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

D7.1 - MARKET WATCH, FIRST VERSION

Work Package	WP7, Market Validation and Roll-out to Other Verticals
Lead Author (Org)	Silvana Muscella, Paolo Lombardi, Stephanie Parker, Timea Biro, Niccolò Zazzeri, Luisa Nardi, (Trust-IT)
Contributing Author(s) (Org)	Silvana Muscella, Paolo Lombardi, Stephanie Parker, Timea Biro, Niccolò Zazzeri, Luisa Nardi, (Trust-IT); Ales Cernivec (XLAB); Atle Refsdal (SINTEF); Antonio Álvarez (ATOS); Elena González (ATOS); Roberto Mannella (Rexel),
Due Date	29.02.2016 M9
Date	26.02.2016
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	13.11.2015	Paolo Lombardi, Trust-IT	ToC, first version
0.2	07.01.2016	Paolo Lombardi, Stephanie Parker, Timea Biro, Niccolò Zazzeri, Trust-IT	First draft
0.3	12.01.2016	Silvana Muscella, Paolo Lombardi, Stephanie Parker, Timea Biro, Niccolò Zazzeri, Luisa Nardi, Trust-IT	Expanded version
0.4	15.01.2016	Silvana Muscella, Paolo Lombardi, Stephanie Parker, Timea Biro, Niccolò Zazzeri, Luisa Nardi, Trust-IT	First complete draft, for contributions to all involved Partners
0.5	15.01.2016	Silvana Muscella, Paolo Lombardi, Stephanie Parker, Timea Biro, Niccolò Zazzeri, Luisa Nardi, Trust-IT	Edits to the first complete draft, for contributions to all involved Partners
0.6	28.01.2016	Ales Cernivec (XLAB), Antonio Álvarez (ATOS),Elena González (ATOS), Roberto Mannella (Rexel),	Contribution to sections 3, 3.1, 3.7 and 3.10
0.7	29.01.2016	Silvana Muscella, Paolo Lombardi, Stephanie Parker, Timea Biro, Niccolò Zazzeri, Luisa Nardi, Trust-IT	First version ready for internal review
0.8	24.02.2016	Silvana Muscella, Paolo Lombardi, Stephanie Parker, Timea Biro, Niccolò Zazzeri, Luisa Nardi, Trust-IT	First version ready for GA approval
1.0	26.02.2016	Antonio Álvarez (ATOS)	Final version submitted to EC

Disclaimer

Table of Contents

List of Tables

List of Figures

Executive Summary

The main goal of this document are to provide an analysis of the WISER market and to define the WISER value chain positioning. Hence, more specifically this document sets out to:

- Report on market conditions by analysing both demand and supply sides.
- Perform a customer/service positioning analysis, including a SWOT and other pre-commercial analyses (including benchmarking activities).
- Identify the potential and requirements to roll-out to other verticals, including detailed analysis of the top 10 verticals, besides Energy and Banking.

Based on the study conducted, the main takeaways of this document:

- Currently there is a big market opportunity to be seized.
- 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.
- The latent demand is particularly relevant for SMEs, also in terms of awareness & 'light-weight' services, reducing or removing the need for specialised consultancy (see Cyber WISER Light.
- 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.
- 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.

Thus, overall it can 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

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 cyber strategy.

Grag Case quotation from the AON 2015 Global risk survey: "For the first time since 2007, damage to brand and reputation has emerged as the top-ranked risk in our survey. Interestingly, cyber risk has entered the top 10 for the first time this year. The connection between these two risks has been felt around the world in 2014, as a rash of data breaches demonstrated the fragile nature of consumer trust in leading corporations".

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 will provide a cyber-risk management framework that will enable companies to assess, monitor and propose risk mitigation measures on a continuous basis, and make cyber-risk management an integrated business process. .
The design of three modes of operations (See section 1.1.3 Go to Market Path) will lead to the rollout as three tools, benefitting ICT-intensive small- and medium-sized enterprises (SMEs) and multiple industries responsible for critical infrastructures and complex systems. Concisely, WISER's three modes of operations are:

- An online assessment tool (commercial name: Cyber WISER Light) giving a first very high-level view of cyber risk exposure;
- A pre-packaged risk management solution (commercial name: Cyber WISER Essential);
- A risk management platform as a service (RMPaaS) mode of operation for highly complex cyber systems requiring the implementation of special controls within the ICT system to be monitored (commercial name: Cyber WISER Plus).

