Project Title	Wide – Impact cyber Security Risk framework
Project Acronym	WISER
Grant Agreement No	653321
Instrument	Innovation Action
Thematic Priority	Cybersecurity, Privacy & Trust, Risk Management, Assurance Models
Start Date of Project	01.06.2015
Duration of Project	30 Months
Project Website	www.cyberwiser.eu

D7.2 - MARKET WATCH, SECOND VERSION

Work Package	WP7, Market Validation and Roll-out to Other Verticals
Lead Author (Org)	Timea Biro (TRUST-IT)
Contributing Author(s) (Org)	Niccolò Zazzeri (TRUST-IT), Stephanie Parker (TRUST-IT), Paolo Lombardi (TRUST-IT), Antonio Álvarez (ATOS), Jan Bastiaensens (Enervalis), Ales Cernivec (XLAB), Marta Stimec (XLAB)
Due Date	30.11.2016
Date	30.11.2016
Version	1.0

Dissemination Level

X	PU: Public
	PP: Restricted to other programme participants (including the Commission)
	RE: Restricted to a group specified by the consortium (including the Commission)
	CO: Confidential, only for members of the consortium (including the Commission)

Versioning and contribution history

Version	Date	Authors	Notes
0.1	28.10.2016	Timea Biro, Niccolò Zazzeri, Stephanie Parker, Paolo Lombardi (TRUST-IT)	TOC, first draft
0.2	04.11.2016	Antonio Álvarez (ATOS)	Contributions on layout and edition guidelines. Input to sections 2, 2.1, 2.2 and 5.3
0.3	07.11.2016	Antonio Álvarez (ATOS)	Contribution to section 5.3
0.4	07.11.2016	Antonio Álvarez (ATOS)	Contribution to sections 4.2 and 4.3
0.5	07.11.2016	Timea Biro, Niccolò Zazzeri, Stephanie Parker, Paolo Lombardi (TRUST-IT)	Complete version for First Internal Review
0.6	09.11.2016	Jan Bastiaensens (Enervalis), Ales Cernivec, Marta Stimec (XLAB)	Review remarks
0.7	16.11.2016	Timea Biro, Niccolò Zazzeri, Stephanie Parker, Paolo Lombardi (TRUST-IT)	Addressing comments of the First Internal Review
0.8	21.11.2016	Antonio Álvarez (ATOS)	Refinement of section 6.1
0.9	25.11.2016	Timea Biro, Niccolò Zazzeri, Stephanie Parker, Paolo Lombardi (TRUST-IT)	Refinement of sections 2, 3 and 4.
0.10	28.11.2016	Timea Biro, Niccolò Zazzeri, Stephanie Parker, Paolo Lombardi (TRUST-IT)	Version ready for General Assembly approval
1.0	30.11.2016	Antonio Álvarez (ATOS)	Submission to EC

Disclaimer

This document contains information which is proprietary to the WISER consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or parts, except with the prior written consent of the WISER consortium.

Table of Contents

List of Tables

List of Figures

Executive Summary

The second in a series of three such documents, the main goal of the Market Watch report is to consolidate the analysis of the WISER market and value chain positioning detailed in the first version of the report (Deliv 7.1) delivered in month 9 of the project.

More specifically the document further reports on market conditions, updating the analysis of both the demand and supply side, as well as the WISER market positioning, highlighting key market developments and related initiatives also on cyber insurance.

Key findings are:

- The market is a fast evolving one with an ever-growing opportunity to be seized.
- Within the prospective cyber security market, risk management in real time can be the differentiating asset.
- On the demand side a considerable opportunity is emerging as demand is forecast forecasted to grow exponentially in coming years.
- On the supply side, a few large players are already present with commercial approaches. However still a lot of what is currently offered is consultancy-based which entail entails high costs.
- Notably some online tools are emerging, but overall there are still plenty of opportunities to be seized.
- Governments are currently playing a decisive role in stimulating the economy through policies entailing a mix of incentives, regulation, and awareness raising actions. Regions with well-established cybersecurity-related legislation have a higher cyber insurance adoption than regions with no such legislation.
- There is a need to move away from the current mind-set where cyber security is associated with costs, to one that acknowledges that a proper cyber security risk management enables cost savings while realising the full potential of digitalisation within the scope of the Digital Single Market.

Overall, it can thus be said that the main elements of WISER innovation are still very relevant vis-à-vis the current market conditions. Likewise it is important to bear in mind that in such a fast-paced environment timing becomes absolutely crucial in order to effectively reap the benefits of an innovative solution.

1 Introduction

1.1 The WISER initiative

Most organisations today are fundamentally digital, and information and communication technology (ICT) have become the backbone of operations, products and services. The multi-faceted nature of cyberspace means that dealing with cyber risks at all levels of an organisation's structure requires a multi-staged methodology to continuously, consistently and appropriately govern an organisation's cyber strategy.

WISER is a collaborative Innovation Action in the field of cybersecurity that puts democratisation of cyber-risk management at the heart of good business practice for all ICT-intensive organisations, and SMEs especially.

> "Increasing overall cybersecurity awareness in Europe and ensuring that all affected users have access to efficient, flexible and cost effective cybersecurity set of products and services."

WISER mission statement

1.2 Goals

WISER sets out to achieve six major goals:

#1: Develop a best practice approach and methodology that can be universally applied to the assessment of cyber risks based on modelling expertise of partners.
#2: Establish a dynamic cyber risk framework that evolves to reflect changes in the cyber risk landscape.
#3: Develop analytical tools to estimate risk exposure, empower situational awareness and facilitate decision support.
#4: Integrate technological advances related to the implementation of the assessment, monitoring, and mitigation IT platform for cyber risk management in real-time.
#5: Conduct feasibility experiments in various industries to demonstrate viability and scalability.
#6: Develop a sustainable business model supported by a continuous awareness-creation action that maximises impact.

1.3 Scope of the Innovation Action

WISER recognises that real-time information is the key for decision makers to manage risks. WISER therefore delivers real-time monitoring and intuitive assessment tools which go beyond the state of the art, to enable agile and near real time management of cyber security risks as a significant step forward beyond current practices in risk management

WISER provides risk managers with the means to understand both economic and sociological impacts of cyber-crime so that both direct and indirect implications are clear. To assess risk, you have to know what you are looking for and quantify the consequences.

WISER goes beyond the current state of the art to offer a novel and agile cyber-risk management framework for modern ICT systems. The integrated approach to control mitigating activities will address cyber-security threats and their consequences in critical information infrastructure and empower decision makers in public and private organisations to assess cyber-risk effectively.

The Innovation Action delivered by WISER is dual. On the one hand, it aims to bring to the attention of the wider audience the various aspects entailed by cyber security. On the other hand, it aims to present to SMEs and other organisations, private as well as public, a set of services that demonstrate how risk management methodologies and solutions can effectively represent practical solutions to improve cyber security in various industries.

WISER provides a cyber risk management framework able to assess, monitor and suggest mitigation measures in real time. The WISER risk assessment approach focuses not only at the level of a given ICT system, but also considering the business processes or services that depend on it. It also considers the societal impact of risk and helps to determine the most appropriate mitigation action(s). WISER intends to address cybersecurity needs of different users as different systems varies in size and complexity. For this reason the Consortium identified a service delivery model based on three different modes of operation: CyberWISER Light, CyberWISER Essential, and CyberWISER Plus.

1.4 The CyberWISER Services

As presented in the deliverable 8.7 WISER Exploitation Plan and Business Models, the three separate "operation modes" are:

1.4.1 CyberWISER Light

CyberWISER Light is the non-intrusive mode of the WISER Framework (the client does not need to install any dedicated software on its infrastructure). It is the first outcome offered by WISER allowing users to obtain a first estimation of the situation of an IT infrastructure with respect to cyber risk. It provides a quick and simple assessment of cyber risk thanks to information regarding the company which is collected in a questionnaire. The user is also given the chance to easily detect vulnerabilities present at the client IT infrastructure and capable of escalating to intrusion into externally exposed resources.

The tool is not intrusive and provides immediate feedback. The output is a report easy to understand, highlighting the main points to be improved as far as the client´s cybersecurity is concerned.

This report gives a first picture of the overall risk exposure by means of a spider web, and a colour code indicating how exposed the company is in each of the chapters evaluated. Then a paragraph is provided with explanations about those chapters for which the exposure is meaningful.

The report goes further by analysing each chapter in detail. The user can make use of the tool autonomously without external assistance and with minimum time investment.

To use the tool, the user only needs to register on the CyberWISER portal (https://www.cyberwiser.eu/), a central unique point to access this service.

CyberWISER Light is an easy to use tool, provided at no cost offering also a straightforward access to WISER service portfolio, a first touchpoint with the customers. It helps the clients understand their business' cyber risk exposure. It is a teaser of what the WISER Framework can provide.

1.4.2 CyberWISER Essential

CyberWISER Essential incorporates a decisive feature brought by WISER: the real-time monitoring and assessment of cyber risk. To do this, sensors are deployed on the target infrastructure, unlike the previous mode, which was non-intrusive. In this operation mode, the sensor scope is limited to the network layer. It enhances the vulnerability scan feature to provide a more complete testing module. CyberWISER Essential combines the information obtained by the monitoring and the testing module with the client profile information collected in the configuration module, in order to provide an evaluation of the risk which is based on both the technical and the business aspect. The information collected for client profiling is much more complete and detailed. The evaluation of risk is performed in a more elaborated way, based on risk models and associated model rules which are executed to calculate the evaluation of cyber risk. The results are shown in a complete dashboard. Besides, mitigation measures are suggested to the user, depending on the result of the risk evaluation.

CyberWISER Essential will be offered as a service tool, accessed through the CyberWISER official site (www.cyberwiser.eu), via a dedicated URL.. There is a difference between the core components of WISER and the ones in charge of capturing the cyber-climate activity. The latter ones have to be installed in the client infrastructure to be monitored (this is mandatory), while the core components can be deployed inside or outside the client premises depending on client preferences and needs.

If the client goes for the first approach, everything is installed on the client premises and it can be said that WISER is an on-line application which is used basically on the client intranet (a user could anyway access from the outside by means of VPN, for instance). This is a pre-packaged risk management solution. This involves more effort and expertise from the client staff to deploy, set up and operate the framework in infrastructure. In return, the client keeps the whole control of the platform, and nothing is exposed in a public IP.

If the user goes for the second approach, it implies choosing the ‘as a Service’ model (Risk Management Platform as a Service, RPaaS). The sensors are likewise deployed on the client premises, while the core components are running in a machine provided by a third party (e.g. a cloud provider) accessible from anywhere. The third party offers not only the hosting, but also expertise on cyber risk management. This will be transparent to the client, who will be provided with a dashboard showing the evolution of a set of representative and easy to understand parameters about the cyber climate of the monitoring infrastructure.

It incorporates a **socio-economic tool**, which builds on current state of the art methodologies and tools, leveraging best practices from multiple industries.

The quantification of the social and economic impact allows transforming technical information (alerts about security) in key business information. This novel approach allows to a non-technical manager (CEOs, Financial managers, Operations managers…) to make decisions about the addressed resources to mitigate a potential attack.

This way, the final service provided to customers doesn’t cover only detection. It gives information that helps to assess the risk in terms of potential economic loss, in order to make decisions.

This mode of operation, unlike the previous one, considers the involvement of the WISER team, composed of consultants with high expertise on cyber security and specific knowledge about the WISER Framework. The conditions governing this involvement are specified in the contract between the provider and client parties, anyway they are limited in comparison with the advanced operation mode, addressed below.

1.4.3 CyberWISER Plus

CyberWISER Plus is the most complex and advanced mode of operation designed for the WISER Platform. WISER sensors catalogue is expanded with the inclusion of sensors able to collect information at the application layer level. This means that the quantity and variety of data available for processing and analysis is larger. CyberWISER Plus offers the possibility to put in place customized sensors tailored to the peculiarities of the target infrastructure and also integrates existing sensors provided for the customers. To do this, a further involvement of the WISER team is required.

CyberWISER Plus is not limited to suggesting mitigation measures, it also offers cost-benefit analysis features allowing the user to make informed decisions on the best mitigation measures to apply, by ranking and prioritizing them. Top management positions, with the authority to decide what to do with respect to cyber security, traditionally lack information to make such informed and critical decisions. Given the fact that cyber security requires an investment which in most cases is not negligible in the company’s overall budget, CEOs or similar positions will always demand this information in order to make these investments. If the information is not in place, the company will apply the typical security patches at most, but will not adopt measures with greater impact. In such sense, CyberWISER Plus makes a relevant contribution helping to steer the company cyber security policy following a strategy making sense, since it is based on a solid methodology and has a contained financial cost that pursues the policy of *"cyber-security for all"* approach.

The risk assessment performed in this operation mode is based on a larger and more detailed amount of information, not only from the technical side (information collected from the testing and monitoring modules), but also from the business configuration side, as the client introduces more detailed information through means of an answered questionnaire. The models used to perform the risk evaluation are more sophisticated and tailored to the client needs. The evaluation also considers intangible aspects such as the societal impact of the risk, applying a methodology aiming at making possible to measure such impact. Then, the risk is evaluated from more sides, and the resulting offered vision is more complete.

CyberWISER Plus is also offered as a service tool. The two approaches for deployment presented in the case of CyberWISER Essential are also applicable to CyberWISER Plus. As for the involvement of the WISER consortium, this way of marketing WISER foresees a full involvement of the complete consortium and their specific skill-set.

1.5 The WISER Value proposition

The table below offers a mapping of the WISER offer, including functionalities and features, related to its main target audiences. The WISER offering is related with the target audiences as the following figure summarises[1]:

(CyberWISER Light)				
First concrete WISER tool: includes user-friendly approach to increase awareness through self-assessment	▪ Password-protected area ▪ PDF report generated on the fly ▪ Vulnerability scanner	▪ Light Risk Assessment Engine	SMEs Public Administration with small IT teams	Online since March 2016
(CyberWISER Essential)				
RPaaS solution for real-time risk assesment	▪ Reporting portal ▪ Risk report including quantification of risk ▪ Mitigation recommendations (automated) ▪ Models (preconfigured, optional configurable) ▪ Societal impact evaluation (preconfigured) ▪ Optional asynchronous interaction with consultants	▪ Full Risk Assessment Engine ▪ Vulnerability Scanners ▪ Sensors network layer	SMEs and ICT systems in general	December 2016
(CyberWISER Plus)				
On-demand services for real time and cross-system assessment of vulnerabilities and	▪ Reporting portal ▪ Risk report including quantification of risk ▪ Full mitigation plan (by consultants,	▪ Full Risk Assessment Engine ▪ Vulnerability	Critical infrastructure or highly complex cyber systems	December 2016

[1] WISER D8.7 - exploitation plan & business models, 1st version

threats	not automatic) - More tailored models - Societal impact evaluation (customized) - Remote (included) and onsite (optional) consultancy - Possibility to integrate with risk systems already in place - Customizable sensors	Scanners - Network and application layer sensors		

Table 1 - WISER Offering related to target audiences

2 Demand side

The Internet, digital services and what we broadly call the cyberspace have gained an ever stronger and more meaningful impact on all parts of society and our daily lives.

