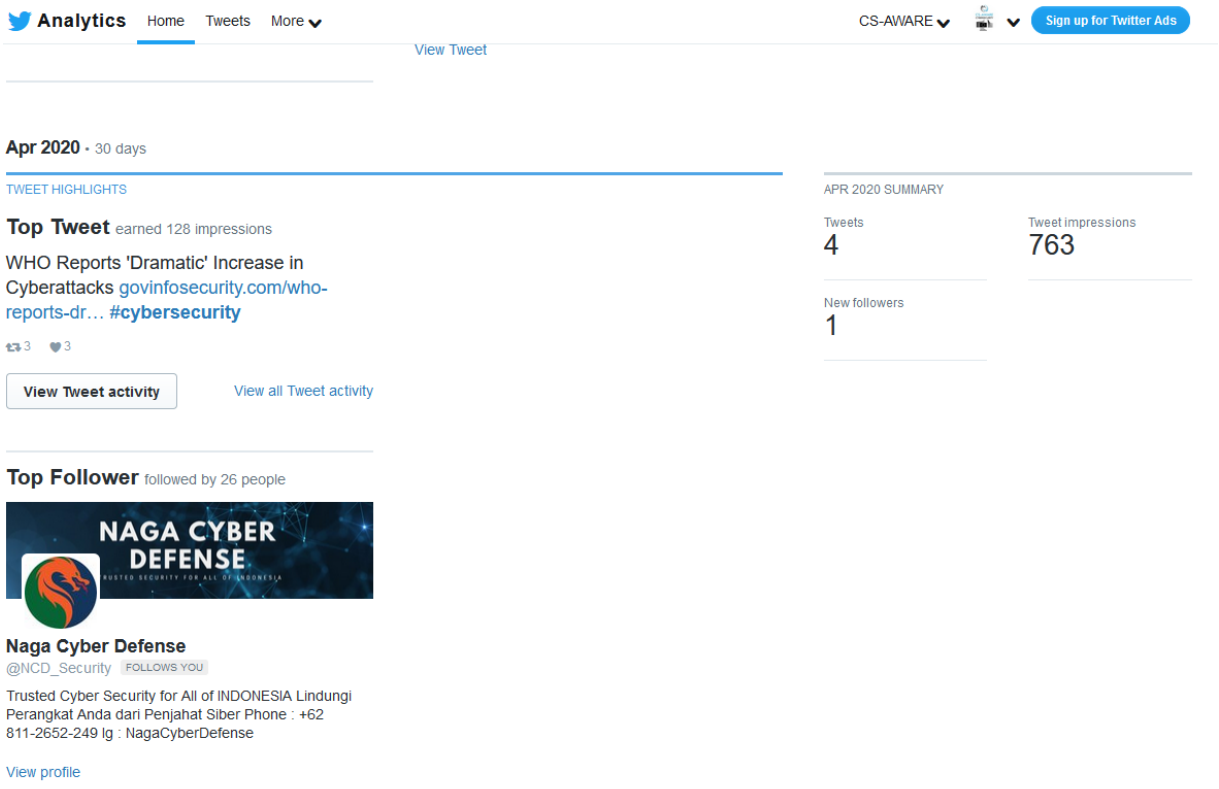

Figure 5: Tweet impressions screenshot from CS-AWARE twitter account analytics – April 2020

Next, we present Facebook statistics on impressions:

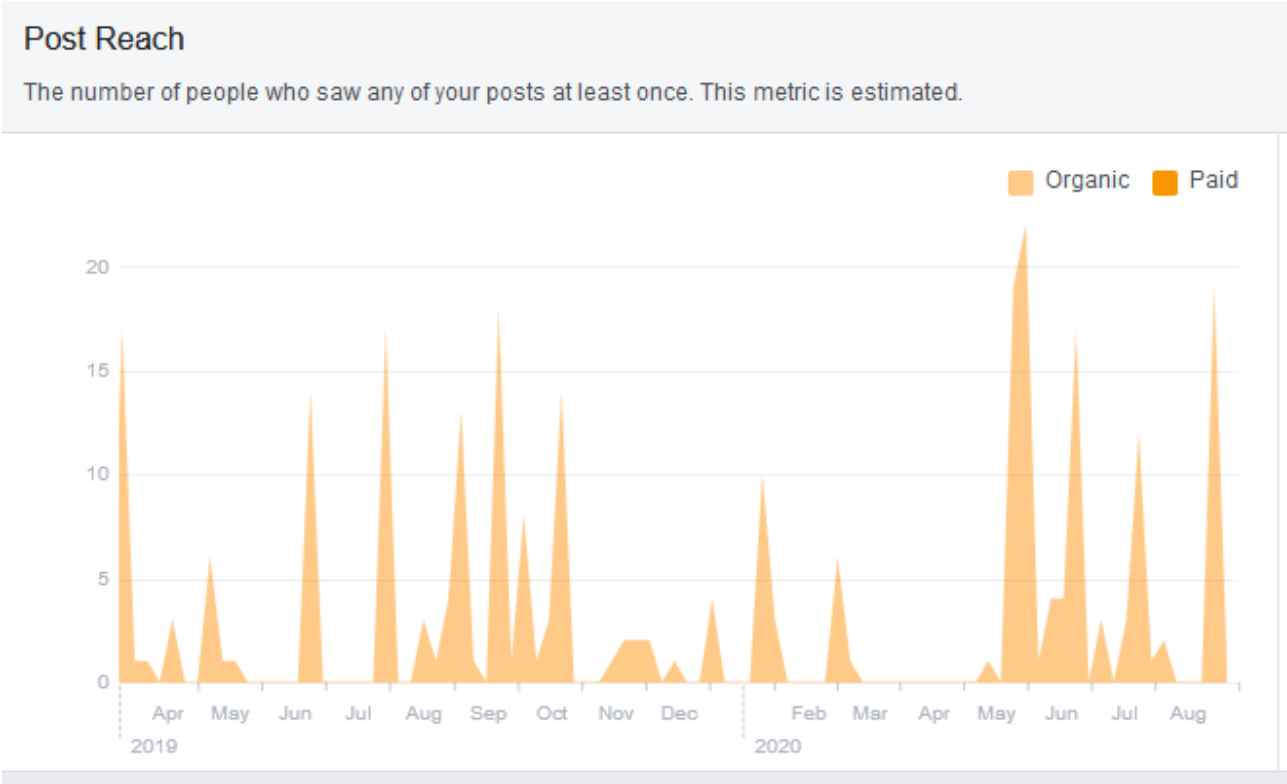

Figure 6: Facebook Post reach during the last reporting period

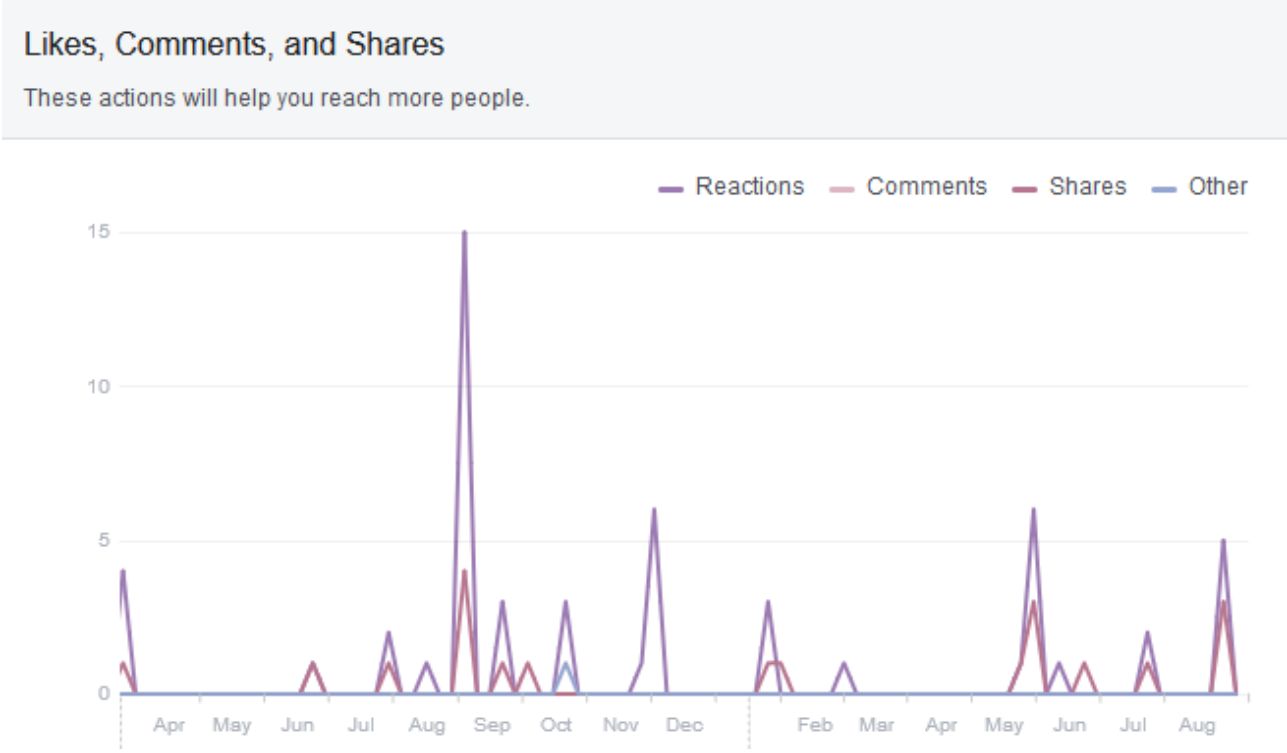

Figure 7: Facebook likes, comments and shares for the last reporting period

2.4 Blog publications

The blog publication on the project website continued sustained over the last period of the project reaching more than 120 published blogs for the duration of the 3-year project. The blog will be taken over by the spin-out team from September 2020 ongoing and continued on the new company website.

2.5 Leaflet and poster

There was no change to both documents. The leaflet and poster template will be taken over by the spin-out team from September 2020 ongoing. Since the last reporting period it was created a pitch deck, comprehensive for both sales and investor use. The pitch deck will be used and further developed after the project ends.