1.1.1 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 will provide 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.

1.1.2 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.

1.1.3 Go-to-market path

WISER delivers a cyber-risk management framework able to assess, monitor and mitigate the risks in real time, in multiple industries. The three WISER tools will satisfy different unmet needs in the private and public sectors with potential customer segments spanning a range of market verticals.

Rollout 1 – Cyber WISER Light, April 2016
Target audiences: small businesses
Benefits: increase the awareness of cyber-risks for their businesses through self-assessment. It is a user-friendly approach for small businesses that lack the time, money and skills to invest in cyber risk management.
Access: online registration on www.cyberwiser.eu

The Cyber WISER Light leverages existing tools available. Organisations can make get a first, high-level view of their cyber risk exposure free of charge and with minimum investment in time and human resources. The tool provides two levels of report. The first report provides a risk assessment based on answers to an online questionnaire. The second report considers information vulnerability scan run in a non-intrusive manner against the user's infrastructure to protect. It is up to the user to decide which report opts for.
Overview of marketing plan:
The launch of CYBERWISER Light represents the first major demonstration of the WISER innovation action. In order to maximise visibility and usage, every partner in the consortium will contribute to the marketing campaign.
All partner SME recruitment

- Each partner will recruit a minimum of 20 SMEs to use CYBERWISER Light.
- Further additional recruitment of early users will come from participation at relevant events by promoting the business opportunities.

Pre-launch announcements:

- Web banner announcing the launch approximately one month before.
- Short slide deck for use at events and on social media.
- Inclusion in updated flier.

Press and Media

- Trust-IT will produce a short media release in English on the business benefits of the CYBERWISER Light.
- ATOS will translate the press release into Spanish for the national business media.
- Partners will send details about their contribution to the circulation plan.
- Trust-IT will produce an exclusive feature for Science Node targeting the research community with a box on the launch of CYBERWISER Light. Publication of the article will coincide with the launch of the tool.

Online campaign:
All partners will contribute to the social media campaign.

- Twitter banner on the tool.
- Google Ad words drawing attention to the tool.
- Twitter ad and pinned tweets.
- Trust-IT will produce a social media plan with sample tweets, handles, hashtags and timings for partners to replicate. The plan will indicate the social media tools used to monitor results and impact. Handles will include target SMEs/business multipliers and relevant media channels.

Synergies:

- CSP Forum to ensure pre-announcements appear on the web site and in newsletter ahead of the launch, followed by publication of the press release and awareness-raising via social media.
- Cyber-security initiatives in Europe, inviting them to support awareness-raising through their websites and social media.

Rollout 2 – Cyber WISER Essential, December 2016

A pre-packaged solution, targeting SMEs and ICT systems in general which can have basic needs for RM, would provide the user the necessary information for risk management on a continuous basis, educating users on the basic vulnerabilities and threats to consider.

Rollout 3 – Cyber WISER Plus, December 2016

On-demand services by a Risk Platform as a Service, intended for critical infrastructure or highly complex cyber systems requiring the implementation of special controls within the ICT system to be monitored, to allow for the real time and cross-system assessment of vulnerabilities and threats.