We depend daily on seamlessly working information and communication technology, making it the backbone of our economic growth and a critical resource on which all economic sectors rely on as well as an indispensable element of modern public administration and all public services.

The dependency comes with a cost as all sectors as well as the citizens themselves become more and more exposed to numerous types of cyber risks that have a great impact not only on the online presence but also on what we can call the offline world.

On the other hand businesses, public authorities and citizens are also the ones that benefit from the potential of the digital economy, thus building their trust to stimulating their uptake of cyber security technologies and solutions is essential. [2]

We are witnessing a transformation in the mindset of organisations of all sizes as stated in the PWC The Global State of Information Security® Survey 2017[3]" Many organizations no longer view cybersecurity as a barrier to change or as an IT cost. They understand that cybersecurity solutions can also facilitate business growth, create market advantages and build brand trust(…)As a result, forward-thinking organizations are pivoting toward a new model of cybersecurity, one that is agile, capable of acting on analytic inputs and adaptive to evolving risks and threats. At the core of this new approach are solutions like data analytics and real-time monitoring, managed security services, advanced authentication and open-source software."

Nevertheless, this trend still needs to be translated into a critical organisational transformation for better cyber risk posture. At worldwide level, only the 32 % of the companies have formally defined an ICT security policy. It is even more surprising the fact that only the 72% of large companies have carried out this important task, when these kinds of companies are supposed to be able to afford the cost that involves putting in place such policies[4]. Figure 1 represents this.

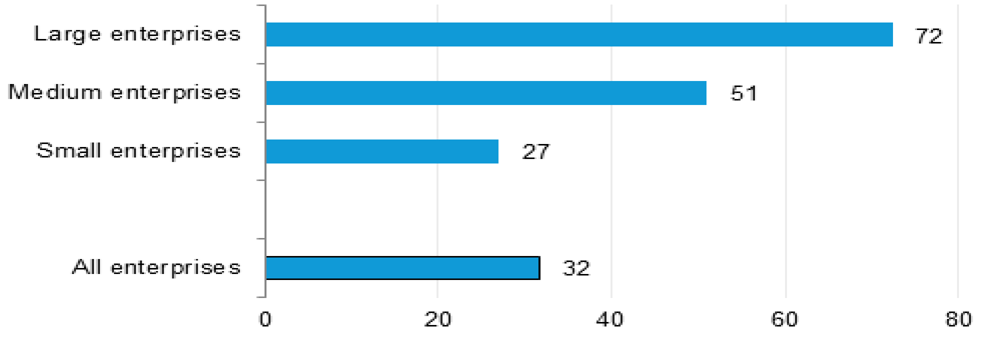


Figure 1. Percentage of companies having defined a formal ICT security policy. Global level

On top of that, the annual study on companies data breach preparedness carried out by the Ponemon Institute shows that a minimum percentage of the companies update on a periodical basis their data breach response plans[5]. This is reflected in Figure 2.

[2] Cybersecurity Industry Roadmap – European Commission Public Private Partnership on Cybersecurity http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_cnect_004_cybersecurity_en.pdf

[3] http://www.pwc.com/gx/en/information-security-survey/assets/gsiss-report-cybersecurity-privacy-safeguards.pdf

[4] http://ec.europa.eu/eurostat/statistics-explained/index.php/File:Enterprises_having_a_formally_defined_ICT_security_policy,_by_size_class,_EU-28,_2015_(%25_enterprises)_new.png

[5] http://www.experian.com/assets/data-breach/white-papers/2015-experian-data-breach-preparedness-study-final.pdf

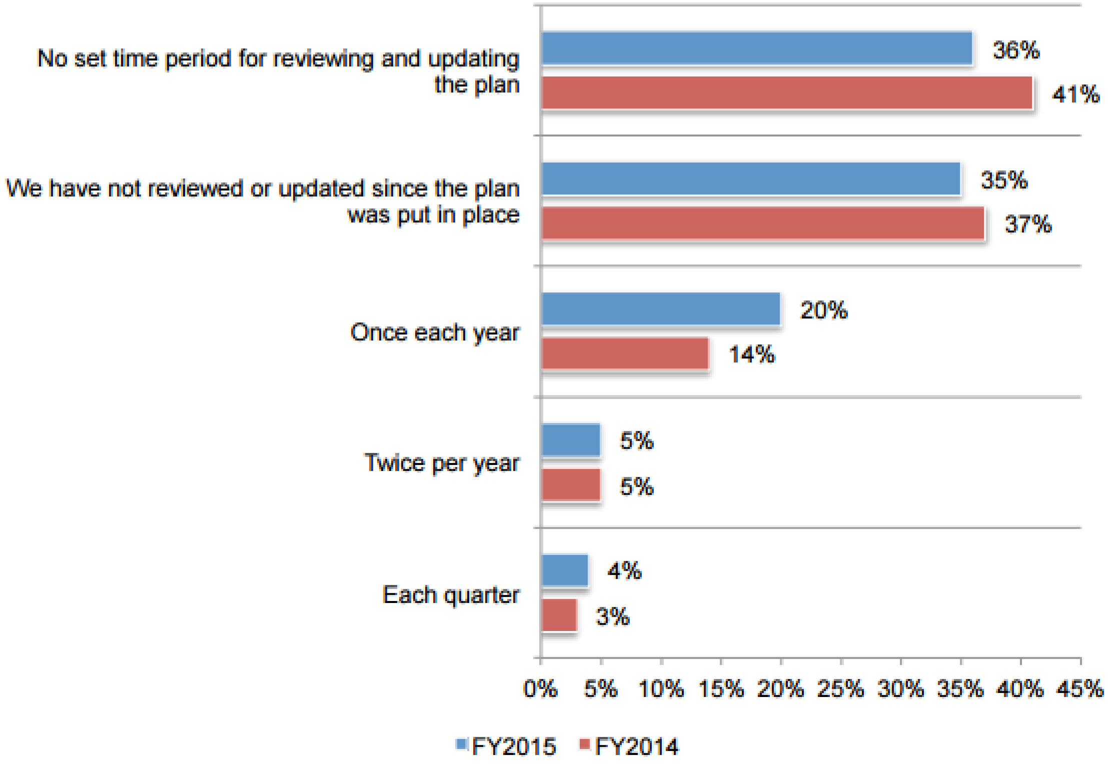
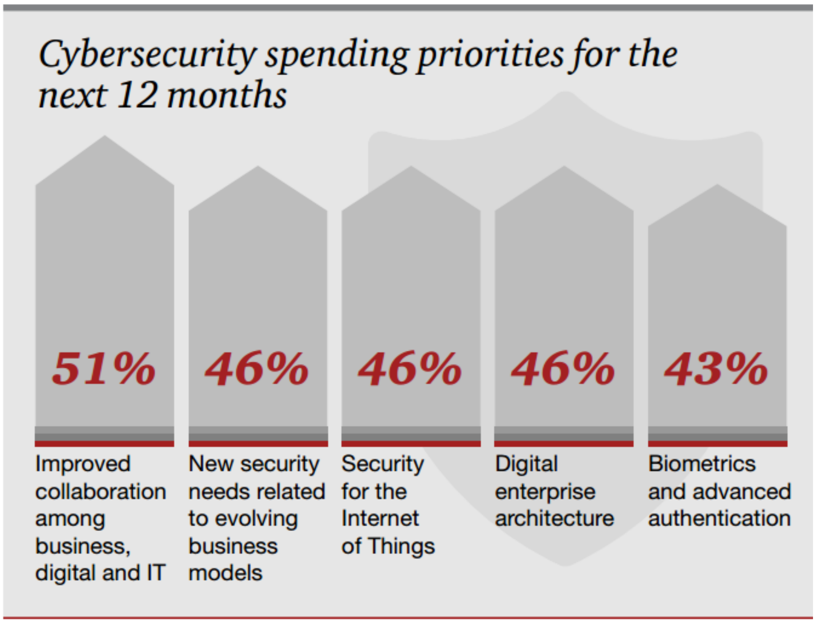


Figure 2. Companies habits with respect to how often they update their data breach response plans

Nevertheless the budget allocated to cybersecurity is growing and according to the PWC and their Global State of Information Security® Survey 2017, 5 new spending priorities emerge for the next 12 months:



Source: PwC, CIO and CSO, *The Global State of Information Security® Survey 2017*, October 5, 2016

Figure 3 -Cybersecurity spending priorities for the next 12 months

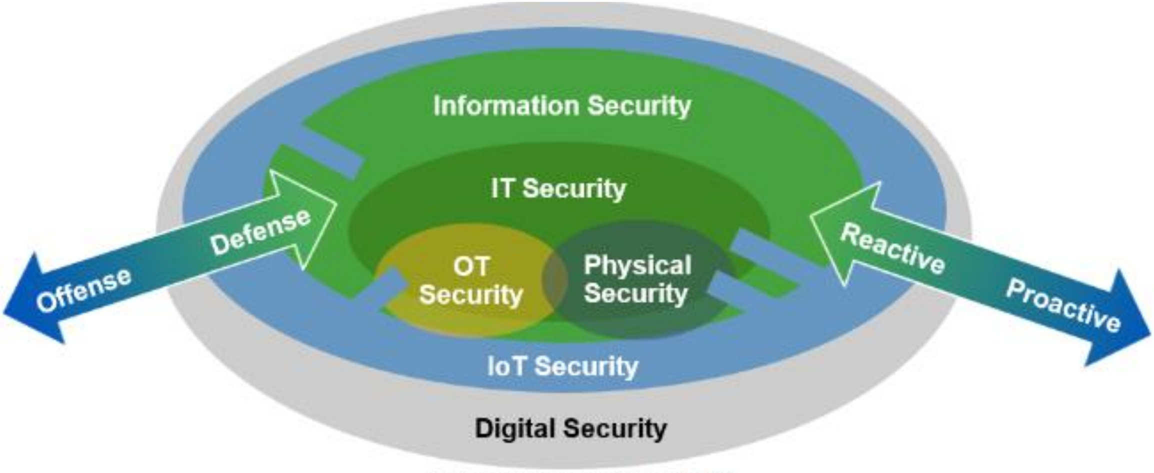
2.1 Stakeholders & target audiences

The demand for Cybersecurity amid the ever-increasing internal and external pressure has become a huge challenge for all organisations. Businesses, public entities and citizens are the first in line for the adoption of cyber security solutions that guarantee their fundamental rights as well as help them take advantage of the digital sphere potential.

Based on the nature of the organisations, it has become clear that the demand side audiences or ICT services and product buyers, have at least two key roles to play in cybersecurity:

- First reduce risk by consolidating the organisations' cybersecurity strategy
- Second, by factoring security into procurement decisions, buyers incentivize ICT suppliers to develop and provide more secure ICT.

In its Special Report: Cybersecurity at the Speed of Digital Business, released in August, 2016, Gartner discussed an extended concept of cybersecurity, as digital cybersecurity: "Cybersecurity is the foundation of digital business and innovation. It must address a new reality in which IT organizations have little direct infrastructure, and their biggest security concerns will come from services outside their control. The scope of cybersecurity is expanding and becoming digital security (see Figure below). As organizations transition to digital business, cybersecurity will need to address the lack of directly owned infrastructures and the prevalence of services outside IT's control. Safety becomes an issue with the intersection of technology and the physical world — IT/operational technology (OT)/Internet of Things (IoT).[6]



SOURCE: GARTNER (AUGUST 2016)

Figure 4 - The Scope of Cybersecurity Is Expanding to Become Digital Security

The report also forecasts that

- By 2020, 60% of digital businesses will suffer major service failures, due to the inability of IT security teams to manage digital risk.
- By 2020, 60% of enterprise information security budgets will be allocated for rapid detection and response approaches, which is an increase from less than 30% in 2016.

[6] https://www.gartner.com/doc/3426427?refval=&pcp=mpe#-1081400657

2.1.1 The small business and the cyber security landscape

Small- and medium sized enterprises (SMEs, or SMBs – small- and medium-sized businesses) are the cornerstone of the European economy. They represent 99% of all businesses in the EU. In the past five years, they have created around 85% of new jobs and provided two-thirds of the total private sector employment in the EU[7].

They have a key role for the Digital Single Market strategy fuelling a fast evolving economy. Small business are seen as facilitators as they enable all types of businesses to go digital and operate across borders more easily and cost effectively.

The table below shows the typical structure of SMEs in Europe.

Estimated number of SMEs in the European Union	23 million. 99 out of every 100 European businesses are SMBs. Clearly, this figure includes many different types of companies (e.g. local shops and crafts). As an example, the UK has an estimated 4.5 million SMEs and 2.4 million tech firms. However, with an increasing number expected to become digital businesses, many will need to ensure they are safe on line.[8]
Typical company size	Roughly 93% of SMEs are micro, that is they employ less than 10 people. 6% of the total number of European SMEs are Medium, employing between 11 and 49 people. 1% of the SMEs are medium employing between 50 and 249 people.[9]
Business priorities	Focusing on running their business and acquiring new customers rather than on investing in delivering new services. They also lack the financial and human resources of large companies.
Level of IT expertise	Fewer than 20% of SMEs in Europe have an IT manager.
Jobs & Growth	SMEs employ 2 in every 3 employees and on average produce 58 cents/euro.

Table 2. WISER Analysis of European Statistics on Small Firms

Lacking the security budgets of large enterprises, SMEs are perceived as ‘easy targets’, highlighting a growing demand from SMEs especially for ‘light-weight’ services. As reference, research provided by the UK Government Security Breaches Survey[10] found that nearly three-quarters, 74%, of small organisations reported a security breach in the last year.

Small businesses have frequently been drawn into the spotlight as subject to high potential losses due to cybersecurity risks. A quantification of the damages from security breaches suffered by SMEs in the UK indicates that the damage can be well above €100,000. Despite this, over 85% of SMEs *“do not have any plans to increase their budgets for security implementation, and less than 13% are working with a third party vendor to protect themselves”*[11]. Research from the UK Federation of Small

[7] https://ec.europa.eu/growth/smes_en

[8] http://ec.europa.eu/growth/smes/business-friendly-environment/performance-review/files/annual-report/infographics_en.pdf.