2.6 Seminars, networking events and training

During the last reporting period, the consortium had various events that attended and planned to attend as listed below:

	Name	Event	Date	Link
1	4th Annual Version2 Info-security Conference	Meeting 3000+ Cyber Security professionals from all fields.	May 1-2, 2019	
2	6th Annual Cyber Security Summit	200 + Cyber Security professionals from the UK Public Sector	July 9th 2019	
3	Meeting Local public administration in Fowey, UK	Reception for Mayor of Fowey and others, presentation of the CS-AWARE project	September 17th 2019	
4	Greek ministry of interior security training course, Athens, Greece	CS-Aware was presented to IT people from 18 municipalities from Greece. The cyber security department's manager of the ministry attended, and is interested to invite us for detailed presentation in the ministry. The first thought was that it could be a ministry's recommendation to municipalities in Greece. Next meeting with the cs manager is for 22/11 in Larissa in order to demonstrate the solution.	October 29 - 31 2019	
5	CrIM19	The international Crisis Management workshop CriM gathers teachers, researchers, experts and students of cybersecurity annually to study pressing issues of security and privacy of our digital systems. Respected international and Finnish lecturers combined with practical workshops each day bring important insights of the current world to students interested in cybersecurity. In the 2019 edition of the workshop, the event focuses on changing critical infrastructure and ways to develop more efficient measurements of security with the aid of machine learning in an increasingly interconnected world: We inspect how	October 30th , to , November 1st , 2019	https://www.oulu.fi/bisg/crim

		legislative regulations like GDPR can impact to digital service providing and their security now that the Finnish data-protection laws have been established. We take a closer look on popularity gaining technologies security such as IoT and Cloud. We also talk about adapting more efficient defence mechanisms for current threats, like trusted systems adaptation to cloud and game-theory's adaptations to security like evaluating obscure threats with their probability distributions.		
6	11th OTS Forum	The 11th annual OTS Greek Forum took place in Ioannina, where hundreds of representatives from Greek public organisations attended it (approximately 580 representatives, from over 100 public organisations, such as ministries, municipalities, regions, water utilities, legal public entities and academic institutions). The main agenda of the Forum was focused around innovative products and services that could improve the operation of public organisations. InnoSec and the Municipality of Larissa gave a joint presentation about the core functionality of CS-AWARE and the latest project developments. Emphasis was given on the added value it will have for LPAs IT staff, by giving examples of real incidents that the currently-installed defence mechanisms failed to detect. It was then explained how the CS-AWARE system could assist in resolving the aforementioned issues.	November 7th-9th, 2019.	https://otsforum.gr/%CF%80%CF%81%CF%8C%CE%B3%CF%81%CE%B1%CE%BC%CE%BC%CE%B1/
7	The Finnish EU Presidency conference: The European Union's Role In Global Cyber Policy	100 diplomats and high-level officials from the EU. We showcased and demonstrated our project to the participants in all breaks of the conference.	November 8th, 2019	
8	Meeting with a group of mayors from Sardinia with Cagliari Mayor Cagliari, Italy	Presentation of the CS-AWARE	November 16th, 2019	https://www.cagliaripad.it/421658/cagliari-appuntamento-col-progetto-di-cybersicurezza-per-comuni-piccole-e-medie-imprese/
9	Cybersecurity Tech meeting, Paris, France	Cybersecurity Tech meeting - by Paris Region: presentation and pitch of CS-AWARE solution to local industry; 1to1 discussions; Peracton invited to present and pitch	December 12th, 2019	
101	The 5th International Conference on Next Generation Computing 2019	Conference Keynote by Gerald Quirchmayr "The Need to Counter Present and Expected Information Security Challenges". The CS-AWARE Approach was presented as example for situational awareness creation.	December 19th - 21th 2019	http://www.icngc.org/

11	LPA meeting Barletta, Italy	Meeting with a group of Italian mayors - Presentation of the CS-Aware	January 21st 2020	https://www.batmagazine.it/news/2020/01/21/barletta-presentazione-di-cs-aware-un-progetto-per-la-cybersicurezza-dei-comuni-e-delle-pmi/
Dissemination Events during the COVID-19 pandemic / EU lockdown period				
12	Cyberwatching.eu Marketplace	CS-AWARE project qualified and was registered in the Cyberwatching.eu Marketplace product list This registration is particularly useful for the spin-out as a follow-up opportunity, reference point and a potential source of prospective clients.	March 2020	https://www.cyberwatching.eu/market-products-list https://www.cyberwatching.eu/projects/959/cs-aware/products/cybersecurity-awareness-solution-local-public-administrations
13	H2020 Booster service	The consortium attended a seminar organized by Booster Service and was made aware of its services. Particularly it was important the knowledge that the Booster services can also be availed after the project ends and this is clearly the plan of the spin-out team to join it and avail of it from September 2020 ongoing.	May 2020	https://www.horizonresultsbooster.eu/
14	Serenity Cybersecurity Network Ireland	Peracton distributed via Enterprise Ireland the newsletters published by consortium to the Serenity Cybersecurity Network - a network organized by Enterprise Ireland that is made of all research and companies' entities in Ireland activating in the cybersecurity space.	July 2020	via e-mail/mailing list driven by Enterprise Ireland
15	Networking with other EU H2020 Projects	our consortium attended a cluster meeting organized by Cyberwatching.eu https://escape.trust-itservices.eu/news-events/news/boosting-synergies-improve-market-readiness-levels-projects where we actively interacted in the second cluster meeting. There has been agreed to continue the cooperation between the CS-AWARE spin-out and Cyberwatching.eu,; Peracton followed up directly with some other members of the cluster meeting for the financial market commercialization direction and agreed to have regular discussions in the coming months as there has been identified a good and complementary match of interests.	July-August 2020	

		CANCELLED EVENTS DUE TO COVID-19		
1	Major Cities of Europe annual conference, Larissa Greece	Major Cities of Europe annual conference - • CS-AWARE is part of Larissa presentations • CS-AWARE has a booth for the whole conference duration	May 27th -29th 2020	(postponed/cancelled due to COVID-19
2	IPICS summer school 2020	• Half day workshop with IT security students (mainly PhD level), introducing them to CS-AWARE SSM analysis and technical components	July 13th -24th 2020	
3	Planning for a meeting with the municipalities of Fiumicino, Cerveteri, and Tivoli (Rome's metropolitan area) .		Early Spring (March or April)2020	
4	Initial contacts made in March (Italy) and will be followed up between March and April.		Spring 2020	
5	Initial contacts made in Catania - Sicily Region (Italy) and will be followed up between March and April.		Spring 2020	
6	Initial contacts made in Spain (Malaga Metropolitan area) and will be followed up in summer 2020.		Summer 2020	
7	Initial contacts in the Piedmont Region (Italy) and will be followed up in summer 2020.		Summer 2020	
8	10th International Conference in Methodologies and Intelligent Systems for Technology Enhanced Learning	Jerry Andriessen to present a paper on CS-AWARE at the Workshop on Technol	Summer 2020	
Dissemination Events after the end of the project (31st August 2020)				
1	CS-AWARE Newsletter published in German by University of Vienna	Mit CS-AWARE für mehr Cybersicherheit		https://medienportal.univie.ac.at/uniview/forschung/detailansicht/artikel/mit-cs-aware-fuer-mehr-cybersicherheit/

2	Rheasoft Meeting with EU MEP Pernille Weiss/EP Research Committee	CS-AWARE project outcomes presented within a wider discussion about Danish SMEs in H2020	3rd November 2020	https://www.eppgroup.eu/about-us/members/pernille-weiss
3	Joining of the Danish Police data sharing group against IT Economic Crime by Rheasoft	Rheasoft joined this group for data access, networking as well as for future potential leads for the benefit of the spin-out.	3rd November 2020	https://politi.dk/samarbejde/fit-forum-mod-it-relateret-oekonomisk-kriminalitet
4	Interview with CORDIS Research.eu magazine	University of Oulu was interviewed as coordinator of the project by CORDIS Research.eu Magazine	18th November 2020	https://cordis.europa.eu/research-eu/en
5	Networking with Geiger project	Cesviter Consulting got in touch with Geiger EU H2020 project and discussed potential synergies. It will be followed up also via the spin-out.	19th November 2020	https://project.cyber-geiger.eu/
6	Critical Chains Webinar Workshop: "Financial Sector infrastructure cyber-physical security and regulatory standards"	The event was organized online by Critical Chains H2020 EU prokect (grant No 8333326) in collaboration with Cyberwatching.eu, Soter, Concordia, Cybersecurity for Europe projects. It was a 5 hour web based workshop focused on Cyber Security, Regulation and Challenges in the Financial sector. CS-AWARE was presented by Peracton in the context of eGovernment type application with potential of usage on the financial markets.	December 14th 2020	https://research.reading.ac.uk/critical-chains/wp-content/uploads/sites/130/2020/12/Financial-Sector-Cyber-Security-Regulatory-Challenges-Workshop-14th-Dec2020-v15.pdf
Participation in future events after the end of the project (31st August 2020)				
1	12th OTS Forum	It will be the follow-up attendance of the OTS forum in2021	TBD	TBD
2	CriM2021 (Cyber Security Seminar and Workshop: CS-AWARE has planned a presentation and/or workshop about the systems and methodologies developed in CS-AWARE	The international Crisis Management workshop CriM gathers the teachers, researchers, experts and students of cybersecurity annually to study pressing issues of security and privacy of our digital systems. Respected international and Finnish lecturers combined with practical workshops each day bring the important insights of the current world to students interested in cybersecurity.	TBD	- https://www.oulu.fi/bisg/crim)
3	Major Cities of Europe annual conference, Greece	In 2021 CS-AWARE consortium members plan to attend this annual conference in Greece	TBD	TBD

Table 2: Events and dissemination activities

2.7 Publications

Next, we present all the project's publications for March 2019 - August 2020 period:

No	Date	Title of Publication / Presentation	Name of Journal / Conference	Additional Material / Info
1	2019-01-27	Exploring Knowledge Graphs in an Interpretable Composite Approach for Text Entailment	Thirty-Third AAAI Conference on Artificial Intelligence (AAAI-19), January 27 – February 1, 2019, Honolulu, USA.	(Mentioned here as not completely listed with open access in the previous reporting) Publication: aaai2019_VSetal_camera-ready.pdf Open access: https://www.alexandria.unisg.ch/255897/
2	2019-06-01	A Cybersecurity Situational Awareness and Information-Sharing Solution for Local Public Administrations based on Advanced Big Data Analysis: The CS-AWARE Project, Challenges in Cybersecurity and Privacy – the European Research Landscape	River Publishers Series in Security and Digital Forensics	DOI: 10.13052/rp-9788770220873 Open access: https://uscholar.univie.ac.at/detail/o:1076812
3	2019-08-29	A quantitative evaluation of trust in the quality of cyber threat intelligence sources	14th International Conference on Availability, Reliability and Security (ARES 2019) – Canterbury, United Kingdom, 26–29 August 2019	DOI: 10.1145/3339252.3342112 Open access: https://uscholar.univie.ac.at/detail/o:1076811
4	2019-08-29	Enhancing credibility of digital evidence through provenance-based incident response handling	ARES '19 Proceedings of the 14th International Conference on Availability, Reliability and Security ACM New York, NY, USA, 26-29 August 2019	DOI: 10.1145/3339252.3339275 Open access: https://uscholar.univie.ac.at/detail/o:1076814
5	2019-10-30	An Information Flow Model to Support NIS Mandated Reporting	Autonomous Systems 2019: An Almanac 137-143, 12th Conference on Autonomous Systems – Cala Millor, Mallorca, Spain, 23-30 October 2019	Open access: https://tinyurl.com/y4txxkfw
6	2020-03-06	Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem	Computers	vol 9(1), 2020, article number 18 DOI: 10.3390/computers9010018

				Open access: https://zenodo.org/record/3700832#.YAG_-zmSlaR
7	2020-07-10	An Innovative Self-Healing Approach with STIX Data Utilisation	17th International Conference on Security and Cryptography (SECRYPT 2020). Lieusant, Paris, 8-10 July 2020	Conference website: http://www.secrypt.icete.org/ DOI: 10.5220/0009893306450651 Open access: https://zenodo.org/record/3961680

Table 3. CS-AWARE Publications list

3 Exploitation and commercialization plan and actions

The commercialization and exploitation of CS-AWARE was agreed by consortium partners to continue after the project conclusion in two main directions: A) spin-out focusing on the EU LPAs market and B) individual commercialization initiative driven by some project partners on other markets than EU LPAs one as described next.

3.1 Spin-out creation for targeting the EU LPAs market

The spin-out creation was discussed and debated from the early phases of the project as a possible commercialisation path.

The consortium balanced the pros and cons on such initiative and decided during the last period of the project to go ahead with setting up commercial vehicle, namely a new company in Estonia. The new company official registration is expected to be done sometime during October 2020, given all administrative processes in Estonia go smoothly.

With the exception of Roma Capitale and Larissa Municipality, all the other partners are involved and committed in various ways to the spin-out success.

3.2 IPR Policy in the Spin-out context

The IPR policy will be the following: for the spin-out benefit, all partners will licence the needed IP and give rights of use in favour of the spin-out, once the new company is incorporated for the desired market segments. For the direct commercialization actions, the required IPR will be discussed and agreed between individual partners as needed.

3.3 Technology in the context of commercialization

There has been no significant change since Version 2 of this deliverable.

3.4 Further industry analysis – EU wide.

As an EU wide overview is necessary, this section presents updated information (2019-2020) relevant for various European countries of potential interest for the follow-up commercialization actions after the end of the project. The next information has been extracted and quoted from the original sources and will be in particular of benefit for the new spin-out, that can distil it further as needed.

3.4.1 EU Cybersecurity readiness: HISCOX Cyber readiness report 2019

Hiscox [3] commissioned Forrester Consulting in 2019 to assess organisations' cyber readiness. In total 5,392 professionals involved with their organisation's cyber security strategy were contacted (1,000 plus each from the UK, USA and Germany, and 500 each from Belgium, France, Spain and The Netherlands). Thirty-nine percent of respondents were from organisations with fewer than 50 employees (small firms), 16% from medium sized firms employing 50-249 people, 16% from large firms employing 250-999 personnel and the remaining 28% from enterprises with 1,000 or more employees. Respondents completed the online survey between 22 October and 7 December 2018.

Next we present 'Cyber Readiness Stalls' as identified by Hiscox:

Loss figures impacted by large incidents The figures above are strongly influenced by a sharp rise in the cost of the biggest single incident reported. The mean cost has jumped from $34,000 a year ago to a fraction under $200,000. For large firms, there has been an 18-fold rise to $395,000. The comparable figure for small firms is $9,000, up from $3,000 in 2018.	**German firms hit hardest – for the second year running** Mean cost for all incidents experienced in Germany during the year was over $1 million for medium and large firms rising to over $1.5 million for enterprise-scale businesses.	**Cyber security spending up 24%** The average spend on cyber is now $1.45 million and the pace of spending is accelerating. The total spent by the 5,400 firms in our report comes to a remarkable $7.9 billion. Two-thirds of respondents say they plan to increase their spending on cyber by 5% or more in the year ahead.
More firms fail the cyber readiness test Our quantitative model of cyber readiness shows a small decline this year in the proportion of firms achieving 'expert' scores for their cyber strategy and execution – down from 11% to 10%.	**Two factors account for the fall in readiness scores** The first-time inclusion of French firms has reduced overall scores. There has also been a drop in the number of large (with 250 to 999 employees) and enterprise firms (1,000 plus) in the USA and Germany that achieve top scores.	**Cyber attacks reach a new intensity** More than three out of five firms (61%) reported an attack in the last year – up from 45% the previous year. The frequency of attacks has also increased. Among the seven countries, Belgian firms are the most likely to have been attacked, US firms the least likely.
Cyber losses soar The mean figure for losses associated with all cyber incidents among firms reporting attacks has risen from $229,000 last year to $369,000 – an increase of 61%, with medium and large firms bearing a disproportionate amount of the cost.	**Supply chain incidents now commonplace** Nearly two-thirds of firms (65%) have experienced cyber-related issues in their supply chain in the past year. Three quarters of technology, media and telecoms (TMT) and transport firms have been hit.	**More small firms attacked this year** While larger firms are still the most likely to suffer a cyber attack, the proportion of small firms (less than 50 employees) reporting one or more incidents is up from 33% to 47%. For medium sized firms with between 50 and 249 employees the proportion has leapt from 36% to 63%.

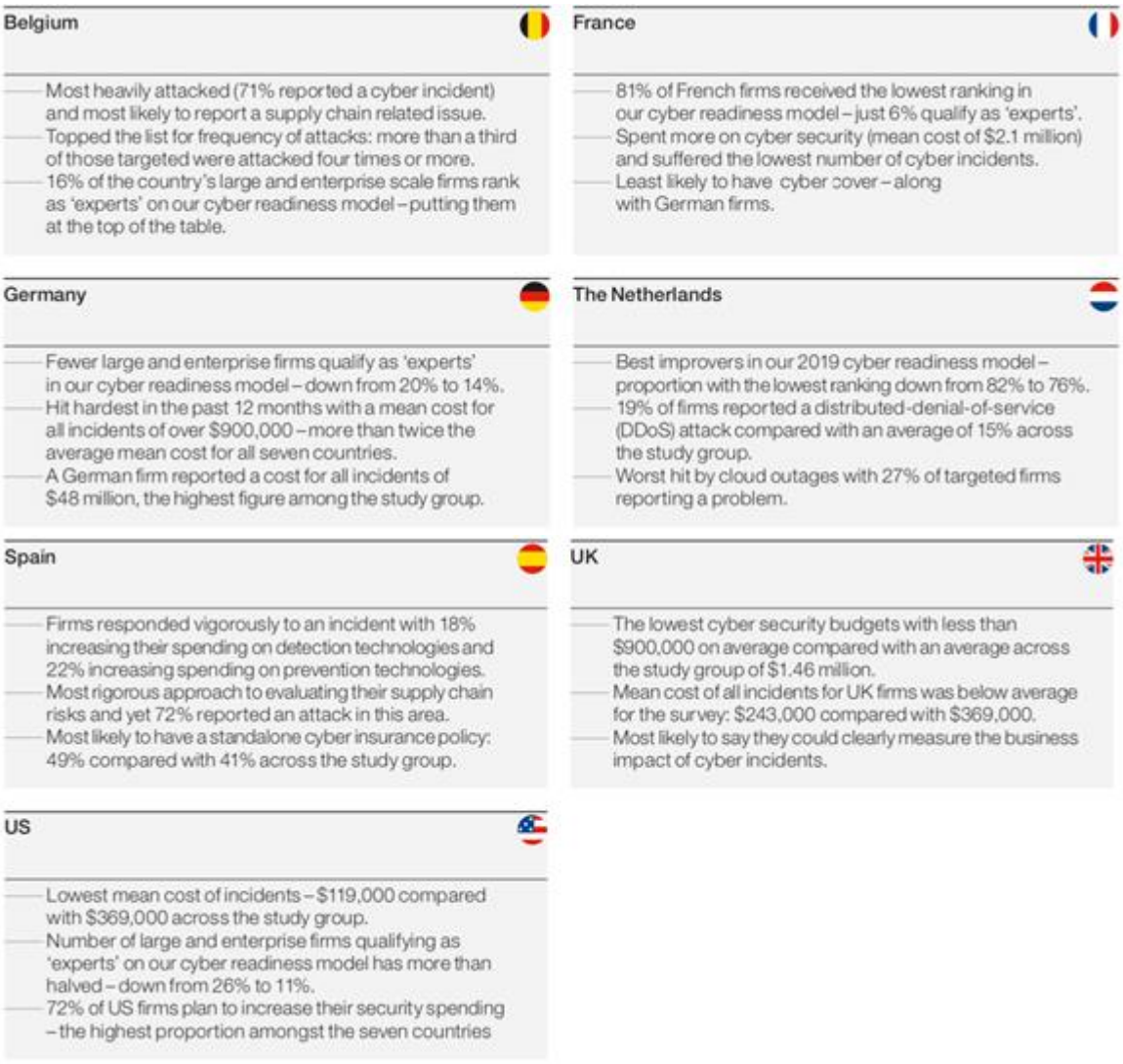

Figure 8: cyber readiness situation 2018-2019 by Hiscox [3]