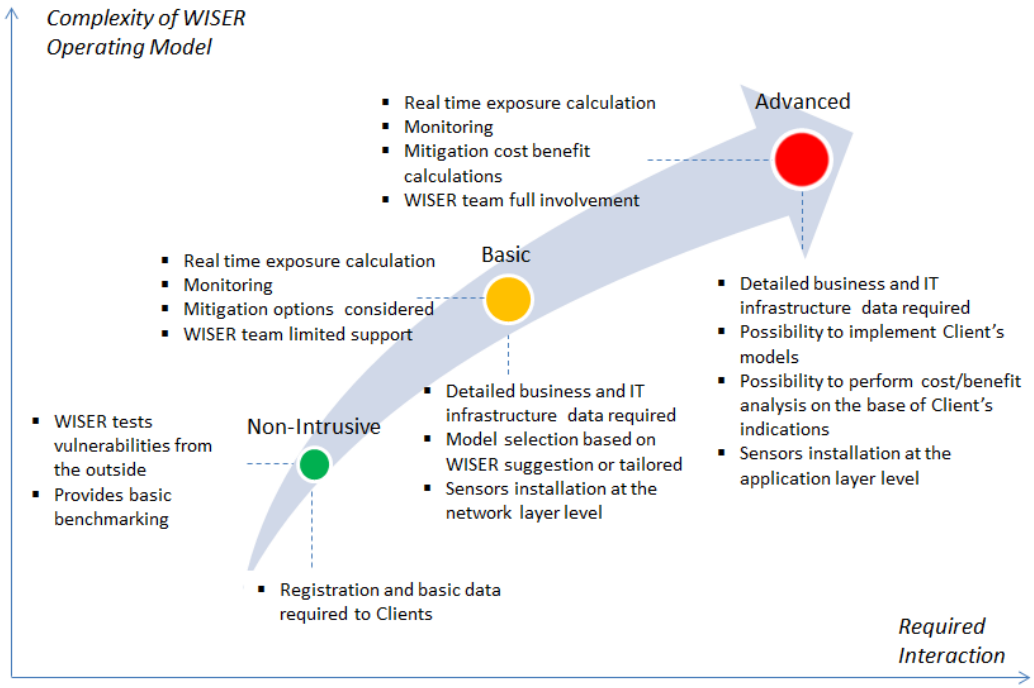

Figure 1 The WISER 3-level offer (non-intrusive Cyber WISER Light, basic Cyber WISER Essential, advanced Cyber WISER Plus)

1.2 The WISER market perimeter

The WISER rollout to market will deliver:

- A truly dynamic, scalable and flexible monitoring infrastructure with plug-and-play mechanisms for dynamic registering of signalling components to adapt to modern dynamic technological contexts;
- 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;
- Wide coverage of cyber threats and vulnerabilities monitored and analysed, by supporting new signalling technologies, event formats and semantics;
- Real-time security analytics to correlate fast-growing and increasingly complex data generated in current and emerging cyber ecosystems;
- Improve situational awareness with regards to cyber risk exposure, both in terms of performance (real-time, high volumes) and coverage of target infrastructures (enterprise-wide and inclusive of both physical and IT security, and all sub-services that depend on a given ICT system at risk.);
- Real-time assessment of the trade-off between societal and economic impact associated to the application of cyber risk mitigation strategies at different levels (basic ICT system, its supported services and the wider scope), in view of the economics of mitigating or eliminating the risk, in a manner inspired by advanced insurance models;
- Ensure the fast transposition of research results into commercial products and services responding to well-identified market needs with the most suitable industrialised business models.

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 are benefitting from the potential of the digital economy, thus building their trust to stimulating their uptake of cyber security technologies and solutions is essential. [1]

2.1 Stakeholders & target audiences

Businesses, public entities and the 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.

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 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.[2]
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.[3]
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

[1] Cybersecurity Industry Roadmap – European Commission Public Private Partnership on Cybersecurity http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_cnect_004_cybersecurity_en.pdf
[2] http://ec.europa.eu/growth/smes/business-friendly-environment/performance-review/files/annual-report/infographics_en.pdf.
[3] http://ec.europa.eu/growth/smes/business-friendly-environment/performance-review/files/supporting-documents/2014/annual-report-smes-2014_en.pdf

	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. In recent years, they have helped create around 80% of new jobs.

Table 1 – European Statistics on Small Firms

Small businesses have recently been drawn into the spotlight as subject to high potential losses due to cybersecurity risks. According to a recent survey, 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"*[4].

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[5] cyber-attacks around the world every day, costing the global economy about €420 billion a year. Large companies, and organisations operating critical infrastructures or complex IT systems need a corporate-wide approach to cyber risks.

Large companies include owners of critical infrastructures and complex IT systems, as well as industry influencers. It is also one of the audiences which holds a particular and considerable interest for all privacy and security concerns.

Specific targets are C-Level executives, especially chief information security officer (twitter hashtag for these stakeholder targets: #CISO), chief information and technology officers (twitter hashtag for these stakeholder targets: #CIO/CTOs) that represent the main IT decision makers, but also chief executive and financial officers (twitter hashtag for these stakeholder targets: #CEO/CFOs) to encourage businesses to pursue a corporate approach (also called "joined-up" approach in the media) to cyber security risk management across different market sectors.

Cyber security is of critical importance to Europe's large companies running complex IT systems and critical infrastructures.

Millions of Euros are lost to cyber-crime each year and online security is a growing concern for businesses, with attacks increasing against large corporate businesses and critical infrastructures.

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 constantly 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[6], 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. Yet only 10% add cyber protections to existing insurance policies[7].