[9] http://ec.europa.eu/growth/smes/business-friendly-environment/performance-review/files/supporting-documents/2014/annual-report-smes-2014_en.pdf

[10] https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

[11] http://www.smallbusiness.co.uk/news/management/2488626/majority-of-small-businesses-unprepared-for-data-breaches.thtml

Businesses shows that SMEs were on average the victims of around 7 million cybercrimes a year in 2014 and 2015[12].

2.1.2 *Large companies as the drivers of cyber-risk management good business practice*

In today’s digital economy, businesses are increasingly connecting to customers, suppliers, and employees over the internet. While this has clear advantages for the businesses, it creates hundreds of potential entrances to the company's data: Google and McAfee estimate that there are 2,000[13] cyber-attacks around the world every day, costing the global economy about €420 billion a year. Lloyd´s has also made an estimation of this cost, giving a figure of $400 billion per year[14].

Cyber security is of critical importance to Europe’s large companies and organisations running complex IT systems and critical infrastructures. These are in need a corporate-wide approach to cyber risks and hold particular and considerable interest for all privacy and security concerns.

Regardless of the sector, large companies are targets for cyber-attacks:

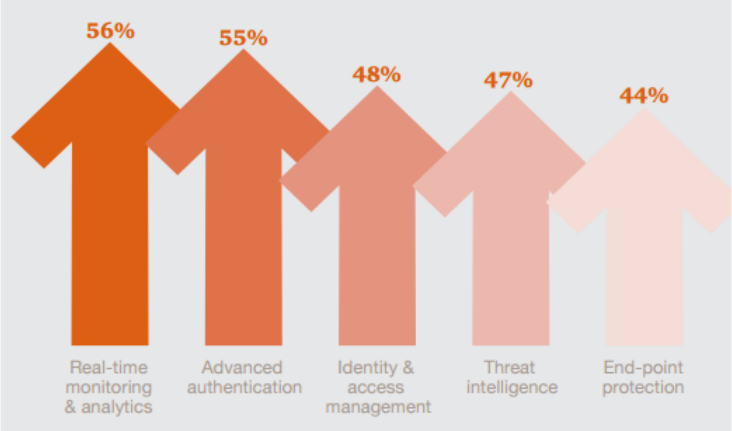
- Telecommunications organisations – in 2015 the number of detected security incidents climbed 45% over the year before.
- Industrial products manufacturers – The cyber theft of «hard» intellectual property (IP) such as product designs doubled in 2015, while loss of «soft» IP like business processes climbed 27% over the year before.
- Retail & consumer organisations – employee & customer records remain top targets of cyber attacks, have boosted their information security budgets by 67% and are investing in risk-based frameworks, cloud based cyber security etc to improve security & reduce risks
- Financial services : organisations are increasing spending and plan to update cybersecurity and privacy safeguards to address risks associated with the Internet of Things

Organisations are increasingly addressing the risks of breaches and improving their ability to deal with them, compared with previous years. A growing number have a formal incident response process in place, including a CERT, more contingency plans are being deployed and, importantly, more report their effectiveness following a breach.

Millions of Euros are lost to cyber-crime each year and online security is a growing concern for businesses of all sizes and from all sectors. For the private sector, the PWC Global State of information security survey 2016[15] highlights key trends:

- 69% organisations use cloud-based cybersecurity services: real-time monitoring & analytic, Advanced authentication, identity & access management, threat intelligence or end-point protection

-



[12] UK Federation of Small Businesses: Cyber Resilience: How to Protect Small Firms in the Digital Economy (June 2016)
[13] http://www.cyberwiser.eu/news/bbc-six-things-firms-can-do-improve-their-cyber-security.
[14] http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/
[15] http://acc-techdata.at/download_pdf/pwc-global-state-of-information-security-survey-2016.pdf

Figure 5 - Adoption of cloud-based cybersecurity services

- 59% Leverage Big Data analytics for security

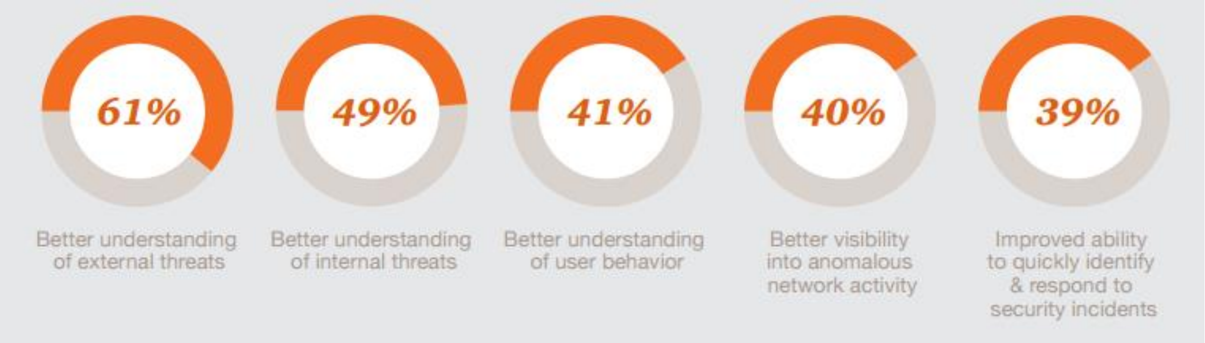


Figure 6 - Benefits of data-driven cybersecurity

.

2.1.3 *Public sector*

One of the key responsibilities of the public sector organisations besides providing citizens with key services is to safeguard the integrity, confidentiality and availability of data, networks and systems.

The entities responsible for protecting sensitive data face a changing regulatory landscape, ongoing budget challenges and a shortage of skilled workers, that is why the adoption of the appropriate and reliable cyber security technologies and solutions becomes crucial.

With digitisation, the public sector is increasingly becoming data controller of important citizen information. Exposure to cyber risks has significant social and financial consequences.

According to the Ponemon Institute[16], public sector companies have the highest estimated probability of having a data breach, which could be attributed to the amount of confidential and sensitive information they collect and store.

The increasing black market value of personal medical data makes the healthcare sector a primary target, with organisations being 340% more likely to be hit by an IT security incident than the average across all sectors. These organisations are also 200% more likely to experience data theft[17].

Educational organisations account for about 9% of disclosed data breaches[18].The per capita cost of a data breach to the public sector is estimated to be around €170 per record, and annual costs of over € 8 million to the public sector.

Recent data shows that there has been a considerable increase in the purchase of cybersecurity insurance and even more impressing, the vast majority of public sector organisations are - 92% - has adopted one or more risk-based cybersecurity frameworks such as ISO 27001 to help boost security capabilities. And more organizations are collaborating with others to share cybersecurity intelligence.[19]

Furthermore according to PWC[20], public sector agencies are investing in a series of core safeguards to better defend their ecosystems against evolving threats:

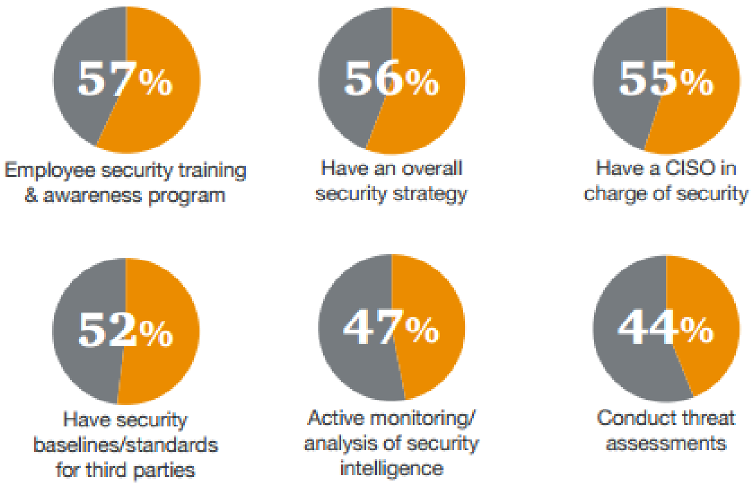
[16] http://www.ponemon.org/library/the-state-of-cybersecurity-in-local-state-and-federal-government.

[17] http://www.cyberwiser.eu/news/healthcare-next-big-cyber-security-target.

[18] http://www.insurancejournal.com/magazines/features/2015/04/20/364390.htm.

[19] https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/pwc-gsiss-2016-public-sector.pdf

[20] https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/pwc-gsiss-2016-public-sector.pdf



Source: The Global State of Information Security® Survey 2016

Figure 7 – Public sector increasing investments in core cybersecurity safeguards

2.1.4 Citizens and general public

It is essential to encourage the industry to supply more secure solutions and stimulate their take-up by citizens. Citizens need to know and trust that the systems underpinning digital services are safe and secure. But citizens and businesses also have to be properly educated and informed about cyber security in order to increase Europe's resiliency and support building the trust in the security of online services in general. Despite the increasingly public nature of cyber attacks on people and businesses, still majority of European citizens, employees and IT experts too are lacking skills to tackle cyber risks.

The recent months have brought the issues related to cybersecurity and attacks more into the public eye. Citizens and the general public, especially as consumers are getting more and more aware of the exposure to cyber-attacks. Awareness raising among the general public is supported through initiatives such as the European Cyber Security Month (ECSM)[21], a pan- EU a campaign that promotes cybersecurity among citizens and advocates for change in the perception by promoting data and information security, education and sharing of good practices.

2.2 Current market figures

The global cyber security market is expected to be among the fastest growing segments of the ICT sector in the coming decade. In 2013 the cyber security market was worth € 59.8 billion (with the European market constituting around 17% of it) and is expected to grow to € 72.6 – € 108.9 billion by 2018. Cyber insurance products deserve a special focus, with a remarkable growth of the global turnover related to annual cyber insurance premiums written from $2,5 billion in 2014 to $7.5 billion in 2020 (the latter is an outlook)[22]. Cyber insurance market is especially intensive in the U.S. This will be addressed in detail in Section 3.3 of this deliverable.

[21] https://cybersecuritymonth.eu/about-ecsm/whats-ecsm

[22] PwC Global State Information Security Survey 2016

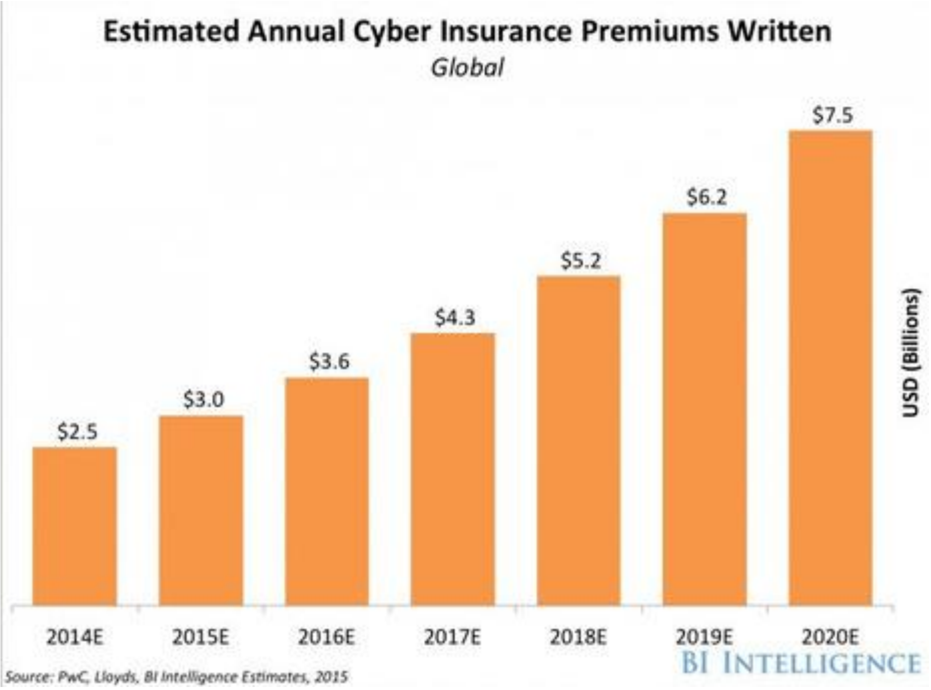


Figure 8 - Evolution of cyber insurance market, according to PwC

The demand for security products and solutions by specific sectors and the overall market, both private as well as public is foreseen to increase in the coming years as a result of the prospective implementation of the currently negotiated NIS Directive and as well as following the efforts to reduce market fragmentation and the confinement to the different EU country policies. The recently approved (April 2016) General Data Protection Regulation[23] is a very important milestone. After a two-year-grace period, all the companies, no matter the size or the business segment, will have to be compliant with the directive, and to report any kind of incident happening. They will be exposed to heavy fines if they do not fulfil this obligation.

Although awareness of vulnerability and risks is fundamental, cyber security should be addressed as a key opportunity for the European businesses and viewed as a potential competitive advantage on the global market.

This would mean not only providing trustworthy solutions for protecting information held by citizens, companies and public institutions but also making sure that the European demand side is a driver for the uptake of innovative cyber security products and services.

A series of policies have been defined as well at the EU level particularly focusing on the demand side with the goal of mainstreaming cyber security across different economic areas by making it a functional requirement in both emerging digital technologies (e.g. cloud, big data, 5G, embedded systems); industrial sectors essential for a well-functioning single market (e.g. energy, automotive, rail, aviation, health, banking, finance…) as well as public administration.

The overarching aim is to increase awareness and stimulate voluntary uptake of cyber security solutions and processes by businesses and public sector organisations.

WISER is focused on a clear understanding of the demand side of the cyber security market as this comes with insight to the requirements, budgeting and challenges of implementing cyber security in different vertical markets.

The current Cyber security market can be divided into different sectors, based also on the different products and services offered:

[23] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

- Infrastructure security
- Data security
- Identity & Access management
- Risk & Vulnerability management
- Education & training
- Other

The figure below provides a visual of the current market from a supply point of view.