3.4.2 Type of attacks

In every one of the 15 sectors tracked in this report, the proportion of firms reporting one or more attacks has risen sharply. Across all seven countries, the most heavily targeted sector was TMT (technology, media and telecoms), where 72% of respondents reported one or more attacks, up from 53% a year ago. Government entities came second (71% reporting an attack, up from 55%), followed by financial services (67%, up from 57%).[3] Nearly two-thirds of respondents (65%) said they had experienced one or more cyber-attacks as a result of a weak link in their supply chain over the past year. The figures were highest in Belgium and Spain (73% and 72% respectively). Overall, three-quarters of TMT and transport firms were targeted. Just over half of all firms in the study now include cyber KPIs in their contracts with suppliers. The figure is 65% among enterprise firms but only 39% among small firms. [3]

Asked how often they evaluated the security of their supplier networks, nearly three quarters of firms (74%) said they did so at least once a quarter or on an ad-hoc basis. Spanish firms look the most prudent in this area: nearly half (47%) said they evaluated the cyber security of their suppliers once a month compared with 32% of respondents overall. 8% of firms said they had increased evaluation of their supply chain as a result of an incident in the past year, with the figure highest among financial services firms (12%). [3]

Many more respondents this year report problems with outages from third-party cloud providers (22%, up from 13%). Dutch firms were worst hit, with more than 27% of those that suffered cyber incidents reporting cloud outages, while across the respondent pool large and enterprise firms are more likely to suffer a cloud-related incident at 27% and 22% respectively. This doubtless reflects the propensity for firms to push more of their data into the cloud as they grow. [3]

3.4.3 Cyber Losses

Of the 3,300 firms in our survey that suffered attacks, around 2,250 tracked the costs to their business. Counting all incidents suffered over a 12-month period, the mean cost to those businesses rose from $229,000 to $369,000 – an increase of 61%. Assuming a similar experience among those firms that failed to track or quantify the impact of cyber-attacks, the total cost for all 3,300 targeted firms was around $1.2 billion. Adjusting for the increase in both the scale of the study group this year and the numbers targeted, that is more than double the cost registered in last year's report.

Averages tell only part of the story, of course. While nearly half (47%) of small firms have suffered a cyber-attack in the past 12 months (up from 33% in 2018), the mean cost of all incidents suffered has actually halved – from $29,000 to $14,000. However, the reverse is true for medium and large firms which have borne a disproportionate cost this year, often multiples of the previous year. This is the case for the UK, France, Spain and The Netherlands in particular.

One of the most striking figures to emerge is the mean cost of the largest single incident. A year ago, this came out at $34,000. This year, there has been a near six-fold increase – to a fraction under $200,000. For companies in every size bracket the cost of the biggest incident is now likely to be anything from three-to-18-times what it was only a year ago. The figures tally with broader industry data that suggest a sharp rise in the scale of ransom demands, for example, over the past year. Overall, German businesses appear to have suffered worst with a mean cost for all incidents experienced in the year of over $1 million for medium and large firms and over $1.5 million for enterprise-scale businesses. It is also a German firm that reported the highest cost of all incidents – $48 million. There is a similar story when it comes to the cost of the largest single incident, with a mean figure for the largest German companies nearly ten times that of their French or Spanish counterparts– $776,000 compared with $78,000 and $82,000 respectively.

At the other end of the spectrum, US firms appear to have got off lightly. For medium and large firms, the mean cost of all incidents is barely $100,000; for enterprises the figure is $213,000. This is despite a sharp drop (from 26% to 11%) in the number of large US firms that get top ranking in our cyber readiness model. One explanation is that US firms were far less exposed to the loss of customer or employee data, or to the theft of intellectual property (IP), trade secrets or research and development (R&D) in the past 12 months. For instance, twice as many French firms (16%) reported a data breach resulting in the loss of employee data as US ones (8%). The average cost of all incidents has reduced in the past year in just five of the 15 sectors tracked (professional services, energy, retail and wholesale, food and drink and government related) and even there the average cost of the single largest incident has risen sharply.

3.4.4 Cyber readiness by country

More than four-fifths of French firms (81%) are in the novice category. Along with The Netherlands, France has the smallest proportion of large and enterprise firms that rank as experts, at 9%. Overall, US, German and Belgian firms score highest – with around a 10% overweighting towards experts. However, there has been a dramatic decline in the number of large and enterprise firms in both the USA and Germany that qualify for expert status. In Germany, the proportion is down from 20% to

14%; in the USA it is down from 26% to 11%. The USA and German figures are the main reason for an overall fall in the number of experts among large and enterprise companies this year – from 21% to 12%. Nearly three-quarters of them (73%) now rank as novices. That compares with 61% a year ago. Given the resources at their disposal and the much higher security budgets they deploy, this comes as something of a surprise.

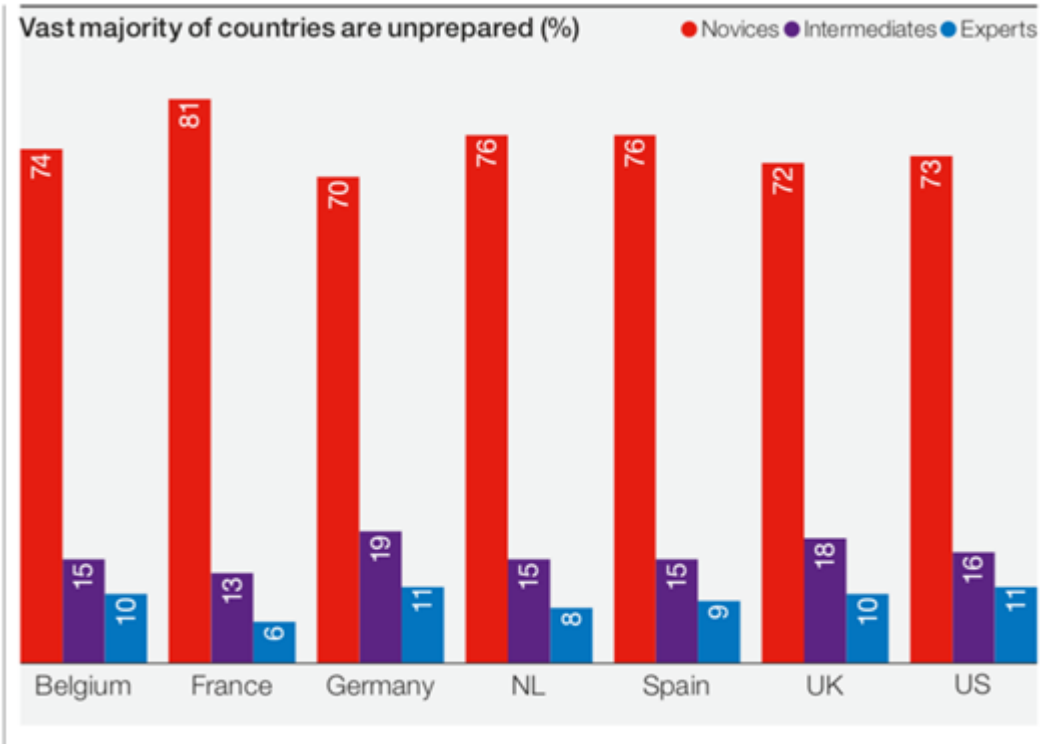

Figure 9: Preparedness level in cybersecurity at country level

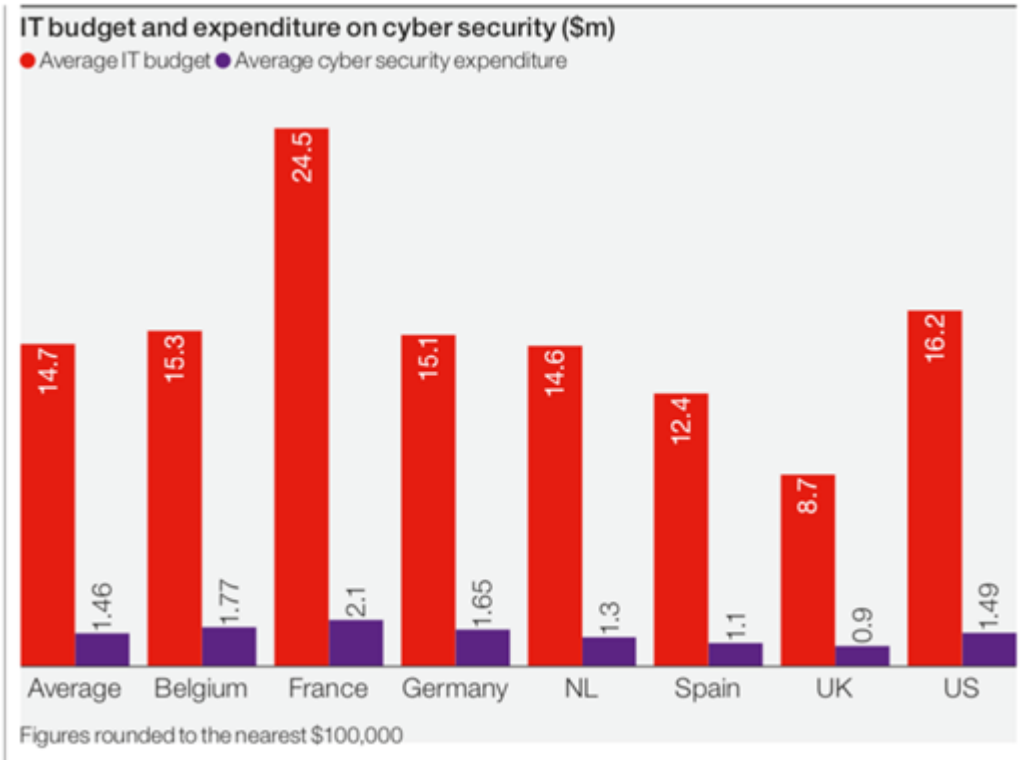

Figure 10: IT budgets on cybersecurity at country level

3.5 Market opportunity

Our focus (within the past and current version of this document) is particularly set on 3 countries Greece, Italy and the UK. This is because while the first two are countries where the two pilots have been implemented and there is also a local business network in place, the UK (in spite of the Brexit uncertainties) is the biggest cybersecurity market in Europe and so, a primary market target for the future spin-out.