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

5 http://www.cyberwiser.eu/news/bbc-six-things-firms-can-do-improve-their-cyber-security.

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

7 http://www.insurancejournal.com/magazines/features/2015/04/20/364390.htm.

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[8].
Educational organisations account for about 9% of disclosed data breaches[9].
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.

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.

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.

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.
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:

- Infrastructure security

[8] http://www.cyberwiser.eu/news/healthcare-next-big-cyber-security-target.
[9] http://www.insurancejournal.com/magazines/features/2015/04/20/364390.htm.

- 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.

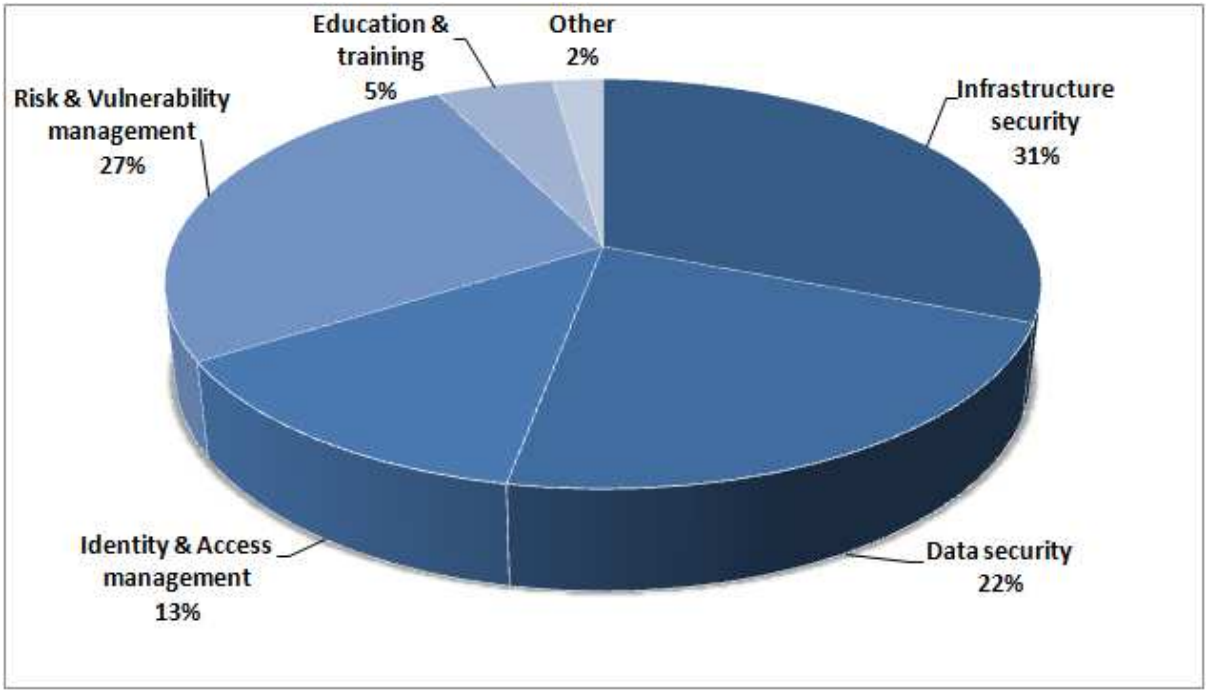

Figure 2- Current cyber security market from demand side

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)[10]. 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.

[10] 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 2 – 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. 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)[11] of 15.8% over the next five years, according to a report

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

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.[12]
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.

3.1 Stakeholders

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

Global technology vendors & systems integrators:
Ranging from multi-billion international players (e.g. Symantec) to small and local specialists. Global IT giants such as IBM or HP have reinitiated their security strategies while others such as Microsoft, SAP, Oracle and Dell are also important in this market by integrating security features into their products and by acquiring security software companies. There are also companies that are surpass these giants by prospects in the fields of network visibility, threat detection solutions or intelligence, such as Lancope, AlienVault and Norse, all these ranked in top 10 of most prospective cyber security companies in 2016[13].

Defence contractors:
In specialised areas such as biometrics or encryption, defence and homeland security specialists, such as Northrop Grumman, Thales or EADS, are very active. Players from this market also sell pure software solutions or virtual appliances.