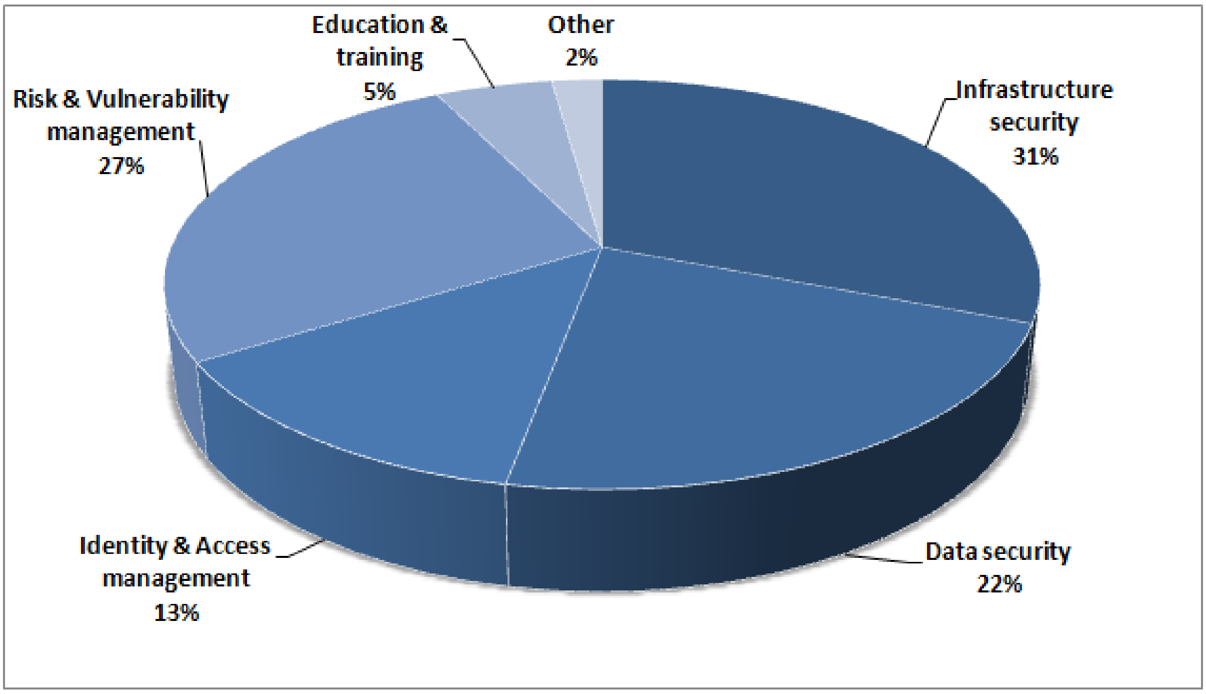


Figure 9- Current cyber security market from demand side

North America and Europe are the leading cyber security revenue contributors, according to a report from TechSci Research. Asia-Pacific is rapidly emerging as a potential market for cyber security solution providers, driven by emerging economies such as China, India and South-East Asian countries, wherein, rising cyber espionage by foreign countries is inducing the need for safeguarding cyber space.

The total cyber security market value has been estimated by Gartner at 68 billion € in 2015 (est. € 68.1 billion)[24]. The following table provides a breakdown of the different market sector with examples of different products and services and an estimate of their economical value.

[24] http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#2715e4857a0b46998c272191

Sector value (in €)	Market sector	Products & Services	Economic value (in €)
21 bn	Infrastructure security	Endpoint & perimeter Security	3bn
		Mobile security	3.5bn
		Cloud security	4 bn
		IoT security	6 bn
		Threat intelligence	3.5 bn
		Other	1bn
15 bn	Data security	Data loss prevention	7.5bn
		Encryption	5.5bn
		Other	2bn
9 bn	Identity & Access management	User Management	2bn
		Authentication & Authorisation	3.5bn
		Identity management	2.5bn
		Other	1bn
18bn	Risk & Vulnerability management	Code analysis	1bn
		Infrastructure & application vulnerability assessment	3bn
		Penetration testing	3 bn
		Policy compliance	4.5bn
		Cyber security insurance	3.5bn
		Other	3bn
3.5bn	Education & training	Awareness raising	1bn
		Training	2bn
		Other	0.5bn
1.5 bn	Other		1.5bn
68bn	**TOTAL**		**68bn**

Table 3 – Products and services

Note: The cyber security market figures presented above have been estimated based on a review of reports from IT industry analysts, vendors, industry associations as well as media organisations.

2.3 Prospect market

Worldwide spending on information security reached € 68.04 billion for 2015, an increase of 4.7% over 2014, according to the latest data from Gartner, Inc. The global cyber security market is expected to be worth € 154.32 billion by 2020.

In a recent report, Cybersecurity Ventures projects $1 trillion will be spent globally on cybersecurity from 2017 to 2021. J.P. Morgan Chase & Co. doubled its annual cybersecurity budget from $250 million to $500 million. Bank of America has gone on the record stating it has an unlimited budget when it comes to combating cybercrime. The U.S. government has increased its annual cyber security budget by 35%, going from $14 billion budgeted in 2016 to $19 billion in 2017 (..) Incremental increases in cyber security spending are not enough (…)businesses of all sizes and types, and governments globally, to double down on cyber protection."[25]

According to IDC, the hot areas for growth are security analytics / SIEM (10%); threat intelligence (10%+); mobile security (18%); and cloud security (50%). Furthermore according to a report from Markets and Markets, the cloud security market is expected to be worth € 7.9 billion by 2019.

The global managed security services market is projected to reach nearly € 27.23 billion by 2020, with a compound average growth rate (CAGR)[26] of 15.8% over the next five years, according to a report from Allied Market Research. The global enterprise governance, risk and compliance (GRC) market is expected to grow from € 5.2 billion in 2014 to € 10.4 billion by 2019, at a CAGR of 14.6% for the period 2014 to 2019, according to MicroMarketMonitor. A new cybercrime wave is driving Internet of Things spending, and its security market is expected to grow from €6.25 billion in 2015 to nearly € 26.3 billion by 2020, according to a report published by Markets and Markets.[27]

A fast growth is also forecasted for the Cyber Security insurance, according to the PwC Global State of Information Security Survey 2016.

3 Supply side

The supplier community operating within the cyber security sector is both complex and fragmented.

It is complex because for many vendors, cyber security is not something that they provide in the form of a discrete product or service, but it is something that is included/ inserted into their wider offering.

For example, Microsoft is by no means a cyber security company, but it invests heavily in ensuring that it has a team of consultants who oversee the implementation on its products in secure environments such as defence and intelligence.

Similarly, Dell is best known as a provider of servers and storage systems, but systems and network security is a key focus area for the company as it looks to adapt to a cloud-centric delivery model.

However, as cyber security market is still growing, a lot of companies have specialised or moved their principal business in IT security positioning themselves or their security operations as pure cyber security players.

As an example, the US giant Intel has decided to resurrect the McAfee brand company as an independent pure-play security firm entirely focused on cyber security challenges.[28]

While many of these firms were born and raised as cybersecurity advisory and consulting services providers, they have updated their business profile including managed security services, products recommendation and implementation, and even their own cybersecurity products or productized services.

This shift of pure play cyber companies clearly documents the requirement for innovative, security-for-a-service companies.

3.1 Stakeholders

Cyber security vendors can be broken down into five different groups:

Global technology vendors & systems integrators:

These kind of players are still predominantly technology/hardware companies, but they compete also in the security infrastructure market in addition to offering security software and services.

The main strategy of these players (such as CISCO and IBM) is to broaden their respective security

[25] http://cybersecurityventures.com/cybersecurity-market-report/

[26] http://www.investopedia.com/terms/c/cagr.asp

[27] Forbes Tech: Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020 - http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/

[28] http://phys.org/news/2016-09-intel-mcafee-cybersecurity-company.html

businesses through acquisitions. This strategy allows companies to offer an increasing variety of security products, potentially cutting down on the number of different vendors a typical organisation depends on.

Defence contractors:

The cybersecurity industry has developed largely on the basis of national governmental demand, including for the defence sector. Most defence contractors such as BAE Systems and Raytheon, have developed cybersecurity divisions or created new business units acquiring companies with existing commercial cyber expertise [29].

Although it is already a crowded market, defence groups could bring new impetus to the market by allowing companies to benefit from the research and advanced data analytics used to protect entire nations.

Local IT services specialists:

Cyber security start-ups have experienced consistent year-over-year growth in funding and deals since 2011. The US and Europe account for most of the total investments in cyber security but the Asian Pacific region has a much higher growth rate, with China and India leading industrial growth in this region. . Israel also stands out as a leader in terms of small-scale specialists with over 430 companies operating in the sector.[30]

Major global consultancies:

The consultancy industry is an increasing part of the business life and special as the international economy gets increasingly more volatile and software driven.

Many consultancy firms have made cyber security a core business line.

According to Gartner, Deloitte Consulting, PwC / Strategy& and EY Advisory are the largest consulting firms of the globe.[31] Demand from the financial services sector and an increasing interest in risk consulting - both of which are signature areas for the Big Four - are driving significant growth.

Telecommunications sector:

An increasing number of telecoms and communications service providers are providing cyber security services particularly as developments like IoT and Big Data, complexities and security challenges in telecom networks and systems have increased manifold. According to the Symantec 2016 Internet Security Threat Report, “many real-world attacks in 2015 identified serious vulnerabilities in cars, medical devices and more. Manufacturers need to reduce the risk of serious personal, economic and social consequences”[32].

Major players such as Vodafone and Samsung have entered the cyber security market thanks to a strategic partnership with BAE systems[33] and strong investment in Cambridge cyber security specialist Darktrace[34].

In October 2016, **ENISA** published its **Annual Incidents** report, providing an overview of the root causes of incidents and an aggregated level of which services and network assets are impacted, revealing patterns that are important for risk and vulnerability assessments while recommending measures to improve security in the telecommunications sector[35].

Most reported incidents usually have an impact on more than one service within the same incident. For example, a faulty hardware change/update caused fixed internet and mobile internet to fail for millions of users (duration: hours, connections: millions, cause: human error). Mobile Internet outages

[29] https://www.ft.com/content/45aedb82-e676-11e5-bc31-138df2ae9ee6.
[30] http://www.globes.co.il/en/article-israeli-cyber-industry-hits-the-big-time-1001114669.
[31] https://www.gartner.com/doc/3317117/market-share-analysis-consulting-services,
[32] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.
[33] http://www.eurocomms.com/industry-news/11435-vodafone-unveils-new-enterprise-focused-cyber-security-unit
[34] http://www.businessweekly.co.uk/news/hi-tech/samsung-invests-darktrace.
[35] ENISA Annual Incidents report, 2016. https://www.enisa.europa.eu/publications/annual-incident-reports-2015.

impacted on average 18% of the national user base. For example, a faulty hardware change/update caused mobile internet to fail for more than an hour impacting a significant number of user connections (duration: hours, connections: millions, cause: system failure). Incidents may also impact on the ability to communicate with an emergency service (20% in 2015).

In the light of the report, ENISA has called for increased transparency and clarity on incidents as essential for risk management and improving the level of security. ENISA will continue to foster and support transparency on incident reporting, promoting a systematic approach towards improved security measures in the sector.

3.2 Main players

There were several notable merge & acquisition transactions during 2016 as the bigger public players – Cisco, Check Point, HP, IBM, Symantec, and others – need to continually add to their arsenal of security solutions as the threat landscape continues to evolve.

As examples CISCO has acquired CloudLock Inc. to bolster its security unit or almost $300 million, Symantec acquired Blue Coat strengthening its cyber defence technology for $4.7 billion.

In the table below we summarized the main top players in cyber security, listing both pure players in cyber security and IT companies with various line of business.

Supply Side						
Actor	**Link**	**Location**	**Sector**	**Products/ Services**	**Revenue**	**Pure-Player**
Symantec	https://www.symantec.com/en/au/cyber-security-services/	USA	Global technology vendors & systems integrators	Encryption Authentication and secure access control Data loss prevention Cloud security	$12.5 billion	Yes
Intel	http://www.intelsecurity.com	USA	ICT Vendors, Consultants, System Integrators, Solution Providers, Managed Service Providers	Encryption Endpoint & perimeter Security Mobile security Cloud security	$13.7 billion	No
IBM	http://www-304.ibm.com/industries/publicsector/us/en/contentemplate1/!!/xmlid=148819	USA	ICT Vendors, Consultants, System Integrators, Solution Providers, Managed Service Providers	Endpoint & perimeter Security	$10.6 billion	No

Supply Side						
Actor	**Link**	**Location**	**Sector**	**Products/ Services**	**Revenue**	**Pure-Player**
HP	http://www8.hp.com/us/en/industries/public-sector.html?compURI=1087532#.Vpd27VIeqT0	USA	ICT Vendors, Consultants, System Integrators, Solution Providers, Managed Service Providers	Data loss prevention Encryption Infrastructure & application vulnerability assessment		
CISCO Systems Inc	http://www.cisco.com/		ICT Vendors, Consultants, System Integrators, Solution Providers, Managed Service Providers		$ 49.24 billion	No
Check Point Software Technologies Ltd.	https://www.checkpoint.com	Israel	ICT Vendors	Network security, Endpoint security, Mobile security, Data security, Security management	$16 billion	Yes
Deloitte	http://www2.deloitte.com/global/en/pages/risk/solutions/cyber-security-services.html	UK	ICT Consultants, Solution Providers	Threat intelligence Data loss prevention	$36.8 billion	No
Ernst and Young	http://www.ey.com/GL/en/Services/Advisory/Cybersecurity	UK	ICT Consultants, Solution Providers	Endpoint & perimeter Security Authentication & Authorisation Identity management Threat intelligence	$29.6 billion	No
Palo Alto Networks	https://www.paloaltonetworks.com	USA	ICT Vendors	Network security,	$12.5 billion	Yes

Supply Side						
Actor	**Link**	**Location**	**Sector**	**Products/ Services**	**Revenue**	**Pure-Player**
Accenture	https://www.accenture.com/us-en/security-index	Ireland	ICT Consultants, Managed Service Providers	IoT security Cloud security	$32.9 billion	No
KPMG	https://home.kpmg.com/xx/en/home/services/advisory/risk-consulting/it-advisory-services/cyber-security.html	Netherlands	ICT Consultants	Infrastructure & application vulnerability assessment	$24.44 billion	No
Fortinet	https://www.fortinet.com	USA	ICT Vendors	Network security, Endpoint security, Data security, Security management	$5.2 billion	Yes
Vodafone	http://www.vodafone.com/business/global-enterprise/enterprise-managed-mobility	UK	Network and Telecoms Players	Mobile security	$40.97 billion	No
Sophos	https://www.sophos.com/en-us.aspx	UK	ICT Vendors	Network security, Endpoint security, Data security, Security management	$446.7 million	Yes
F5 networks	http://www.f5.com/	USA	ICT Vendors, System Integrators, Solution Providers, Managed Service Providers	Network security, Endpoint security, Data security, Security management, Mobile security	$525.3 million	No
VMware	http://www.vmware.com	USA	ICT Vendors, Consultants, System Integrators, Solution Providers,	Network security, Endpoint security, Data security, Security	$1.59 billion	No

Supply Side						
Actor	**Link**	**Location**	**Sector**	**Products/ Services**	**Revenue**	**Pure-Player**
			Managed Service Providers	management		

Table 4 – Supply side: Main players

3.3 Cyber insurance

Cyber insurance is a product created to counter residual risk associated with the information systems of asset owners. While a large number of developments have been taking place in recent years, evidence shows that the cyber insurance market is still at a nascent stage. Many member states are recognising the importance of addressing **cyber risk** and several EU countries have published guides on good cyber-hygiene[36]. Insurance Europe and GDV (Germany) are symptomatic of the increased interest of insurance federations in cyber insurance at both European and national levels.