As CS-AWARE platform falls into the SIEM category, according to Research and Markets, SIEMs and related technologies were a $5.3 billion market in 2018, and the market is expected to grow at a compound annual growth rate of 19.7 percent – to $12.9 billion by 2023. SIEMs are the fastest-growing segment of the market, the analyst company said see https://www.datacenterknowledge.com/security/siem-pricing-models-set-shake

3.5.1 Italian market and cybersecurity

Italy's economy comprises a highly developed industrial north, dominated by private companies, and a less-developed, highly subsidized, agricultural south, with a legacy of unemployment and underdevelopment. The Italian economy is driven largely by the manufacture of high-quality consumer goods produced by small and medium-sized enterprises, many of whom are family-owned (comprising over 99% of Italian businesses and producing around 68% of the national GDP). Italy also has a sizable underground economy, which by some estimates accounts for as much as 17% of GDP. These activities are most common within the agriculture, construction, and service sectors.

The Italian cybersecurity market is largely driven by investments of larger companies, where most of the top management has become more aware of the increasing risk of intrusion into their business information systems. Italian firms are also becoming more concerned about threats to data confidentiality, integrity, availability, and authentication. The financial and utility sectors are generally the top end-users of ICT security in Italy, followed by defence, national and local government, manufacturing, transportation, and sectors. Medium-sized companies, which are a significant portion of Italian enterprises, and to a lesser extent smaller companies, are increasingly in recent years investing in security. However, there remains resistance on the managerial level to expenditures for cybersecurity security activities due to the perception in both business and government sectors that security is a cost rather than an investment.

The following table illustrates the complicated nature of the Italian market [4]and how the potential market for many cybersecurity solutions is limited to a small number of firms:

	Distribution of firms in Italy	
	By firm size	
	Firm size (employees) Number %	
All firms	3,867,813	100.0%
SMEs (0-249)	**3,864,582**	**99.9%**
* Micro (0-9)	3,660,256	94.6%
* Small (10-49)	184,925	4.8%

* Medium (50-249)	19,401	0.5%
Large (250+)	3,231	0.1%
Note: Data does not include financial and insurance businesses.		

Table 4: Firms distribution in Italy

In recent years, the government is starting to recognize cybersecurity as a national priority [6], [7]. In February 2016 the Italian government presented the first-ever National Cyber Security Framework (NCSF) which was developed from the Framework for Improving Critical Infrastructure Cybersecurity compiled by the U.S. National Institute of Standards and Technology (NIST) [8], [9]. The voluntary framework was meant to serve as a common frame of reference to identify existing and future standards and regulations. According to the Cyber Intelligence and Information Security Centre of the Sapienza University in Rome, city governments, local units of the National Healthcare System, and public hospitals are still the most vulnerable to cybersecurity threats. The Director of the Postal Police (the ones charged with national cybersecurity) has expressed interest in numerous occasions in establishing in each region a contact point for cybersecurity activity. She, too, perceives local governments and other affiliated agencies as weak points in the chain. Since local government is the one agency charged with overseeing the personal data of citizens throughout the lives of citizens, it is imperative, according to the Director, to make the protection of this data a priority. Once CS-AWARE has a more market-ready presence we will contact the Director to discuss possible opportunities for further action.

Larger businesses increasingly perceive cybersecurity as a core business requirement and security spending has been growing and will certainly continue to grow across the board, particularly in those areas which need to be improved to reduce vulnerability [10]. The most important market drivers for cybersecurity include [11], [12], [13]:

1) Increased security awareness and willingness to comply with current legislation regarding cybersecurity;
2) Challenges arising from the adoption of new technologies and business models requiring the implementation of security measures such as secure mobility and virtualization;
   3) New government measures and investments to protect the digital identity of citizens and critical infrastructure from increasing cyber assaults;
3) The implementation of Italian legislation calling for security measures to protect the privacy and personal data of citizens and compliance with national and international norms like EU General Data Protection Regulation (GDPR); and
   5) The implementation of industry-specific legislation, calling for compliance with national and international norms.

A common characteristic of all these market drivers is an increasing awareness in some select sectors of the importance of cybersecurity but not necessarily accompanied by a concerted effort to dedicate resources and staff to facilitate change.

Italy is the third-largest economy in the eurozone, but its high public debt and structural impediments to growth have continued to keep it vulnerable to pressures from financial markets. Public debt has been increasing steadily since 2007, reaching 131% of GDP in 2017. The government faces pressure from investors and other European partners to sustain its efforts to address Italy's longstanding

structural economic problems, including labour market issues, an inefficient and cumbersome judicial system, and a weak banking sector. By the end of 2020, Italy's unemployment rate will have risen, it is predicted to 12.4% wiping out four years of slow improvement. Predictions are that if the pandemic is contained the unemployment could gradually fall back down to 2021. Youth unemployment remains a concern that the Government at all levels still needs to address.[10]

It should be remembered that despite the existence of the EU common market, the cultivation and maintenance of personal relationships are still a vital part of doing business in Italy. Finding the right local agent, distributor, or business partner remains essential to enter the Italian market. It is rarely effective to rely on agents or distributors in neighbouring markets. At least within the LPA sector, this issue is not that uncommon in other countries in Europe. In small and medium-sized LPAs across Europe, experience has shown that most municipal leaders prefer to deal with local or regional contacts [13].

3.5.2 UK market and cybersecurity

At the end of January 2020, the Department for Digital, Culture, Media & Sport (DCMS) announced that "the UK's cyber security industry is worth an estimated £8.3bn, an increase of 46% from £5.7bn in 2017". The findings from the Department's research report [2] show:

- The number of active cyber security firms in the UK has increased 44 per cent – up from 846 in 2017 to over 1,200 at year-end 2019. This growth is the equivalent to a new cyber security business being set up in the UK every week
- There are now approximately 43,000 full time employees working in the cyber security sector, up 37 per cent from 2017
- Total revenues within the sector have increased by 46 per cent to an estimated £8.3 billion. On average, revenue per employee reached £193,500 – an increase of 7 per cent since 2017
- 2019 was a record year for the sector with more than £348 million of investment
- Over the last four years (2016-19), total investment identified within the cyber security sector has exceeded £1.1 billion, demonstrating how confidence has grown in the industry.

The UK public sector has in excess ***of five million members of staff*** – and so, it is much more exposed to the security vulnerabilities caused by security mistakes, inadequate training, and criminal activity from within. Despite the understandable focus placed on criminal cyberattacks targeting organisations from the outside, employees remain the largest security risk in any organisation. A primary group is careless users - those who accidently reveal information that helps others carry out attacks, much of which is due to lack of awareness about how to minimise risk. The problem is further exacerbated by today's bring-your-own-device (BYOD) culture, when employees can easily access and share sensitive information from a range of secured and unsecured devices. To prevent insider breaches - especially accidental ones - internal users must be vigilant. And to be vigilant, they need to know how to behave.

3.5.2.1 Reported breaches by company size

Around a third (32%) of businesses and two in ten charities (22%) report having cyber security breaches or attacks in the last 12 months. As in previous years, this is much higher specifically among medium businesses (60%), large businesses (61%) and high-income charities (52%).

Among this 32 per cent of businesses and 22 per cent of charities facing breaches or attacks, the most common types are:

- phishing attacks (identified by 80% of these businesses and 81% of these charities)
- others impersonating an organisation in emails or online (28% of these businesses and 20% of these charities)
- viruses, spyware or malware, including ransomware attacks (27% of these businesses and18% of these charities).

3.5.2.2 Decline in reported breaches

For businesses, the proportion identifying breaches or attacks (32%) is lower than in 2018 (when it was 43%) and 2017 (46%). The charities result is similar to 2018. At the same time, among the 32 per cent of businesses that did identify any breaches or attacks, the typical (median) number they recall facing has gone up, from 2 attacks in 2017 to 6 in 2019. One plausible explanation for fewer businesses identifying breaches is if they are generally becoming more cyber secure. The survey shows that businesses have increased their planning and defences against cyber-attacks since 2018. Another possibility is a change in attacker behaviour, with more attacks being focused on a narrower (though still numerous) range of businesses. Although the survey does not directly measure attacker behaviour, this may help to explain the observed fall in the number of businesses identifying breaches, alongside the rise in the typical number of breaches among those that do identify them.

3.5.2.3 Cost of data breaches

Among the 32 per cent of businesses recording breaches or attacks [2] , this resulted in a negative outcome, such as a loss of data or assets, in 30 per cent of cases. Among the charities recording breaches or attacks, this happened 21 per cent of the time. In businesses that had these kinds of negative outcomes, the average (mean) cost to the business was £4,180 in 2019. This is higher than in 2018 (£3,160) and 2017 (£2,450). It indicates a broad trend of rising costs in cases where cyber-attacks are able to penetrate an organisation's defences. Once again, the average costs faced by larger businesses in these cases tend to be much higher (£9,270 for medium firms and £22,700 for large firms in 2019). And for charities facing such negative outcomes from breaches, the average cost was £9,470 in 2019.

3.5.2.4 Prevention strategies

Around three-quarters of businesses (78%) and charities (75%) say that cyber security is a high priority for their organisation's senior management [2]. These proportions are higher than in 2018 (when it was 74% of businesses and 53% of charities). For businesses, there is a longer-term upwards trend going back to 2016 (when it was 69%).

Alongside this change in attitudes since 2018, there have also been various shifts in behaviour and action taken in this latest survey[2]:

- More businesses (57%, vs. 51% in 2018) and charities (43%, vs. 27% in 2018) update their senior management on actions taken around cyber security at least once a quarter.
- Written cyber security policies are more common both among businesses (33%, vs. 27% in 2018) and charities (36%, vs. 21% in 2018).
- Both businesses (27%, vs. 20% in 2018) and charities (29%, vs. 15% in 2018) are more likely to have had staff attend any kind of cyber security training in the last 12 months.
- Over half of all businesses (56%, vs. 51% in 2018) and two-fifths of charities (41%, vs. 29% in 2018) say they have implemented controls in all the five technical areas listed under the Government's Cyber Essentials scheme.