Local IT services specialists:
There is a very large community of small, local services companies focused on providing cyber security expertise to public and commercial sector organisations. As we shall see, the majority of these companies are very small in scale (typically less than 50 employees and <£1m annual revenue), and generate much of their business on the back of the networking contacts of senior management figures.

Major global consultancies:
Many of the leading management and business consulting groups have established cyber security advisory arms as their clients in both the public and commercial sectors see external help with their

[12] 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/
[13] http://cybersecurityventures.com/cybersecurity-500

security strategies. For example, KPMG has more than 200 information security experts based in the UK.

Telecoms operators:
Telcos have invested heavily in cyber security. The link between security, cloud and mobility are strengthening their positioning and security is one of their assets to invade the IT landscape. For example, BT's Assure division pools together more than 1,800 security consultants, architects and designers worldwide.

The cyber security market will only become more diverse over the next years as a much greater array of devices become inter-connected and the targets for cyber attacks evolve.

3.2 Main players

Symantec, Intel and IBM are the three largest security companies. IBM is the fastest growing security vendor. On the other hand analytics show that a new breed of pure-play cyber firms has emerged. These niche firms focus exclusively on cyber security advisory, consulting, risk management, data breach and incident response, and managed security services. The pure-play firms tend to be smaller and regionally focused, and cater to the needs of CISOs (chief information security officers) at mid-sized up to Fortune 500 corporations.[14]

Supply Side				
Actor	**Link**	**Location**	**Sector**	**Products/ Services**
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
Intel Security	http://www.intelsecurity.com/	USA	ICT Vendors, Consultants, System Integrators, Solution Providers, Managed Service Providers	Encryption Endpoint & perimeter Security Mobile security Cloud security
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

[14] Forbes Tech: The Business of Cybersecurity: 2015 Market Size, Cyber Crime, Employment, and Industry Statistics - http://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics

Supply Side				
Actor	**Link**	**Location**	**Sector**	**Products/ Services**
HP	http://www8.hp.com/us/en/industries/public-sector.html?compURI=1087532#.Vpd27VleqT0	USA	ICT Vendors, Consultants, System Integrators, Solution Providers, Managed Service Providers	Data loss prevention Encryption Infrastructure & application vulnerability assessment
Dell	http://www.dell.com/learn/us/en/rc1009777/fed-solutions-information-security	USA	ICT Vendors, Consultants, System Integrators, Solution Providers, Managed Service Providers	Data loss prevention User Management Authentication & Authorisation Identity management
Deloitte	http://www2.deloitte.com/global/en/pages/risk/solutions/cyber-security-services.html	UK	ICT Consultants, Solution Providers	Threat intelligence Data loss prevention
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
Accenture	https://www.accenture.com/us-en/security-index	Ireland	ICT Consultants, Managed Service Providers	Iot security Cloud security
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
Atos	http://atos.net/en-us/home/your-business/defense-and-security/cyber-security.html	France	ICT Vendors, Solution Providers	Infrastructure & application vulnerability assessment Penetration testing Encryption Data loss prevention
CGI	https://www.cgi.com/en/informatio	Canada	ICT Vendors,	Cloud security

Supply Side				
Actor	**Link**	**Location**	**Sector**	**Products/ Services**
	n-security/cybersecurity		ICT Consultants, System Integrators	Cyber security insurance
Thales	https://www.thalesgroup.com/en/worldwide/critical-information-systems-and-cybersecurity	France	Managed Service Providers	Mobile security Cloud security Penetration testing Threat intelligence
T-Systems International	http://security.t-systems.com/solutions/enterprise-cyber-security	Germany	ICT Vendors, ICT Consultants , Network and Telecoms Players	Data loss prevention
BT Global	http://www.globalservices.bt.com/us/en/industries/defence/cyber_security	UK	Network and Telecoms Players	Mobile security
Vodafone	http://www.vodafone.com/business/global-enterprise/enterprise-managed-mobility	UK	Network and Telecoms Players	Mobile security

Table 3 – Supply side: Main players

Note: some examples of cyber security main players revenues are: Symantec € 2.791.014, Intel Security € 1.659.694, IBM € 1.351.400.

Innovative partnerships are also on the rise pushing forward state-of-the-art solutions like the one between the technology commercialisation company, Crossword Cyber security Plc, and the leading accountancy firm, MHA MacIntyre Hudson, to co-market Rizikon, a new cyber risk analysis tool.
Under the terms of the agreement, MHA MacIntyre Hudson, with 85 partners and over 550 staff servicing the UK, will introduce Rizikon to its large client base of small and medium-sized enterprises. Rizikon builds on four years of research and development and among benefits it brings are its jargon-free summaries of a company's existing security, broken down into the areas of greatest risk. It also recommends adjustments to existing protections, such as anti-virus and firewalls, to maximize their effectiveness[15].