Cyber insurance, often referenced as “the last line of defence” against cyber attacks, is the quintessential risk transfer mechanism tool, and hence unsurprisingly represents a fast-paced growing market. According to estimates €2.26 billion in cyber insurance premium was written in 2014, while PwC maintains that “the cyber insurance market could grow to € 4.5 billion in annual premiums by 2018 and at least €6.8 billion by 2020”[37].The estimate has been recently upgraded as to actually reach $7.5 billion in annual sales by 2020[38] According to the same report by PCW the main insurance products cover data destruction, denial of service attacks, theft and extortion; they also may include incident response and remediation, investigation and cybersecurity audit expenses. Other key areas of coverage include privacy notifications, crisis management, forensic investigations, data restoration and business interruption. The insurance industry are expanding into policies that cover the value of lost intellectual property, reputation and brand image, as well as cyber-related infrastructure failures.

Main drivers for the cyber insurance market growth are the increase in cyber accidents, both in numbers and severity, as well as regulatory standards and incentives. The US market is a global driver as in fact US companies, legally mandated to disclose data breaches incidents, currently account for the lions’ share of purchases while Europe’s market is lagging behind representing only 10% of the global market. Nevertheless, it should be highlighted that the adoption by 2017 of the EU NIS Directive [see para 3.5], also entailing binding data-breach notification requirements, is expected to drive a sharp increase in the European demand for cyber insurance[39].

If geographic coverage of cyber insurance is skewed, the same holds true when the market is segmented by company size, with large organizations being notably more proactive in seeking coverage and SMEs trailing behind. For instance, an AON Risk Solutions research founded that only 4% of UK SMEs said they had insurance cover in place to help protect them from the implications of cyber attacks, with virtually no change from Spring 2015 (3%)[40] To a significant extent, small and medium-sized business owners do not perceive themselves as preferential hackers’ targets and

[36] France, ANSSI, “40 essential measures for a healthy network”, http://www.ssi.gouv.fr/en/actualite/40-essential-measures-for-a-healthy-network/ and United Kingdon, Department for Business, Energy and Industrial Strategy “Cyber essentials scheme: overview”, https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

[37] PwC, Insurance 2020 & beyond: Reaping the dividends of cyber resilience, 2015 pg. 10 http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf

[38] http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf

[39]ACM, Communications of the ACM, Vo. 58, No. 10, Oct. 2015, pg. 21.

[40] Research findings reported in Burns Eleanor, 5 shocking numbers behind the SME cyber insurance market, Computer Business Review, http://www.cbronline.com/news/verticals/small-business/5-shocking-numbers-behind-the-sme-cyber-insurance-market-4746644 [last accessed on 13/01/2016]

hence do not actively seek to shield against associated risks. However, according to a survey mandated by UK government, last year 74% of small business reported experiencing a data breach, up from 60% in 2014, 38% of them were attacked by an unauthorised outsider in the last year, while 16% of them were hit by a denial-of-service type of attack[41].

Costs of breaches, featuring elements such as business disruption, lost sales, recovery of assets, and fines and compensation, are also sharply increasing for large and small business alike. Again, according to the same survey UK SMEs "lower end for security breach costs increase to £75,200 (from £65,000 in 2014) and the higher end has more than doubled this year to £310,800"[42]. The escalating costs of breaches, a generalised worldwide trend, is mostly driven by the lost business costs component, hence featuring abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill. The lost business costs are difficult to measure and forecast but can also prove particularly vicious and all the more so for SMEs, as one study reports that "sixty percent of small businesses close their doors within half a year of being victimized by cybercrime"[43].

Yet according to the 2015 Betterley survey currently larger/retail/healthcare insured experience rates that are definitely rising in a range comprised between 5 and 50%, while SMEs would face a much friendlier cyber insurance market as "rates are still competitive and renewals are generally flat, perhaps even a bit soft"[44]. Having said that, it is clear that, even for SMEs, the costs of cyber coverage may vary widely, depending on the industry, and that preferred rates and in some instances even eligibility are likely to be based upon the strength of a company's security. Policies systems and practices that can demonstrate a reduction in cyber risk will indeed result in lower cyber insurance costs.

As for the type of costs usually covered by cyber insurance, the Ponemon Institute study reports that according to the survey respondents the top five costs are: forensics and investigative costs (71% of respondents), replacement of lost or damaged equipment (64 percent of respondents) legal defence costs (52% of respondents), notification costs to data breach victims (49% of respondents) and employee productivity losses (45% of respondents). Only 15% of respondents reported coverage for brand damage that, as indicated above, is one of those hard-to-measure variables[45].

Recent research shows that in addition to mitigation of financial risks associated with cybercrime, companies that purchase insurance stand to gain a better understanding of their cyber-readiness. That is because insurers require a thorough assessment of current capabilities and risks as a precondition to purchasing a policy. These evaluations can help businesses better predict legal and regulatory exposures, costs of response, and potential brand damage related to cybersecurity risks and help them improve their cyber hygiene.

A proper cyber hygiene would not only result in lower insurance costs but even more importantly decrease the likelihood of suffering data breaches and ensuing lost business costs against which even cyber insurance may fall short.

More recent insights on cyber insurance and related good practices come from a multi-stakeholder ENISA study, to which WISER partner Aon has contributed – "Cyber Insurance: Recent Advances, Good Practices and Challenges"[46].

In terms of market growth, projections estimate the global insurance market to reach $7.5 billion in

[41] PwC, 2015 Information Security Breaches Survey, UK Department for Business, Innovation and Skills, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf

[42] Ibidem, pg. 6.

[43] BITS Financial Services Roundtable, An Assessment of Cyber Insurance, CTO Corner Feb. 2015, http://fsroundtable.org/cto-corner-assessment-cyber-insurance/

[44] Betterley Richard, CYBER/PRIVACY INSURANCE MARKET SURVEY—2015 For Larger Insureds, a Market in Turmoil For the SME Insured, Eager Insurers Await, Betterley Risk Consultants, 2015, pg. 8, http://betterley.com/samples/cpims15_nt.pdf

[45] Ponemon Institute, 2015 Global Cyber Impact Report, 2015, pg. 14., http://www.aon.com/attachments/risk-services/2015-Global-Cyber-Impact-Report-Final.pdf

[46] https://www.enisa.europa.eu/publications/cyber-insurance-recent-advances-good-practices-and-challenges. AON contributer: Giorgio Aprile.

annual sales by 2020 and over $20 billion by 2025[47]. This growth can be embraced by enabling an informative product development and adoption. Interestingly, the study also highlights the correlation between established legislation on cyber security and higher cyber insurance adoption.

The ENISA study highlights that the European market is expected to grow further with the adoption of the General Data Protection Reform (GDPR – adopted in April 2016)[48] and the Network Information Security Directive (NISD – adopted in August 2016)[49]. According to the ENISA study, these regulatory changes will impact cyber insurance to a considerable extent. Whether they have the form of mandatory notification, the introduction of fines, or "right to know" users, they are expected to result in better market preparation, where cyber insurance also plays a role. The GDPR and NISD may have a similar effect to relevant law-making in the U.S. cyber insurance market. With regard to the NISD, a high level of interest in the cyber insurance market is expected to occur particularly for the following industries:

- Essential services in critical sectors: energy, transport, banking, financial services, health. water supply and distribution, digital infrastructure.
- Digital service providers: online marketplace, online search engine, cloud computing service.

Current evidence reported by ENISA shows how the growth of the cyber insurance market has led to an increased number of claims, functioning as both feedback and an evolutionary force for the market, allowing brokers and product development to improve over time. Knowing the cause of loss is another key factor. British-based insurers writing policies for US-based companies provide a good example of this rising maturity. Exposure to a more legislative environment and mandatory incident reporting has given valuable lessons to these companies well in advance of recently adopted EU regulations.

4 Support to R&D, awareness & policy in cyber security from governments

Cyber security is an essential enabling factor for the development and exploitation of digital technologies and innovation and is linked to future prospects for growth and job creation. Therefore, governments worldwide have set out plans to support R&D and innovation in the field of cyber security.

In this section we briefly analyze new initiatives put in place worldwide to address the challenges of cyber security.

4.1 European Union: H2020

The Commission and the European External Action Service launched the EU Cyber security Strategy in 2013. The strategy outlines the principles that will guide the EU action in this domain – for example on the importance of access to the internet and of the protection of fundamental rights online. It sets five priorities:

1. Increasing cyber resilience;
2. Drastically reducing cybercrime;
3. Developing EU cyber defence policy and capabilities related to the Common Security and Defence
4. Developing the industrial and technological resources for cyber security;
5. Establishing a coherent international cyberspace policy for the EU and promote core EU values.

European Agenda on Security (2015) Fighting cybercrime more effectively is one of the three priorities under the new European Agenda on Security 2015-2020 which was adopted by the Commission in April 2015. Cybercrime requires a coordinated response at European level. Therefore, the European Agenda on Security sets out the following actions:

[47] Allianz Global Corporate & Speciality, "A Guide to Cyber Risk: Managing the Impact of increasing Interconnectivity", http://www.agcs.allianz.com/assets/PDFs/risk%20bulletins/CyberRiskGuide.pdf.
[48] http://ec.europa.eu/justice/data-protection/reform/index_en.htm.
[49] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

- giving renewed emphasis to implementation of existing policies on cyber security, attacks against information systems, and combating child sexual exploitation;
- reviewing and possibly extending legislation on combating fraud and counterfeiting of non-cash means of payments to take account of newer forms of crime and counterfeiting in financial instruments, with proposals in 2016;
- reviewing obstacles to criminal investigations on cybercrime, notably on issues of competent jurisdiction and rules on access to evidence and information;
- enhancing cyber capacity building action under external assistance instruments.

The Key objectives of the European Commission in the field of cyber security are to:
1. Increase cyber security capabilities & cooperation;
2. Make the EU a strong player in cyber security
3. Mainstream cyber security in EU policies.

On cyber security research, significant investment has been made, for example € 350 ml under FP7, allowing for future funding around the twin objectives of strengthening the European industrial base through uptake of research results, and providing financial incentives under Horizon 2020 to develop technological solutions for improved cyber security. This takes place against a background of unprecedented focus on cyber security and increasing instances of major security flaws and cyber attacks. In addition, new technological developments with a high impact, such as cloud computing and big data, are likely to create new security challenges that need to be addressed properly to allow for trustworthy market developments.

The European Commission’s unit of DG Connect Cyber security & Trust envisaged under the Horizon 2020 programme of spending in the order of € 138 ml (years 2014-15), both under H2020 Leadership in enabling and industrial technologies (LEIT) and Societal Challenge 7 on Secure societies.
The goal is to ensure a secure and trustworthy digital environment for the benefit of all EU citizens and businesses, and to promote a coherent international approach on cyber security.

The Digital Assembly 2015 on 17 & 18 June 2015 in Riga key conclusions from the Digital Single Market strategy launch were that: **Trust and confidence** called for a swift implementation of the NIS directive, the establishment of a Cyber security contractual PPP and an initiative on free flow of data / ownership.

4.2 Digital Single Market Strategy (2015)

Trust and security are essential to reap the benefits of the digital economy. This is why the Digital Single Market Strategy adopted in May 2015 includes a public-private partnership on cyber security as one of its 16 key initiatives. The goal of this partnership will be to stimulate European competitiveness and help overcome cyber security market fragmentation through innovation, building trust between Member States and industrial actors as well as helping align the demand and supply sectors for cyber security products and solutions. This partnership will be instrumental in structuring and coordinating digital security industrial resources in Europe. It will include a wide range of actors, from innovative SMEs and national security agencies to producers of components and equipment, critical infrastructure operators and research institutes. The initiative will leverage EU, national, regional and private efforts and resources – including research and innovation funds – to increase investments in cyber security.

Ultimately, the partnership will enable to:

- gather industrial and public resources to deliver innovation against a jointly-agreed strategic research and innovation roadmap;
- maximize the impact of available funds;
- focus on targeted technical priorities defined jointly with industry;
- provide visibility to European research and innovation excellence in cyber security.

The aim is to set up the partnership in the course of 2016. It will be supported by EU funds coming from the Horizon 2020 Framework Programme.

A public consultation has been launched[50] to gather views on the partnership and other possible policy measures to strengthen cyber security capacities in Europe.

4.3 The NIS initiative & WISER EU National Strategies watch

NISD

In August 2016, the European Parliament has passed the new network and information security directive (NISD), which establishes minimum requirements for cyber-security on critical infrastructure operators and digital service providers.

Both these players have to be identified by the Member States based on specific criteria stipulated in the NIS Directive and they will have to take appropriate security measures and to notify significant incidents to the relevant national authority.
The security measures that will need to be implemented should include:

- Technical and organisational measures that are appropriate and proportionate to the risk.
- Measures that should ensure a level of security of network and information systems appropriate to the risks.
- Measures that should prevent and minimize the impact of incidents on the IT systems used to provide the services.

At National level member states will have 21 months to transpose the Directive into their National laws plus 6 months to identify operators of essential services.
More specifically, every member state will:

- Adopt a national strategy on the security of network and information systems.
- Designate one or more national competent authorities to supervise the application of the NISD.
- Designate a point of contact to liaise with other Member States and ensure cross-border co-operation.
- Designate Computer Security Incident Response Teams (“CSIRTs”) to monitor, respond and report on national level incidents.

At European Level a co-operation group with representatives from member states, EU Commission and ENISA will be established to support member states on the activities of the NIS Directive and to report to the EU Commission on a 1.5 yearly basis.