- More charities have taken actions to identify cyber risks, such as health checks, audits or risk assessments (60%, vs. 46% in 2018), bringing them in line with businesses (62%).
- More medium businesses (31%, vs. 19% in 2018) and large businesses (35%, vs. 24% in 2018) have cyber insurance, though the proportion of all businesses (11%) and charities (6%) that have this remains relatively low.

Three in ten businesses (30%) and over a third of charities (36%) say they have made changes to their cyber security policies or processes as a result of GDPR. Just over a third of businesses (35%) and three in ten charities (30%) have a board member or trustee with specific responsibility for cyber security. For businesses, this is higher than in 2018 (when it was 30%), but the proportion remains low overall. Moreover, the qualitative findings suggest that embedding knowledge and understanding of cyber security within management boards is a strong driver of behaviour change [2].

- Around one in five businesses (18%) and one in seven charities (14%) require their suppliers to adhere to any cyber security standards. In the qualitative interviews, some had simply not considered suppliers as a potential source of cyber risk before, while some others simply did not consider their suppliers' cyber security to be their responsibility.
- Very few organisations (16% of businesses and 11% of charities) have formal cyber security incident management processes in place. For businesses, this is somewhat higher than in 2018 (when it was 13%), although again the proportion is still low overall. This continues to be the area in the Government's 10 Steps to Cyber Security guidance6 where organisations are least likely to have taken action [2].

3.5.2.5 Cyber security expenditure

Larger businesses tend to spend more, as illustrated in the next table. Spending for charities also follows a similar pattern, with high-income charities (with £500,000 or more) spending a median amount of £2,100, and the very largest charities (with £5 million or more) spending a median amount of £12,100. [2]

Average investment in cyber security in last financial year

	All businesses	Micro/ small businesses[19]	Medium businesses	Large businesses	All charities
Mean spend	£5,100	£3,490	£25,100	£277,000	£1,500
Median spend	£200	£200	£5,000	£42,600	£0
% spending £0	33%	33%	18%	16%	59%
Base	1,272	933	204	135	424

Figure 11: Average investment in cyber security in UK in the last financial year[2]

Spending across businesses tends to be higher in sectors that consider cyber security as more of a priority, notably among finance or insurance, health, social work and social care, and information or communications firms – this is consistent with previous years.

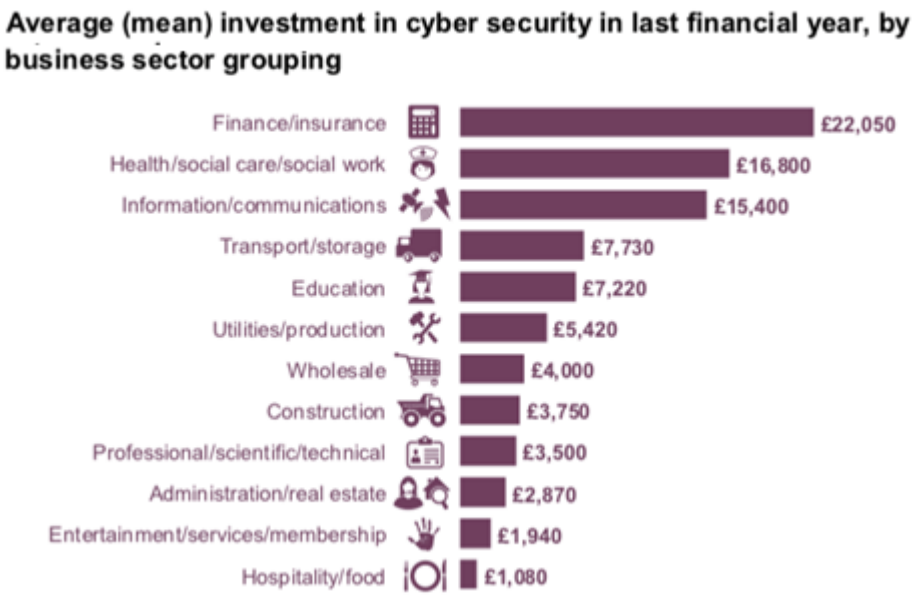

Figure 12: Average investment in cybersecurity by business sector group [2]

Among the organisations that do invest in cyber security, the main (unprompted) reason they give for doing so is to protect customer or donor data. The next most common concern is around protecting trade secrets, intellectual property or cash, followed by other reasons such as business continuity, fraud prevention and compliance outsourcing of cyber security

Around half of all businesses (49%) and three in ten charities (32%) have an external cyber security provider. There is an indication that this has risen among charities since 2018, although the change is not statistically significant.

As Figure 4.3 shows, outsourcing is more common among small and medium businesses than others – a similar pattern to previous years – and among firms in the finance or insurance, and health, social care or social work sectors. The pattern is different for charities, where outsourcing is more typical among high-income charities with incomes of £500,000 or more (72%). [2]

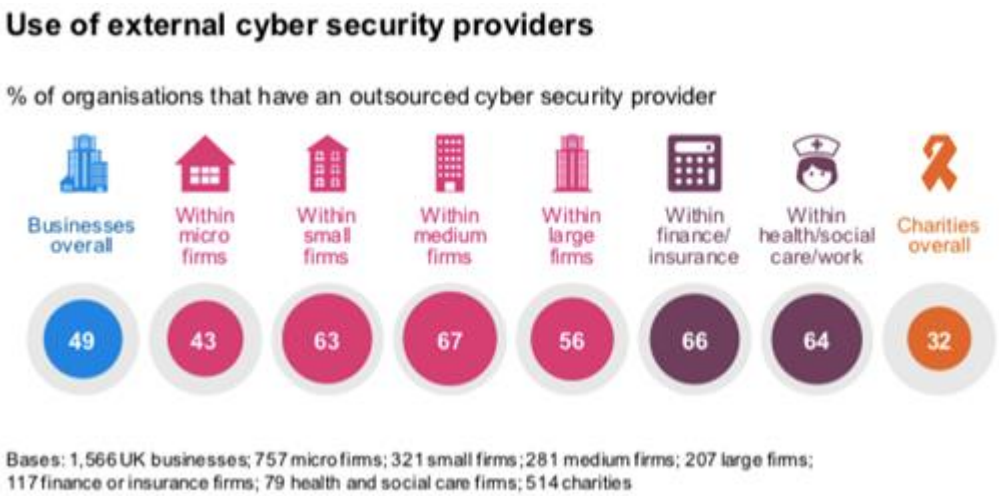

Figure 13: Use of external cyber security providers [2]

Figure 13: Rules and control measures implemented [2]

3.5.2.6 UK Businesses hit by cyberattacks every 50 seconds

According to internet services provider Beaming (www.beaming.co.uk), in the second quarter of 2019, businesses in the UK have faced an average of 146,491 attempted cyberattacks [4]. This current rate of cyberattacks equates to one attack every 50 seconds. The figure is a significant increase of 179% from 2018, in which businesses had faced 52,596 attacks on average.

Sonia Blizzard, managing director of Beaming commented: "The rate at which UK businesses are attacked online has soared over the last year and companies large and small are under sustained attack from hackers around the world."

It was identified that IoT devices and file sharing services were targeted the most by cyber-criminals, attracting 17,737 and 10,192 attacks respectively in Q2 2019. Within the first quarter both remotely controlled IoT applications and file sharing services attracted 201 and 114 attacks per day within Q1 2019. Beaming identified 371,000 unique IP addresses which had been utilised to launch cyberattacks on UK businesses in Q2 2019 – to which 52,860 were traced to locations in China as well as activity originating in Brazil, Taiwan, Egypt and the US.

3.5.3 Greek market and cybersecurity

Based on the relevant ministerial decision, the National Cyber Security Strategy 2020-2025 (approved on 07/12/2020) in accordance with the provisions of article 6 of law 4577/2018 (A' 199) (3rd revision).
Regarding the 1st revision, in 2018, the first draft of the national cyber security strategy entered into force, where the following were identified as general principles:

- The development and consolidation of a secure and resilient cyberspace.

- The continuous improvement of protection capabilities against cyber-attacks with emphasis on critical infrastructure and ensuring business continuity.
- The institutional shielding of the national cyber security framework, in order to effectively deal with cyber-attacks and minimize the impact of cyber threats.
- The development of a strong culture of citizens' security, of the public and private sector, utilizing the relevant possibilities of the academic community and in general of the public and private sector bodies.

It is also important to mention that the strategic planning was also revised and now extends to six (6) dimensions: Emergency Planning, Incident Reporting, Security and Privacy Protection, Research and Development, Partnerships Public - Private Sector (PPP), Investments in security measures.

3.5.3.1 The central guidelines

This framework defines the basic principles governing the protection of the Bodies, which are the pillars on which the Strategy is based:

- The actions specified in the Strategy and the Action Plan aim at the protection of the citizens and the structures of the Institutions, constituting the basis on which the digital governance and prosperity of the country are based.
- The cyber threats and the factors that may affect the operational continuity of the Public Administration and other involved Bodies are identified, recorded, categorized and treated with due diligence.
- The protection of human life and rights (such as the protection of personal data in particular) is of the utmost importance for the Strategy. The Authority and the Bodies shall take all possible measures to ensure the protection of citizens in accordance with applicable laws and regulations.
- The successful implementation of the Strategy requires a collective effort and partnership between the Bodies.
- The effectiveness of the Strategy in ensuring the continuity of the operational activities of the Bodies is based on the continuous information and education of all the Bodies involved and the citizens.
- The Strategy sets the framework for defining specific objectives, roles and responsibilities, as well as indicators that will assist in its ongoing evaluation and review.

Key elements of the vision are:

- *Building a modern digital environment*: A digital environment that allows the continuous inflow and development of new technologies and innovations in the digital age.
- *The high level of cyber security*: Across the range of information infrastructures, applications and services, adapted to the ever-changing challenges and requirements
- *The protection of fundamental rights*: personal data, the protection of privacy, the development of personality, equality and participation in the digital society
- *The development of a culture of safe use*: In the sense of digital education, continuous information and awareness of the risks and pitfalls of new technologies
- *Increasing confidence in digital governance*: As the key achievement of a secure digital environment, i.e. the use of new technologies across the spectrum of social and economic life for the benefit of citizens and businesses and socio-economic prosperity.