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

To stimulate the economy on a very sensitive issue, governments worldwide have set out plans to support R&D and innovation in the field of cyber security. The two most relevant efforts are H2020 from the European Commission and the initiatives performed in the US especially by NIST. In the following sections, we present these initiatives, as well as some other major efforts in the cyber security field.

[15] http://www.city.ac.uk/news/2016/jan/crossword-cybersecurity-plc-develops-cyber-risk-assessment-tool-utilising-city-research

3.3.1 *ENISA – an evaluation framework for cyber Security strategies*

ENISA[16], 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.[17]
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 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.

3.3.2 *European efforts on providing an EU28 Cyber security landscape.*

In 2015, the BSA Software Alliance created a cyber security dashboard[18] to provide government officials in each EU member state with an opportunity to evaluate their country's policies against these metrics as well as their European neighbours. The report examined five key areas of each EU Member State's cyber security policy environment:

- Legal foundations for cyber security;
- Operational capabilities;

[16] https://www.enisa.europa.eu
[17] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world
[18] http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf EU Cyber security Dashboard – A Path to a secure European cyberspace

- Public-private partnerships;
- Sector-specific cyber security plans;
- Education

The report[18] states that only 19 of the 28 Member States have more or less detailed and comprehensive cyber security strategies in place, while eight have not declared any such framework at all. Even in the case of those countries with adopted cyber security strategies, the quality of these is variable, many remaining vague and high-level, lacking a clear implementation plan. Furthermore, most of these documents seem static.
Only a small number of countries have already revised and improved their initial strategies and published an updated one. Finally, only a minority of the Member States have reinforced their cyber security strategy with relevant legislative and policy instruments that address security, information classification obligations and critical information infrastructure protection requirements.

The report provides country summaries of the cyber security landscape.
For more detailed information on each country surveyed, refer to the detailed Member State summaries available at www.bsa.org/EUcybersecurity.
WISER services come at a crucial time to help tap into each one of these country bases and their individual CERT services. (i.e. CERT.LV, GOVCERT.LU, CERT-PT etc..) One of our activities will be to contact each EU28 once the WISER services come into place.

3.3.3 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:

- 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.

3.3.4 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.[19]

NIST on the takes several 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[20] 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[21] are either fully or partially adopting the NIST framework, perhaps more telling is that 53% of organizations[22] 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.

[19] http://www.cyberwiser.eu/news/italian-cyber-security-report-2015-national-framework
[20] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
[21] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
[22] https://powermore.dell.com/technology/nist-done-lately/

Improving the security and safety of cyberspace has been an important priority of President Obama's Administration. The 2009 President's Cyberspace Policy Review[23] indeed pointed to cyber security 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*[24], 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

[23] Executive Office of the President of The U.S., Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure (2009), available at https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [last accessed on 11/01/20016].
[24] 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].

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 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[25].

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[26], an amount only slightly above the 2015 and 2014 figures but more than doubling the 2009 budgetary allocation of 320.1 million USD[27]. 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"[28].

[25] 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].
[26] 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].
[27] 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].
[28] Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure, *op. cit.*, pg. 1.

3.4 Cyber insurance

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"[29].

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[30].

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%)[31] To a significant extent, small and medium-sized business owners do not perceive themselves as preferential hackers' targets and 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[32].

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"[33]. The escalating costs of breaches, a generalized 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"[34].

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"[35]. Having said that, it is clear that, even for SMEs, the costs of cyber

[29] 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

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

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

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

[33] Ibidem, pg. 6.

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

[35] 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. Available at

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 defense 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[36].
Then, 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.

3.5 The NIS initiative

The NIS Directive, proposed by the Commission in 2013 and currently agreed on by the European Parliament and the Council, aims to ensure a high common level of cyber security in the EU.

Specifically, the NIS directive is aimed at reducing fragmentation within 28 different member states with 28 rulebooks, 28 referees and 28 mind sets with regard to cyber security measures.