WISER EU National Strategies watch

As result of the activities under Task 6.5: Synergies and international liaison on best practices, a specific cartography of the EU national Cyber Strategy has been produced and make publicly available at www.cyberwiser.eu/cartography

The cartography is built upon the positive experiences of the ENISA map of National Cyber Security Strategy, the BSA Cybersecurity Dashboard, desk research on the current state of national cyber

[50] http://ec.europa.eu/digital-agenda/en/news/consultation-public-private-partnership-cybersecurity

security strategies and individual interviews with national CSIRTs carried out by WISER.

WISER aims at developing a continuously updated cartography service as an information hub, providing accurate and practical information for businesses and organizations who want to have a clear understanding of their national cyber security progress.

This will lead to the possibility to track and identify the progress being made by every member state on compliance with the NIS Directive, highlighting possible gaps, international co-operation and best practice adoptions.

4.4 ECSO & the European cPPP

The cyber security market will become increasingly diverse in the shift towards the “networked society”, which will inter-connect things as well as people while increasing cyber risks.

In July 2016, the EC launched a new public private partnership on cyber security, which is expected to trigger €1.8 billion in investment by 2020. The partnership is part of a series of new initiatives to better equip Europe against cyber attacks and to strengthen the competitiveness of its cyber security sector. Trust and security are seen as critical factors for the DSM, which aims to reinforce co-operation across borders and help develop innovative and secure technologies, products and services across the EU. Within Horizon 2020, the EC will invest €450 million with cyber security market players represented by the European Cyber Security Organisation (ECSO)[51] expected to invest three times that amount.

ECSO is a self-financed, non-profit, industry-led organisation bringing together a wide variety of stakeholders such as large companies, SMEs and Start-ups, research centres, universities, clusters and association as well as European Member State’s local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries.

The main objective of ECSO is to support all types of initiatives or projects that aim to develop, promote and encourage cybersecurity and in particular to:

- Foster and protect from cyber threats the growth of the European Digital Single Market.
- Develop the cybersecurity market in Europe and the growth of a competitive cybersecurity and ICT industry, with an increased market position.
- Develop and implement cybersecurity solutions for the critical steps of trusted supply chains jn sectorial applications where Europe is a leader.

ECSO is engaged in taking concrete actions to achieve these objectives by:

- Collaborating with the European Commission and national public administrations to promote Research and Innovation in cybersecurity
- Propose a Strategic Research and Innovation Agenda (SRIA) and a Multiannual Roadmap with its regular updates.
- Foster market development and investments in demonstration projects and pilots to facilitate bringing innovation to cybersecurity market.
- Foster competitiveness and growth of the cybersecurity industry in Europe (large companies and SMEs) as well as end users / operators through innovative cyber security technologies applications services solutions.
- Support the widest and best market uptake of innovative cybersecurity technologies and services for professional and private use.

[51] http://www.ecs-org.eu/.

- Promote and assist in the definition and implementation of a European cybersecurity industry policy to encourage the use of cybersecurity solutions as well as secure and trustworthy ICT solutions to increase digital autonomy.
- Support the development and the interests of the entire cybersecurity and ICT security ecosystem (including education, training, awareness, etc).

ECSO is working directly with the European Commission to improve Europe's industrial policy on cybersecurity, focusing on innovation and following a strategic R&I roadmap through a Public-Private Partnership[52]. The EU will invest €450 million in this partnership under its research and innovation (R&I) programme H2020. In return, each euro of public funding is expected to trigger additional investments of three or more Euro by the cybersecurity market players represented by ECSO. In total, this partnership on cybersecurity is expected to raise around €1.8 billion of investment by 2020 and with this, develop innovative and trusted cybersecurity solutions, products and services in Europe.

4.5 ENISA – an evaluation framework for cyber Security strategies

ENISA[53], the European Union for Network & Information Security, work on the evaluation of National Cyber Security Strategies (NCSS) addressing to policy experts and government officials who design, implement and evaluate an NCSS policy. It aims to be a flexible and pragmatic tool based on principles rather than prescriptive checklists, in alignment with the provisions of the EU Cyber Security Strategy.

ENISA has created an interactive informative map to present the situation of the cyber-security strategies adoption across the globe.[54]

The ENISA Study on National Cyber Security Strategies aims to produce a **Good Practice Guide** highlighting good practices and recommendations on how to develop, implement and maintain a Cyber Security Strategy. The Good Practice Guide is intended to be a useful tool and practical advice for those, such as regulators and policy makers, responsible and involved in cyber security strategies. National Cyber Security Strategies have not yet been established or implemented in all 28 Member States. Therefore, raising awareness of and promoting good practices in relation to cyber security among the EU Member States continues to be an important task to do in supporting national good practices.

Other initiatives, such as cyberessentials.gov.uk in the UK are worth mentioning, too, for their timeliness and sense of closeness to SMEs, although they provide less overall impact because of their intrinsic size. This programme offers a pragmatic, risk-based approach for smaller organisations to protect themselves from the most widespread forms of threat that derive from the internet.

The ISF produce the **Standard of Good Practice for Information Security** (SOGP) which is updated every two years, the SOGP is the most comprehensive information security guide in the world. It provides complete coverage of other recognised standards such as ISO/IEC 27001:2013, 27002:2013, 27014, and 27036, as well as PCI DSS 3.0 and the NIST Cyber security Framework.

Today, many European Union Member States have published or are in the process of publishing an NCSS (National Cyber security Strategies). Of these, several (e.g., Czech Republic, Estonia, Netherlands and the United Kingdom) have also updated their strategies since their first edition.

National Cyber Security Strategies aim to ensure that Member States are prepared to face serious

[52] http://europa.eu/rapid/press-release_IP-16-2321_en.htm
[53] https://www.enisa.europa.eu
[54] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

risks, are aware of their consequences, and are equipped to appropriately respond to breaches in the network and information system. However, it is not always clear if and how the effectiveness of these strategies is evaluated. Evaluation can be interpreted as a tool to assess if and how well the expected objectives have been achieved and whether the costs involved were justified, given the changes which have been achieved.

4.6 ISACA

ISACA[55] is an independent, non-profit, global association. It engages in the development, adoption and use of globally, accepted industry-leading knowledge and practices for information systems. ISACA is the short name for ‘Information Systems Audit and Control Association. ISACA provides practical guidance, benchmarks and other effective tools for all enterprises that use information systems. Through its comprehensive guidance and services, ISACA defines the roles of information systems governance, security, audit and assurance professionals worldwide.

ISACA has developed and currently maintains the COBIT framework. Besides, ISACA membership and its certification programs are globally accepted and recognized. In fact, independent studies continue to demonstrate that holding an ISACA designation enhances professional recognition, credibility and earning potential. As of today, ISACA offers the following certifications:

- Certified Information Systems Auditor (CISA): This certificate aims at those who audit, control, monitor and assess an organization´s information technology and business systems.
- Certified Information Security Manager (CISM): This certificate targets managerial positions. It is the globally accepted standard for individuals who design, build and manage enterprise information security programs.
- Certified in the Governance of Enterprise IT (CGEIT): This certificate recognizes a range of professionals for their knowledge and application of enterprise IT governance principles and practices. The certificate provides the credibility to discuss critical issues around governance and strategic alignment based on recognized skills, knowledge and business experience.
- Certificate in Risk and Information Systems Control (CRISC). This certification positions IT professionals for future career growth by linking IT risk management to enterprise risk management.

ISACA has singled out cybersecurity by creating ISACA´s Cybersecurity Nexus (CSX)[56]. It is a single, comprehensive source for performance-based certification, networking, professional membership, training and education. Launched in 2014, in response to the growing cybersecurity skills crisis, CSX is a commitment to fortify the industry by educating, training and certifying a stronger, more informed workforce that can keep organizations and their information secure. CSX provides skills-based trainings leading to obtaining a certificate. Not only this, CSX supports cybersecurity research and helps to shape the career roadmap of cybersecurity professionals. CSX conferences are expanding globally. CSX aligns to existing domains: 1) Identify; 2) Protect; 3) Detect; 4) Respond and 5) Recover. The CSX certifications are enumerated below:

- CSX Practitioner: This a globally offered certification allowing holders to professionally serve as a first responder who is an expert at following established procedures, using defined processes and working mostly with known problems on a single system. It is an entry-level certification for professionals who want to demonstrate technical skills and abilities in cybersecurity.
- CSX Specialist: It is the natural leap forward after completing the CSX Practitioner certification. This makes the holder to stand out as a specialist in one or more of the five domains established by the NIST Framework: identify; protect; detect; respond; and recover.

[55] https://www.isaca.org
[56] https://cybersecurity.isaca.org/about-csx

It is a certification for professionals who want to demonstrate deeper, intermediate, technical skills in a expertise area within cybersecurity

- CSX Expert: The holder is a person with an expert level who can identify, analyze, respond to and mitigate complex cybersecurity events. This a certification for professionals with master-level technical skills who serve as the authoritative source for all cybersecurity matters within an organization.

ISACA currently serves more than 140000 constituents (members and professionals holding ISACA certifications) in more than 180 countries. They work in nearly all industry categories. There is a network of ISACA chapters with more than 200 chapters established in over 180 countries. Chapters provide education, resource sharing, advocacy, networking and other benefits.

4.7 International initiatives: the NIST cyber security framework and the U.S examples

The NIST represent a global reference model at worldwide level to define a standard approach to strengthen cyber security especially within the business community. A recent example of how NIST is defining cyber security standard approaches is the 2015 Italian Cyber Security Report, which is based on the reference "Framework for Improving Critical Infrastructure Cybersecurity" developed by NIST but expanded and updated to reflect the Italian context.[57]

NIST takes on international collaborations including its risk management framework. For example, it has worked with the Cloud Security Alliance EU and Global, the SPECS project and SLA-Ready on extensions to its risk management framework and cloud security SLAs.
The NIST Cyber security Framework[58] was developed as a flexible framework of security standards, guidelines and best practices for federal agencies to build upon. Since the first release in 2014, there has been a rapid adoption of the framework. Within the federal government, 82% of agencies[59] are either fully or partially adopting the NIST framework, perhaps more telling is that 53% of organizations[60] outside the federal government have adopted NIST standards. The core functions of the cyber security framework focus on identifying risks, protecting data or deterring threads, detecting threats, incident response and recovery planning. Each of these functions lay out a clear roadmap for organizations of any industry to plan a cohesive risk-based strategy around.
The primary agencies conducting cyber security research within the U.S. Federal Government and internationally include: the Defense Advanced Research Projects Agency (DARPA), the Department of Energy (DOE), the Department of Homeland Security (DHS), the Intelligence Advanced Research Projects Activity (IARPA), the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), the National Science Foundation (NSF), the Office of the Secretary of Defense (OSD), and the Department of Defense Service research organizations in the Air Force, Army, and Navy.
No single agency addresses all the priority areas in the Strategic Plan, rather the many different agency efforts, with guidance from the Strategic Plan and coordination through the Subcommittee on Networking and Information Technology Research and Development (NITRD), enable collective progress towards the Plan's goals.

Improving the security and safety of cyberspace has been an important priority of President Obama's Administration. The 2009 President's Cyberspace Policy Review[61] indeed pointed to cyber security

[57] http://www.cyberwiser.eu/news/italian-cyber-security-report-2015-national-framework
[58] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
[59] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
[60] https://powermore.dell.com/technology/nist-done-lately/
[61] Executive Office of the President of The U.S., Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure (2009), available at

risks as “some of the most serious economic and national security challenges of the 21st Century" and called upon Federal agencies to develop a framework for game-changing cyber security research with the goal of fundamentally improving the security, safety, and trustworthiness of the Nation’s digital infrastructure.

As a result, in December 2011, the National Science and Technology Council *released Trustworthy Cyberspace: Strategic Plan for the Federal Cyber security Research and Development Program*[62], the result of a continuing dialogue between Federal agencies conducting cyber security research, agencies with cyber security as a critical facet of their mission, and leading industry and academic experts.

The Strategic Plan is then a framework for a set of coordinated Federal strategic priorities and objectives for unclassified cyber security research. The challenges identified in the Strategic Plan are clustered around four main thrusts:

- **Inducing Change** – Utilizing game-changing themes to direct efforts towards understanding the underlying root causes of known current threats with the goal of disrupting the status quo with radically different approaches to improve the security of the critical cyber systems and infrastructure that serve society. Within the Inducing Change thrust a number of research themes are then flashed out:
  - ✓ **Moving Target** aiming to develop, evaluate, and deploy diverse mechanisms and strategies that dynamically shift and change over time in order to increase complexity and costs for attackers, limit the exposure of vulnerabilities and opportunities for attack, and increase system resiliency.
  - ✓ **Tailored Trustworthy Spaces** whose vision is to create flexible and distributed trust environments that can support a range of functional and policy requirements arising from a wide spectrum of activities in cyberspace, as well as to support operating capabilities across multiple dimensions, including confidentiality, anonymity, data and system integrity, provenance, availability, and performance.
  - ✓ **Designed-In Security** to develop the capability to design, implement, and evolve software/hardware systems that are resistant to cyber-attacks, while effectively managing risk, quality, cost, schedule, and complexity. Provide assurance evidence necessary to attest to the level of confidence in the system’s ability to withstand attacks.
  - ✓ **Cyber Economic Incentives** whereby a science-based understanding of markets, decision making, and motivators, could promote an environment where deployment of security technology is balanced, providing incentives to engage in responsible behavior and deter criminal and malicious behavior.
- **Developing Scientific Foundations** – Developing an organized, cohesive scientific foundation to the body of knowledge that informs the field of cyber security through adoption of a systematic, rigorous, and disciplined scientific approach. Promoting the discovery of laws, hypothesis testing, repeatable experimental designs, standardized data-gathering methods, metrics, common terminology, and critical analysis that engenders reproducible results and rationally based conclusions.
- **Maximising Research Impact** – Catalyzing integration across the game-changing R&D themes, cooperation between governmental and private-sector communities, collaboration across international borders, and strengthening linkages to other national priorities, such as health IT and Smart Grid.
- **Accelerating Transition to Practice** – Focusing efforts to ensure adoption and implementation of the powerful new technologies and strategies that emerge from the

https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [last accessed on 11/01/20016].

[62] National Science and Technology Council, Subcommittee on Networking and Information Technology Research and Development, Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program (2011), available at https://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf [last accessed on 11/01/20016].

research themes, and the activities to build a scientific foundation so as to create measurable improvements in the cyber security landscape.

Within this framework, industry, academia, and critical infrastructure providers benefit from a host of opportunities offered by the different agencies such as the DHS Small Business Innovation Research program, the NSF's solicitation for the Secure and Trustworthy Cyberspace Program providing funding to university investigators, public-private partnerships like the NIST Smart Grid Interoperability Panel, and so on[63].