3.5.3.2 Strategic development objectives

Based on the results of the Strategic Priorities Analysis, we arrive at a total of five (5) strategic development objectives (SDO), which will cover fifteen (15) specific ENISA strategy development objectives for the EU Member States, as follows:

1. An operating system of governance
2. Critical infrastructure shielding, security and new technologies
3. Optimizing incident management, combating cybercrime and protecting privacy
4. A modern investment environment with an emphasis on promoting Research and Development
5. Capacity building, promoting information and awareness

The specific objectives aim at specializing and better managing the strategic framework (cascade effect) and in turn specialize in activities that cover the full range of recognition, prevention and protection, deterrence and recovery from cyber-attacks.

1. SDO 1: An operating system of governance
   - Optimization of the organization and operation framework structures and processes
   - Effective planning of risk assessment and emergency management
   - Strengthening collaborations in national, European and international level
2. SDO 2: Critical infrastructure shielding, security and new technologies
   - Understanding technological developments and how they affect digital governance
   - Upgrading the protection of critical infrastructure
   - Shielding systems and applications through enhanced security requirements
3. SDO 3: Optimizing incident management, combating cybercrime and protecting privacy
   - Optimization of methods, techniques and tools for analysis, response and notification of events
   - Strengthening deterrence mechanisms and optimizing business cooperation
   - Promoting data security in conjunction with privacy protection
4. SDO 4: A modern investment environment with an emphasis on promoting Research and Development
   - Promotion of Research and Development
   - Providing incentives in the private sector to invest in security measures
   - Utilization of Public-Private Partnerships (PPPs)
5. SDO 5: Capacity building, promoting information and awareness
   - Improving skills through the organization of appropriate exercises
   - Utilization of modern methods and tools of training and education
   - Constant information of Institutions and citizens regarding cyber security issues

3.5.3.3 Stakeholder mapping

- General Directorate of Cyber Security - National Authority
- Cybersecurity Authority
- National Cyber Assault Authority - National CERT
- Directorate of Cyber Defence (Ministry of National defence)
- Cyber Crime
- Personal Data Protection Authority
- National Telecommunications and Post Commission
- Communications Confidentiality Authority
- Centre for Security Studies

3.5.3.4 Need for cybersecurity

So far, the critical sectors were those of Telecommunications, Justice and Education. However, Law 4577/2018 extends this list to also include the sectors of Energy, Transport, Banking, Stock market, health, water and digital infrastructure (IXP, DNS, TLD), therefore considerably increasing the need for cybersecurity services. Furthermore, the COVID-19 pandemic created an increased need for remote working, not only for the system administrators, but also for the vast majority of the employees. Several technological solutions were extensively employed, one of which being the Virtual Private Network (VPN). This allowed employees to securely connect to their organization's internal network and carry out their work. However, despite the fact that the connection to their organization's systems was secure, several of them were using their personal computers at home, the configuration of which significantly diverged from the organization's security policy (antivirus protection, system updates, access control to files, etc.). Hence, their personal computers were potential "Trojan horses" through which malware or unauthorized users could obtain access to resources within the internal network. What is more, there were cases where, once remote users securely connected to the internal systems, they could access more resources than they should have been able to, due to inadequate or flawed access control.

Companies that managed to face this problem almost effortlessly were the ones that already had a significant portion of their employees working remotely (either partially or fully) during their normal operation. The said employees were therefore already in possession of appropriate equipment bearing the necessary security configurations and were able to carry out their daily work in almost the same way they were used to. For an organization to reach this state of secure remote working starting from zero requires significant financial resources, which most of the Greek Public Sector could not afford at that time. A large amount of money had to be spent to initially upgrade the existing infrastructure so as to be able to support that many remote users, as well as for e.g., teleconferencing equipment and services.

It is therefore clear that a need has emerged for cybersecurity services in the Greek Public Sector, which is a great opportunity for the CS-AWARE platform to grab this market segment, using the Larissa pilot installation as a reference site, so as to convince about its applicability and effectiveness. On the other hand, the majority of the Greek SMEs have been severely affected by the COVID-19 pandemic and it is currently unclear whether they could be potential customers in the near future.

3.6 Individual Driven Commercialisation – Partner level

This section presents the individual commercialization interests of partners willing to pursue after the end of the project independently or together with the new spin-out.

3.6.1 Peracton Ltd focusing on- Financial/Banking market

In line with its main market expertise for financial markets, Peracton plans to approach the financial /banking market (focusing on UK in particular) as there is an obvious potential, only if we consider that (according to a Critical Chains EU H2020 workshop presentation, December 2020) cyber criminals are netting billions from digital currency exchanges (e.g. $4.3 billion in 2019) while banking malware attacks are on a continuous ascending trend.

While the finance industry has historically had more robust cyber defences compared to other industries, the many third parties involved in its massive supply chain – including legal organizations, accounting and human resources firms, management consulting and outsourcing firms, and information technology and software providers – all pose potential weak spots. This begs several

important questions: How is the finance industry responding to the growing challenges associated with third-party cyber risk?

In order to assess how financial institutions are responding to growing third-party cyber risk, the Center for Financial Professionals (CeFPro) and BitSight launched a joint study: *"The State of Third-Party Cyber Risk Management (TPRM) in Financial Services, 2019."* The survey polled 126 financial services professionals from various industry sectors, including banking (49 percent), insurance (16 percent) and professional services (13 percent), among others. Respondents are located around the world, with the majority coming from the United States (35 percent), Europe (28 percent, not including the UK), and the United Kingdom (16 percent). The majority of respondents were at the manager level (36 percent) and the SVP/VP/Director level (30 percent), as well as the analyst (about 15 percent), C-level (about 10 percent) and board member (about 3 percent) levels.

What the data also makes clear, however, is that while many companies consider TPRM a key business issue that guides decision-making about which companies they do business with, many still struggle to measure and regularly report on this risk. Meanwhile, many organizations are not utilizing key tools like security ratings, leaving them unable to effectively and continuously monitor third-party risk. Nearly 80% of financial services firms say they would decline, or already have declined, a business relationship due to a third party's cybersecurity performance.

Nearly 97 percent of respondents said that cyber risk affecting third-party vendors is a 'critical' (57 percent) or 'Important' (40 percent) issue. The C-suite is particularly aware of this issue and is taking responsibility for it in new ways. Respondents reported that CISOs, CIOs, Chief Risk Officers, Chief Compliance Officers and CEOs are primarily accountable for third-party risk within their organizations, and 1 in 10 organizations have a dedicated role for managing vendor, third-party or supplier risk.

Organizations that have made third-party risk a C-level concern have firmly established cybersecurity posture as an important part of vendor selection. 41 percent of respondents said they would decline a business relationship, or terminate an existing relationship, due to a vendor's cybersecurity performance, while 37 percent say they have already done so. For this reason, demonstrating strong cybersecurity posture is now a clear imperative for organizations seeking to do business in the financial sector, as cybersecurity performance can be a business differentiator.

82 percent of those surveyed said that they believe executives and boards are confident in their approach to measuring and managing third-party risk, yet only around 44 percent are reporting on this risk to their executives and boards on a regular basis. Clearly, financial services firms are still challenged to communicate and measure the effectiveness of their third- party risk management strategies to board members and to leadership. Organizations need to be thinking about what security metrics are most important, how to track them, and how to leverage them more effectively in executive communications. Beyond that, they need to consistently communicate how they are improving security and managing risk among third parties and other vendors.

CeFPro and BitSight's survey also asked respondents to share the key third-party risk management challenges faced by their organizations. Many respondents reported concerns about the data gained from these risk assessments: its accuracy and quality, the actionability of the data, its timeliness, and the cost of data collection tools. Others cited the speed of the risk assessment process itself as a key challenge, as well as unclear responsibility within their organizations. Meanwhile, the majority of respondents think that their firms' technology budget (55 percent) and services budget (57 percent) for third-party risk management will only increase slightly over the next three years.

Despite these concerns and challenges, many organizations fail to utilize some of the most effective tools to assess the security of their vendors. Respondents reported that they still rely on tools like annual on-site assessments, questionnaires and facility tours to assess third-party security posture, giving them limited visibility into their third-party cyber risk. Meanwhile, only 22 percent of organizations are currently using a security ratings service to continuously monitor the cybersecurity performance of third-parties, though nearly 30 percent are currently evaluating a security ratings solution.

Therefore, Peracton will build upon the original work done within the CS-AWARE and will offer for the banking / financial market the CS-AWARE platform with the following features and goals:

- Versatile connectivity, Anomaly/Threat detection capability, Information correlation capability, Healing advisory ability, Self-Healing, Self-Healing, Knowledge Management, Compliance and Monitoring, STIX2.0 compatibility.
- Targeted markets: EU space and UK
- Potential clients: belong to the big financial banking space
- Competitors and pricing: as we identified ourselves in the same provider niche as SIEM providers (Security Information and Event Management) solutions, the competitors are more or less the same as we identified for the LPAs markets given they sell also to multiple markets. There is a comprehensive list detailed in D6.6 confidential Annex 1.
- IPR status: the intellectual property rights status for this commercialization doesn't differ almost at all from the LPA commercialization one, where partners can team up, and use the project developed technologies for market opportunities. The only difference is that the CS-AWARE components in this scenario will be licensed by the partners to be used for a banking/financial market space

3.6.2 3rdPlace focusing on e-Commerce market

The enforcement of social distancing, lockdowns and other measures in response to the COVID-19 pandemic has led consumers to ramp up online shopping. This has resulted in spikes in business-to-consumers (B2C) sales and an increase in business-to-business (B2B) e-commerce. In fact, while an eMarketer survey - released in July 2020 - predicts that retail sales will decline 10.5% this year - including a 14% decrease in brick-and-mortar - eCommerce, on the flip side, is expected to see 18% growth in 2020, largely driven by BOPUS initiatives (Buy Online and Pick Up in-Store) that have seen unexpected growth due to the pandemic. Between February and March 2020, the online sales in Italy grew significantly compared to the same period in 2019. Particularly, during the weekend, the e-commerce sector was largely impacted by the outbreak of coronavirus (COVID-19). On March 8, online sales registered an increase by 90 percent compared to the same period of the previous year and from the beginning of 2020 to date, the Italian market has seen 2 million of new online buyers, ramping up during the Covid-19 emergency. Many physical stores, especially those focused on food and basic necessities, have engaged with eCommerce for the first time. The most immediate solution has been the use of third parties already online. Many restaurants have put their menu of ready-to-eat dishes online through food delivery platforms and many supermarkets have activated eCommerce solutions through alliances with platforms that have already enabled (from a technological and operational point of view) online shopping under the aegis of certain major retail chains. Even more widespread are the numerous neighbourhood stores that have started working with less advanced digital tools than eCommerce, but with are just as interesting tools, such as the many neighbourhood stores (grocery stores, pharmacies, …..) that can take orders via WhatsApp or by phone.