As for the resources devoted to the implementation of the Strategic Plan, the President's budget request for 2016 amount to 738.2 million USD[64], an amount only slightly above the 2015 and 2014 figures but more than doubling the 2009 budgetary allocation of 320.1 million USD[65]. These figures testify once more, if needed, that cyber security is perceived by the current US Administration as an extremely high priority and a crucial one as to "allow the United States to continue to lead innovation and adoption of cutting-edge technology, while enhancing national security and the global economy"[66].

5 Other relevant initiatives

5.1 EC-funded & related initiatives

The table below provides a concise analysis of European initiatives that are relevant for WISER from two different perspectives: potential synergies on common goals and helping to position WISER service offer in the EU landscape.

Project / Initiative Description	***Relevance for WISER***
The **National Cyber Security Programme** announced by UK Govt. July 2015 invests £860m to protect and enhance the UK in cyber space & to protect small businesses from cyber attacks.	To engage with the national programme to allow those to test and deploy the WISER tools. Opportunity to showcase best practices.
eIDAS regulation[67] The EU Regulation N°910/2014 on electronic identification and trust services for electronic transactions.	eIDAS offers could be integrated in the products & services array of WISER. Moreover, WISER may attend some of the events it organises throughout 2016 & 2017.
WITDOM *empoWering prIvacy and securiTy in non-trusteD envirOnMents*. **[**H2020; date: Jan 2015 – Feb 2017] produces a framework for end-to-end (E2E) protection of data in untrusted and fast evolving ICT-based environments.	The project focuses around privacy-enhancing solutions, trustworthiness, security & privacy by design. Project results may be showcased on the Cyberwiser. eu website to promote the methodology, tools & guidelines for fast adoption.
Tredisec *Trust-aware, REliable and Distributed Information SEcurity in the Cloud.* [H2020; date: Apr 2015 – Mar 2017] aims at developing systems & techniques to cloud security.	TREDISEC results & best practices may be showcased on the Cyberwiser. eu website to promote the methodology, tools & guidelines for fast adoption.

[63] For a thorough overview of the actions undertaken by the various agencies in furtherance of the Strategic Plan, please see NITRD, Report on Implementing the Federal Cybersecurity Research and Development Strategy, June 2014, available at https://www.nitrd.gov/PUBS/ImplFedCybersecurityRDStrategy-June2014.pdf [last accessed on 11/01/20016].

[64] NITRD, NITRD Supplement to the President's FY 2016 Budget, available at https://www.nitrd.gov/pubs/2016supplement/FY2016NITRDSupplement.pdf [last accessed on 11/01/20016].

[65] NITRD, NITRD Supplement to the President's FY 2010 Budget, available at https://www.nitrd.gov/pubs/2010supplement/FY10Supp-FINALFormat-Web.pdf [last accessed on 11/01/20016].

[66] Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure, *op. cit*., pg. 1.

[67] https://ec.europa.eu/futurium/en/blog/rolling-out-eidas-how-fully-benefit-transformative-nature-electronic-identification-means-eid

Project / Initiative Description	***Relevance for WISER***
Prismacloud *PRIvacy and Security MAintaining Services in the CLOUD* [H2020 research, date: Feb 2015 – Aug 2018] https://prismacloud.eu develops the **next generation of cloud security technologies.**	Mutual synergies can be included on the Cyberwiser. eu website to promote the methodology, tools and guidelines for fast adoption.
CUMULUS *Certification infrastrUcture for MUlti-Layer cloUd Services* [EU FP7, date: Oct 2012 – Sep 2015] supports the certification of security properties of services in cloud.	The work in cloud certification as an enabling technology for building trust for end users can be fed into Cyberwiser. eu website
MASTER Managing assurance, security and trust for services [EU FP7, date: Feb 2008 – Jan 2011]. One of the first IPs to approach trust&security with a coherent BPM and risk management approach	Best practices the IT security models coupled with the methodological and verification tools for the analysis and assessment of business processes. Useful for the analysis of the risk management framework.
OPTET *OPerational Trustworthiness Enabling Technologies* [EU FP7, date: Nov 2011 – Oct 2015] http://www.optet.eu/ defines an approach to cover all relevant aspects of trust and trustworthiness.	The cross-disciplinary model of trust and trustworthiness designed in OPTET can be used in the project for the socio-economic model.
NIST Cyber Security Programme - The NIST *Framework for Improving Critical Infrastructure Cybersecurity*[1] to manage cyber security related risk	WISER Partners regularly engage with NIST cybersecurity framework & associated Roadmap for Improving Critical Infrastructure Cybersecurity.
ACDC *Advanced Cyber Defence Centre.* Project bringing together organizations from 14 European countries, including public administrations, private sector and academia, in order to achieve a sustainable victory over a powerful cyber threat commonly known as botnet	Sharing of data and the pool of knowledge to help organizations across Europe to fight botnets. One ACDC goal was to deploy an infrastructure of interconnected support centres across European Member States linked to a central ACDC clearing house. The goal of the infrastructure was to provide solutions to users to fight botnets, and to build up through data collection an analysis capability of botnets occurrence and behaviour to also provide early detection of emerging botnets. Botfree.eu and their national Antibotnet Advisory centres are a significant result to improve prevention, detection and mitigation of botnets.
NECOMA *Nippon-European Cyberdefense-Oriented Multilayer Threat Analysys.* FP7 project aiming at providing new means to understand cyberthreats and to mitigate their effect on infrastructure and endpoints	Development of new background as far as countermeasures definition and implementation are concerned.
Cyber Security Protection Alliance (CYSPA) – FP7. A European Alliance that brings together 17 organisations,from across industry and research.	Increases the capacity of industry to protect itself from cyber disruptions. Best practices in cyber security. Broadens industrial networks for the project
International Cyber Security Protection Alliance (ICSPA) business-driven organisation comprising large national and multi-national companies.	Sharing information and best practices on increased capability, knowledge, training, skills, capacity and expertise. Identifying case studies.
Europol European Cybercrime Centre (EC3). EC3 strengthens the law enforcement response to cybercrime in the EU to help protect citizens, businesses and governments.	EC3 is a potentially significant partner particularly in relation to threat awareness activity for citizens, threat intelligence arrangements for enterprise, and cyber incident response activities.

Project / Initiative Description	*Relevance for WISER*
Compositional Risk Assessment and Security Testing of Networked Systems (RASEN). RASEN strengthens organisations' ability to conduct security assessments of large scale networked systems through the combination of security risk assessment and security testing, taking into account the context in which the system is used, such as liability, legal and organisational issues as well as technical issues.	RASEN results related to security risk assessment method and techniques for updating the risk picture based on test results. In particular, the RASEN results are useful for the exposure and mitigation modelling block in WISER.
Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSoS). NESSoS aims at constituting and integrating a long lasting research community on engineering secure software-based services and systems.	Best practices addressing security concerns related to system analysis and design, identification and detection of vulnerabilities, as well as systematic treatment of security needs.
VISION: Visual Privacy Management in User Centric Open Environments: This project delivers a visual privacy management platform targeting public administrations. This platform empowers any citizen to achieve desired levels of privacy by creating and monitoring a personal Privacy Level Agreement. The platform provides clear visualization of privacy preferences, relevant threats and trust issues along with an insight into the economic value of user data.	The focus on privacy is highly relevant for WISER. The project may benefit from the extensive research done on the issues that entail threats for the user privacy.
ECOSSIAN: European Control System Security Incident Analysis Network: The mission of ECOSSIAN is to improve the detection and management of highly sophisticated cyber security incidents and attacks against critical infrastructures by implementing a pan-European early warning and situational awareness framework with command and control facilities.	WISER may benefit from the knowledge gained thanks to the strong focus on critical infrastructures of the ECOSSIAN Project. This is especially relevant for a clear target of CyberWISER-Plus, which are the managers of critical infrastructures.
TRESPASS: Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security: This project provides a tool playing the role of 'attack navigator'. This tool makes possible to predict and assess threats basing on systematic brainstorming. On top of that, it adds an analysis of most effective countermeasures. To this end, the project combines knowledge from technical sciences (how vulnerable protocols and software are), social sciences (how likely are people to succumb to social engineering) and state-of-the-art industry processes and tools.	The predictive capabilities and countermeasure analysis features of TRESPASS are of high interest to WISER
PANOPTESEC is producing a cyber defence decision support system that will account for the dynamic nature of information and communication technologies, and the evolving capabilities of cyber threats	Findings from PANOPTESEC with respect to mitigation measures and empowering the decision makers provide background of high interest for WISER.

Project / Initiative Description	*Relevance for WISER*
CANVAS: Constructing an Alliance for Value-driven Cybersecurity. This is a Coordination Support Action aiming at tackling the challenge of aligning cybersecurity with European values and fundamental rights. Within three years, CANVAS aims to bring together stakeholders from key areas of the European Digital Agenda – the health system, business/finance, and law enforcement/national security – for discussing challenges and solutions when aligning cyber security with ethics	As a cybersecurity project, the WISER Consortium is interested in participating in this initiative, contributing with WISER partners´ view on the challenge cybersecurity ethics poses and benefiting from the insights of these discussions. Along with this, CANVAS is expected to help to boost the outcomes of WISER and ease the communication tasks, in order to achieve an appropriate transfer of project results to real world market
RESISTAND: Increasing disaster Resilience by establishing a sustainable process to support Standardisation of technologies and services: Resistand aims to identify new ways to improve the crisis management and disaster resilience capabilities of the European Union and individual Member States through standardization. The objective is to contribute to an improved disaster resilience by identifying and analyzing the drivers, constraints and expectations of three main stakeholder communities: Standardisation Organizations, End-users and Suppliers, consisting of researchers, industry and SMEs.	Cooperation with RESISTAND may be a way to explore the way WISER could contribute to standards on cyber risk management.
IPACSO – Innovation Framework for ICT Security: FP7 Coordination and Support Action ran from November 2013 to October 2015. IPACSO aims to support ICT Security innovators with state of the art innovation methodologies and best practices in their innovation process, that will help them to find their road to market faster, more effective and more efficient.	Keeping track of innovative solutions in cyber security landscape thanks to the IPACSO framework for innovation development, specifically aimed at cyber security & privacy innovators.

Table 5 – EC-funded initiatives

5.2 Cybersecurity & Privacy Clusters

Cyber Security Clusters are informal groups of small companies who actively work in cyber security mainly at a national or local level. The Clusters bring together private companies and public sector to promote the uptake of cyber security products and services as well as raise awareness, share best practice, and build cyber resilience.
For example, the UK has 17 cyber security clusters where small companies work together to take on the security threats in their regions: they hold regular updates, seminars and best practices across the country.

The following section highlights some of the key initiatives that are driving the cyber security awareness and technology development, both globally and within Europe.

UK Cyber Security Forum (UK) - www.ukcybersecurityforum.com/

Consortium of 120 SME companies across the UK with focus on cyber security. Companies are grouped into six regional clusters (Cambridge, London, Malvern, North East, North West, South Wales).

Hague Security Delta (Netherlands) - www.thehaguesecuritydelta.com

HSD is the largest security cluster in Europe, gathering businesses, governments, and knowledge institutions working together on innovations and knowledge in the field of cyber security, national and urban security, protection of critical infrastructure, and forensics. The Hague Security Delta has taken the initiative to stimulate cooperation with other regions that are strong in safety and security. First steps have been made, connecting to regions in France (Aix-en-Provence – SAFE Cluster), Denmark (Denmark - CenSec), Finland (Tampere – Safety and Security Region) and Germany (Karlsruhe – KIT, Munich – Security Cluster). The ambition is to jointly stimulate innovation in the security domain. This will ultimately lead to European solutions, reduce fragmentations and create industrial opportunities for systems and processes that are world class. Starting point is to share experiences and practices, promote education, create and share high quality facilities, support the exchange of people and seek for common action and cooperation in (European) research programmes.[68]

Distretto Cyber Security (Italy) - www.distrettocybersecurity.it

The DCS is a joint initiative between Italian large companies, universities and research centers which aims at implementing safer models for the interaction of the end-user with the internet services, for the protection of the end user in the utilization of network services via mobile devices and for the secure document dematerialisation.

5.3 Information Security forum Ltd (ISF) [69]

The Information Security Forum (ISF) is an independent, not-for-profit organisation with a Membership comprising many of the world's leading organisations featured on the Fortune 500 and Forbes 2000 lists and many governmental cyber security authorities. The ISF provides Members with a trusted and confidential environment within which their in-depth knowledge and practical experience can be shared. This approach enables the ISF to harness the collective insights and knowledge of its Members to deliver leading-edge solutions and standards that are comprehensive, pragmatic and effective. They have extensive experience in the field of information risk assessment and strong pedigree in identifying up and coming cyber threats (‘Threat Horizon’) will lend valuable context to this activity.

6 WISER prospect market and positioning

Data privacy and trust have become critical business requirements as exponentially more consumers and business information is generated and shared.
As a result, forward-thinking organizations are pivoting toward a new model of cybersecurity capable of acting on analytic inputs and adaptive to evolving risks and threats.

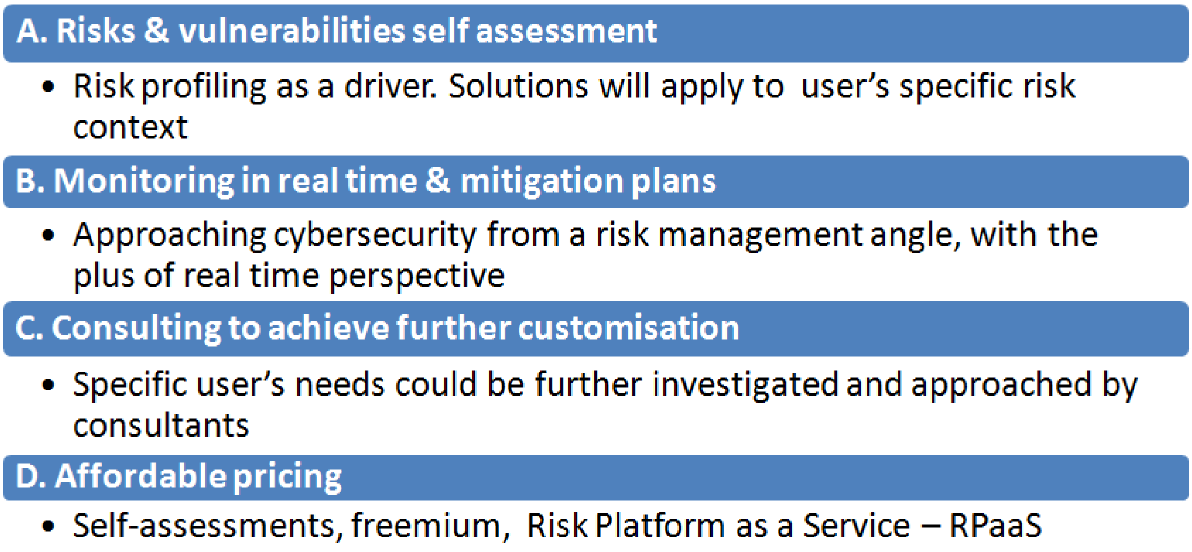
However the majority of businesses are outsourcing a range of technology safeguards to managed security providers, including authentication, data loss prevention, identity and access management,

[68] https://www.thehaguesecuritydelta.com/news/newsitem/661-common-ambitions-strengthening-cooperation-between-european-security-clusters
[69] www.securityforum.org

and real-time monitoring.
In fact, almost two-thirds (62%) of Global State of Information Security Survey 2017 respondents say they use security service providers to operate and enhance their cybersecurity strategies[70].

A primary driver is the global dearth of skilled cyber security specialists. A recent report by Cybersecurity Ventures predicted that the existing cybersecurity workforce gap will widen to 1.5 million job openings by 2019[71]. The ongoing talent squeeze is likely to drive more organizations to turn to third parties to help run some or all of their security programs.
Cost is another factor. Businesses may not have the resources to hire an end-to-end team of full-time cybersecurity and privacy professionals. Or they may need to scale an existing solution but do not want to tie up highly skilled in-house staff to execute a relatively simple initiative.

WISER will directly address these needs by offering competitive advantages through the following features:



A. Risks & vulnerabilities self assessment

- Risk profiling as a driver. Solutions will apply to user's specific risk context

B. Monitoring in real time & mitigation plans

- Approaching cybersecurity from a risk management angle, with the plus of real time perspective

C. Consulting to achieve further customisation

- Specific user's needs could be further investigated and approached by consultants

D. Affordable pricing

- Self-assessments, freemium, Risk Platform as a Service – RPaaS

Figure 10 - WISER competitive advantages

6.1 Innovation potential

WISER is an Innovation Action and, as such, it focuses on packaging of existing technical and commercial assets of the various Partners to define an innovative offering and draw for it a path to market. The go to market strategy, as detailed in Deliverable D8.7 - exploitation plan & business models, 1st version highlights the initial main elements of innovation brought forward by WISER and outlines new assets following the project developments as listed below:

- **Sensoring:** End-to-end reliable monitoring approach with accurate tamper-proof transference of data from signalling components (deployed at the edge of the infrastructure) to the monitoring core.Additional testing module that performs vulnerability scans on its targets vulnerabilities of the machines and applications within the target infrastructure, which could be potentially exploited by a hacker to obtain some kind of advantage. Wide coverage of cyber

[70] http://www.pwc.com/us/en/cfodirect/multimedia/webcasts/global-state-information-security-survey-2017.html
[71] http://cybersecurityventures.com/jobs/

threats and vulnerabilities monitored and analysed, by supporting new signalling technologies, event formats and semantics.The WISER Network and application sensors are in charge of collecting information at the network and application levels respectively. These are enhanced by WISER although they can be decoupled and independent from other WISER entities.

- **Monitoring Engine:** Real-time security analytics to correlate fast-growing and increasingly complex data generated in current and emerging cyber ecosystems.The WISER monitoring module provides continuous analysis of huge amounts of data. It aggregates data from many sources and provides the ability to consolidate and correlate data to generate events and alarms.
- **Risk Assessment Engine based on innovative risk models:** assessment of the cyber risk of the Company combining information coming from both the ICT and the business sides. Reporting of such risk both in qualitative and quantitative (economical) terms. Modelling tools allow users to create the appropriate risk models basing on what risk assessment is carried out. The purpose of the risk model is to identify the risks and vulnerabilities of relevance for the client organization. Once the risk models are created a set of model rules are defined to shape the way the risk is calculated, based on information coming from the configuration, the testing and the monitoring
- **Support to the decision-making process**: WISER provides a feature allowing the user to analyze in terms of cost and benefit possible mitigation measures recommended by the framework according to the calculated risk. In addition, the user is made aware of the societal impact associated to the risk. This societal impact is non-visible but has a harming effect on the company. A specific feature enables its assessment basing on the answers to a set of questions. This evaluation is done per each risk detected and evaluated.
- **Service provision based on an on-line model** with two approaches: a SaaS (Software as a Service Solution) and RPaaS (Risk Platform as a Service). Ultimately, the user can also go for a prepackaged solution where the whole framework is deployed on its premises. For more details, the user can refer to deliverable D2.4[72].
- **Target a wider range of organizations, allow for three modes of operation of the service** (CyberWISER'Light, CyberWISER-Essential, CyberWISER-Plus) as detailed in Section 1.4 provisioning :
  - **CyberWISER-Light** is specifically designed for small and medium-sized enterprises (SMEs), providing a user-friendly cyber risk self-assessment tool available online for free. It is simple, quick and effective to use so SMEs can make cyber security a top priority without having to invest time and resources.
  - **CyberWISER-Essential** is a solution for self-assessment of cyber risk exposure levels that incorporates continuous real-time monitoring.
  - **CyberWISER-Plus** evolves the features of CyberWISER-Essential providing a higher degree of customization, in terms of integration with the client´s existing systems and tailoring of sensors, with the engagement of the WISER consultants team and their specific skillset.
- **And, above all, making cybersecurity affordable for all the companies, no matter the size, the sector or the available resources. CyberWISER services put the company in control with a smart 'Do It Yourself' approach and will ensure that cybersecurity becomes part of the business process.**

6.2 The WISER positioning

When describing the current security services market along the dimensions of external support / customisation needed (hence, the pricing of the intervention) and degree of innovation of it (hence, the potential effectiveness of it against the current cyber-threats), WISER aims to position itself in a quite distinctive way from current best players, as illustrated in Figure 5 - Current offerings and

[72] D2.4: Framework Prototype. Chapter 2.2 on the delivery modes and the architecture.

WISER positioning. In particular, WISER will differentiate itself from its competitors through the following aspects:

- Real-time risk assessment monitoring tool & Mitigation actions - WISER provides a cyber risk management framework able to assess, monitor and suggest mitigation measures in real time. The WISER risk assessment approach focuses not only at the level of a given ICT system, but also considering the business processes or services that depend on it. It also considers the societal impact of risk and helps to determine the most appropriate mitigation action(s).
- Affordable pricing - Due to the real-time monitoring and the increase of automatization of this assessment, prices could be more competitive, and be affordable for segments as SMEs, that have a low budget for these types of services.
- Customization through consultancy services - The mitigation plan could be designed and communicated by consultants if customers opt for more customized approach. In this way, companies do not need to have internal resources to a non-core business activity critical as cybersecurity.

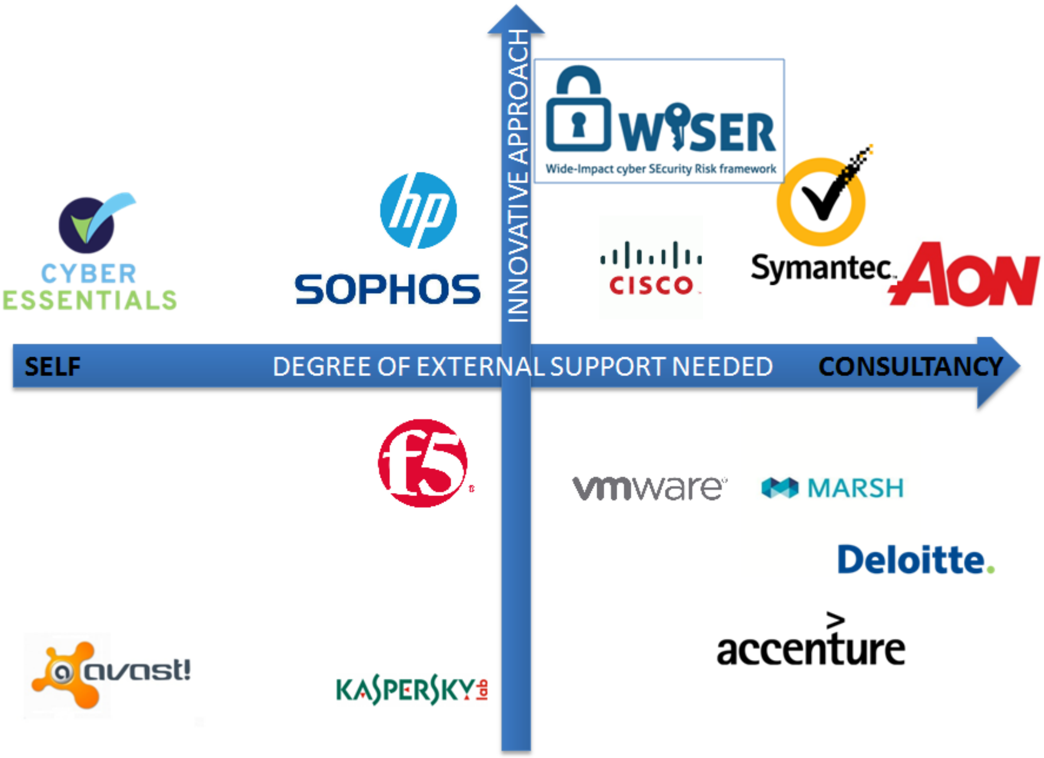


Figure 11 – Current offerings and WISER positioning

6.3 Value chain

A representation of the security services value chain is reported below, where the objective of the WISER initiative is also represented.

The WISER perimeter and positioning in the cyber security services value chain is grounded/topical to: Security Assessment, Continuous Risk Management & Mitigation

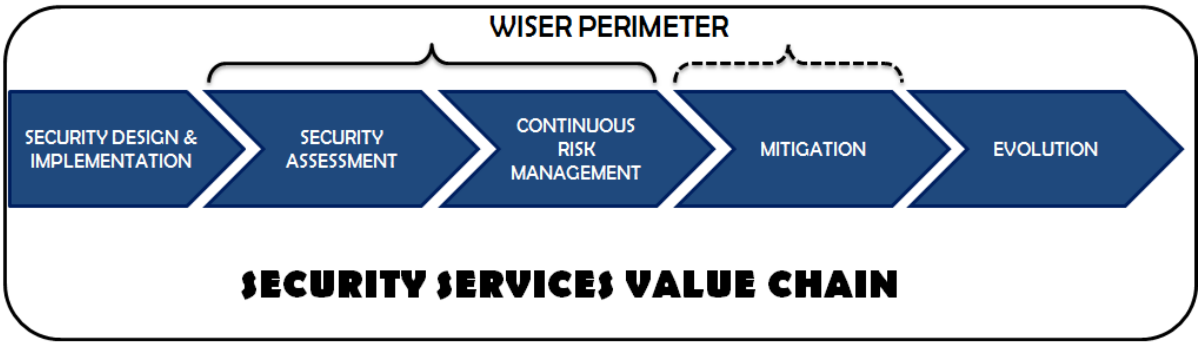

WISER PERIMETER
SECURITY DESIGN & IMPLEMENTATION
SECURITY ASSESSMENT
CONTINUOUS RISK MANAGEMENT
MITIGATION
EVOLUTION
SECURITY SERVICES VALUE CHAIN

Figure 12 – The security services value chain and WISER

6.4 SWOT

A SWOT analysis for WISER is reported below.

STRENGTHS	WEAKNESSES
• Assets delivered by WISER partners & individual networks as multipliers • Innovation potential of the WISER concept (risk management applied to cyber security) • Continuous monitoring of the market & policy alignment • Multi-industry approach & customised approach for different target audiences • Real-time risk assessment monitoring tool & Mitigation actions • Online delivery & Affordable pricing for advanced solutions • Advanced service offer consisting in the delivery of customised assessment & mitigation plan	• WISER relatively limited investments • Limited visibility of the WISER initiative • Support needed for integration of WISER components in basic/advanced mode • Trust related barriers to market entry

OPPORTUNITIES	THREATS
• Rapidly expanding market • PA and Large Enterprises increasingly aware • More funding from local governments soon available • NIS Directive & GDPR • WISER targets specific target segments (i.e. SMEs) that cannot afford IT consultant fees but will be able to assess risks. • Leveraging on National & International Multipliers cooperation (ENISA, CERTs,ECSO etc.) • Regulatory pressures – stimulating the demand for ready to use cyber security solutions	• Rapidly evolving competition • High level of public stimulation package in the US that may result in ground-breaking new solutions. • Persistent low level of awareness among SMEs of the financial and reputational implications of the cyber risks they are facing, • Lack of generally available stimulation initiatives dedicated to SMEs • Growing number of online tools & fragmented market

Figure 13 – SWOT analysis for WISER

7 Conclusions

The main conclusions from the second version of the Market Watch report (http://www.cyberwiser.eu/Market-watch) are:

- The market is fast evolving with an ever-growing opportunity to be seized, particularly by encouraging the market to value and therefore manage cyber risk correctly.
- Within the prospective cyber security market, risk management in real time can be the differentiating asset.
- More specifically, on the demand side a considerable opportunity is emerging as demand is forecast to grow exponentially in coming years.
- Spending will continue to increase as more organisations define and implement appropriate levels of security controls through internal resources.
- On the supply side, a few large players are already present with commercial approaches. However still a lot of what is currently offered is consultancy-based which entail high costs.
- Notably some online tools are emerging, but overall there are still plenty of opportunities to be seized.
- Governments are currently playing a decisive role in stimulating the economy through policies entailing a mix of incentives, regulation, and awareness raising actions.
- Regulatory pressures to build resilience and develop mitigation plans have increased especially for organisations managing private data
- A number of clusters, associations and initiatives have been launched across Europe around the topics of cybersecurity and privacy, these provide a key forum of discussion and platforms for knowledge exchange and innovation
- In spite of progress brought on improved informative campaigns and media coverage, there is a need to move away from the current mind-set where cyber security is associated with costs to one that acknowledges that a proper cyber security risk management enables to save costs and exploit digital opportunities to their full potential.
- The is a growing number of organisations that are starting to understand that cybersecurity solutions can also facilitate business growth, create market advantages and build brand trust.

The third and final Market Watch document will be delivered in project month 30, offering the consolidated analysis of the WISER market and value chain positioning as well as the up to date market overview, factors affecting growth including policies, market constraints and development prospective.