During the health emergency Italian consumers have understood the value of this channel as never before: eCommerce has allowed a large slice of the population to benefit from value-added services,

important and essential as they are, like food delivery. Growth of web shoppers (who at the end of 2019 amounted to just over a third of the Italian population) and greater familiarity with and confidence in online transactions and digital payments (including those shoppers already used to purchasing online) can generate a positive effect on the development of eCommerce.

Unfortunately, the other side of the coin is that the Covid-19 lockdown has been (and still is) also a good time for cybercriminals. Many people are relying more heavily than before on online services for work, entertainment and shopping. This makes them more likely to become the targets of different types of online crimes. And the websites and online platforms, that these internet users' access, become more attractive targets to motivated hackers who aim to take them over. For example, "Magecart" is a software used by a range of hacking groups for injecting malicious code into eCommerce sites to steal payment details. Magecart attacks on online retailers and banks have increased by 20% during the pandemic. In March 2020 alone, many established brands like Nutribullet, True Fire and Tupperware all hit with these types of attacks; 19 SMB websites were attacked during this period. No business is too small.

Only last year, in July 2019, a study [14] found that the number of malware-affected Magento stores doubled monthly for three consecutive months. Besides that, a study by Cynet has found a correlation between rising cases of COVID-19 in Italy and increasing cyber-attacks on remote workers. The findings reveal that companies with higher instances of the virus and that have quarantined or instructed employees to work from home, are now experiencing a sharp rise in both phishing attacks that target remote user credentials and include weaponised email attacks. This shows the propensity for hackers to shift their focus to remote work environments in order to capitalise on the virus while thwarting corporate security measures. While this data reflects the current cyberthreat landscape in Italy, it also illustrates the future cyber implications for any territory in which the Coronavirus would spread to the level that justifies a similar quarantine policy.

From this point of view, Assolombarda, which is the largest territorial association of the entire entrepreneurial system in Italy, is hosting a webinar called "Cyber Security & ECommerce" in July 2020 and 3rdPlace will join the event as one of the main speakers. Approximately 6.300 firms located in the Provinces of Milan, Lodi, Monza and Brianza, Pavia are associated to Assolombarda, whose principal focus, as an entrepreneurial Association, is encouraging the development of the local industry by promoting solidarity and cooperation among its member firms and by fostering and protecting their interests when they have to face problems related to industrial, social, economic or cultural matters. Since cybersecurity represents a crucial aspect that can impact the online retailer's reputation, Assolombarda's webinar represents not only an opportunity to understand the best practices to optimize customers experience when they approach digital stores but also to raise awareness about the protection of their data.

3rdPlace's mission was always aimed to provide eCommerce organizations with AI-based proprietary solutions in order to build data-driven customer journeys that are more relevant and increase conversion and loyalty. So, the idea is to empower 3rdPlace's proposition for retailers and eCommerce combining its more consolidated activities related to user/customer intelligence with a new cyber security offering, based on CS-Aware platform/technology. This combination of solutions will not only optimize the user experience through customized recommendations, touchpoints, etc, but also guarantee the security of users' sensitive data:

- raising awareness on possible cyber threats
- activating self-healing strategies
- sharing knowledge and best practices among retailers

In particular:

- Offered solution: CS-AWARE platform (as designed during the project) will be offered with the same unique selling points as for LPAs but it will be included in a broader sales narrative for eCommerce players that can be summarized in: "customized experiences + data security = higher customers loyalty"
- Targeted markets: EU space and UK
- Potential clients: Retail, eCommerce, Travel & Leisure
- competitors and pricing: as far as cybersecurity is concerned the competitors are more or less the same as we identified for the LPAs markets given, they sell also to multiple markets. There is a comprehensive list detailed in D6.6, V3, section 4.3. But, at the same time, we believe that the uniqueness of our proposition is based on a data-driven approach that can serve two different goals at the same time: 1) user experience 2) data security
- IPR status: the intellectual property rights status for this commercialization doesn't differ almost at all from the LPA commercialization one, where partners can team up, and use the project developed technologies for market opportunities. The only difference is that the CS-AWARE components in this scenario will be licensed by the partners to be used for a Retail/eCommerce market space

3.6.3 Cesviter focusing on consultancy services for cybersecurity risks and readiness in LPA sector

Cesviter will continue the activities pursued during the life-time of the project and will support both the spin-out and independent initiative with the followings:

- **Solutions being offered** - In this initial phase, Cesviter will focus on developing consultancy services for small and medium-sized municipalities concerning cybersecurity. Before proceeding to the application of the CS-AWARE platform Cesviter will be encouraging municipalities to analyse what services and activities they offer to their communities and how well they are fulfilling this basic mission of the provision of social services to their citizens and businesses.
- **Potential clients** - Cesviter will focus on small and medium-sized municipalities plus municipal utility companies (water, electricity, gas, etc.).
- **Competitors** - As described earlier for the CS-AWARE platform in general, there are even fewer, if any, competitors when dealing with small and medium-sized municipalities. Other businesses tend to concentrate on a combination of hardware and software to sell their solutions to municipalities. Many municipalities are concerned about the fact that they really have no idea of what they have, what should be protected, and the issues to resolve. As one municipal official put it "I would like to understand better where we are now before buying anything else."
- **Pricing**: In the initial phase where the focus will be helping municipalities understand better where they are, what their environment is, and where they would like to going through 2+ days of consulting activities as outlined in WP2. In late 2021 as the current crisis begins to resolve itself (at least, following the "medium-risk scenario") and work has been done on bringing the CS-AWARE platform up to a market-readiness of T9 it should be possible to proceed further.
- **IPR status:** As noted above, the partners can team up and use the project developed technologies for market opportunities. The only difference is that the CS-AWARE components in this scenario will be licensed by the partners to be used in the public sector.

4 Intellectual Property Rights management

The intellectual property of the developed CS-AWARE platform during September 2017 - August 2020 time period covers various artefacts and can be categorized as follows:

1. **Know-how** accumulated during the duration of the project (cybersecurity, IT, methodology modelling, etc) - all partners;
2. **Copyright** developed during the project lifetime:
    1. *Codebase* grouped in software components
    2. *Analysis methodology*
    3. *Project logo*
    4. *Project website*
    5. *Project internet domain*
    6. *Project Twitter account*
    7. *Project Facebook account*
    8. *Project YouTube account*
3. **Pre-existing intellectual property** brought to the project at the start: MAARS decision engine by Peracton that is incorporated into the Data Analysis component

For point 2a above, we list below the copyright owners of the code base grouped in dedicated software components:

Copyright Owner	CS-AWARE software components
3rdPlace	data collection client
3rdPlace	logs adaptors
3rdPlace	package collector
3rdPlace	social media (days)
Peracton	data analysis
Peracton	patterns (not component)
Peracton	STIX2jason/library
InnoSec	self-healing
InnoSec	cyber info exchange
Consortium	watcher
Consortium	translation (not component)
RheaSoft	visualisation
RheaSoft	node extension

Table 5 CS-AWARE platform copyright owners

5 Future work and next steps

As next steps, the information centralized during the 3 versions of this deliverable will be re-used (spin-out business plan, business pitches, investment discussions) and enhanced primarily by the spin-out but also used by the individual partners commercialization effort as a basis of their market analysis and discussions with prospects. In this respect, the future spin-out has a solid market analysis basis and positioning and will have to further do more market testing to identify the most important cyber security elements, consolidate the existing one and determine new ones that LPA prospects are interested about.

References

[1] 'Research and Markets, April 2020' [1] https://www.prnewswire.com/news-releases/worldwide-cyber-security-market-analysis-2020-featuring-impact-of-covid-19-on-the-market-301057900.html

[2] Report finds UK cyber security sector now worth £8.3bn: Jan 2020: http://www.publicsectorexecutive.com/Robot-News/report-finds-uk-cyber-security-sector-now-worth-83bn

[3] Hiscox CyberReadiness Report2019 https://www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF

[4] UK businesses hit by cyber-attacks every 50 seconds https://gdpr.report/news/2019/07/09/uk-businesses/

[5] SMES OVERVIEW http://doitbetter.info/smes-overview/

[6] Italy unemployment up to 12.4% end 2020 – OECD https://www.ansa.it/english/news/business/2020/07/07/italy-unemployment-up-to-12.4-end-2020-oecd_ea5a41ab-0287-4bfb-a68a-907d2e5a9fe2.html

[
7] Clusit: rischi cyber, situazione di inaudita gravità https://www.bitmat.it/blog/news/93768/clusit-rischi-cyber-situazione-di-inaudita-gravita

[8] Italy https://www.cia.gov/library/publications/the-world-factbook/geos/it.html

[9] Rapporto Clusit 2020 https://clusit.it/rapporto-clusit/

[10] ECFIN forecast summer 2020 Italy https://ec.europa.eu/economy_finance/forecasts/2020/summer/ecfin_forecast_summer_2020_it_en.pdf

[11] Doing Business in Italy:2016 Country Commercial Guide https://it.usembassy.gov/wp-content/uploads/sites/67/2016/10/Italy-2016-CCG.pdf

[12] OECD: funding sub-national governments according to needs and capacity - Italy https://read.oecd-ilibrary.org/economics/oecd-economic-surveys-italy-2019_369ec0f2-en#page152

[13] Cybersecurity and Economic Incentives https://read.oecd-ilibrary.org/science-and-technology/computer-viruses-and-other-malicious-software/cybersecurity-and-economic-incentives_9789264056510-6-en#page7

[14] Securing your ecommerce store during COVID-19 https://multichannelmerchant.com/blog/securing-your-ecommerce-store-during-covid-19/