The new rules of the Network and Information Security (NIS) Directive act on three levels:

- Improve cyber security capabilities in Member States.
  Each Member State is obliged to have a national strategy, to identify who will enforce this and to set up a Computer Security Incident Response Team to handle incidents and risks.
- Improve Member States' cooperation on cyber security.
  According to Günther H. Oettinger, Commissioner for the Digital Economy and Society, "Improving cooperation and information exchange between Member States is a key element of the agreed rules and will help us tackle the increasing number of cyber-attacks."[37] The competent authorities in EU member states and the European Commission will form a co-operation network to co-ordinate against risks and incidents affecting network and information systems. The network will exchange information between authorities, provide early warnings on information security issues and agree on a co-ordinated response in accordance with an EU NIS co-operation plan.
- Impose new security and incident reporting requirements on a broader range of private sector companies.
  The NIS directive will demand that 'operators of critical infrastructures' or 'critical national infrastructure market operators - which include those working in the energy, financial services, health and transport sectors, alongside public sector bodies adopt appropriate steps to manage security risks and to notify serious incidents to the relevant national authority.

http://betterley.com/samples/cpims15_nt.pdf
[36] Ponemon Institute, 2015 Global Cyber Impact Report, 2015, pg. 14. Available at http://www.aon.com/attachments/risk-services/2015-Global-Cyber-Impact-Report-Final.pdf
[37] http://europa.eu/rapid/press-release_IP-15-6270_en.htm

3.6 Other relevant initiatives

3.6.1 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[38] to gather views on the partnership and other possible policy measures to strengthen cyber security capacities in Europe.

3.6.2 Information Security forum Ltd (ISF) [39]

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.

3.7 EC-funded 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**	To engage with the national programme to allow

[38] http://ec.europa.eu/digital-agenda/en/news/consultation-public-private-partnership-cybersecurity
[39] www.securityforum.org

Project / Initiative Description	*Relevance for WISER*
announced by UK Govt. July 2015 invests £860m to protect and enhance the UK in cyber space & to protect small businesses from cyber attacks.	those to test and deploy the WISER tools. Opportunity to showcase best practices.
eIDAS regulation[40] 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.
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. Contribution to the background on sensoring and monitoring.
NECOMA *Nippon-European Cyberdefense-Oriented Multilayer Threat Analysys.* FP7 project aiming at providing new means to	Development of new background as far as countermeasures definition and implementation are concerned.

[40] 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*
understand cyberthreats and to mitigate their effect on infrastructure and endpoints	
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.
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.

Table 4 – EC-funded initiatives

3.8 Prospect market

The Global Cyber security Market 2015-2025 report predicts the industry to reach € 15.7 billion by 2025 at a CAGR of 4.23%[41].
Cyber security is constantly evolving as new threats appear every day and attacks become more sophisticated. The rise of the Internet of Things is starting to create yet more points of vulnerability, as all manner of devices—refrigerators, pace makers, cars, etc. are becoming networked together. Penetrating one can give hackers access into all.

The network security market is estimated to account for 44% of the global cyber security market. Data security and Identity and Access security are also expected to account for a significant portion of the total cyber security market during the forecast period, with shares of 25% and 16% respectively.
Lastly, the cyber security industry has become keenly aware that there are not enough cyber security professionals to meet its needs. This shortage is a very significant problem for the industry as a whole and will continue to be so for the foreseeable future, especially given the rate of high profile cyber attacks.
Israel is second to the U.S. as the largest exporter of cyber products. The Asia-Pacific cyber security

[41] http://www.businesswire.com/news/home/20160113005544/en/Research-Markets-Global-Cyber-Security-Market-2015-2025

market is expanding and being driven by DDoS (distributed denial-of-service) attacks, adoption of cloud computing and mobile devices. Cybercrime and cyber security spending are on the rise in a maturing Latin American region.[42]

3.9 Job watch

The WISER JobWatch, part of the marketing and communication activities of WISER, is an online service that not only advertises cyber security jobs, but also enables the periodic monitoring of the job market, including salary brackets and expected incentives for eSkills and training.
The WISER job watch can be found on the WISER media platform (www.cyberwiser.eu) at the page: http://www.cyberwiser.eu/job-watch. At the moment, the service is a simple selection of relevant opportunities extracted from probably one of the most authoritative sources currently available: https://www.cybersecurityjobsite.com/ . Other opportunities are collected, for instance from the EC website: http://ec.europa.eu/euraxess/index.cfm/jobs/index.

However, at this moment, the central objective of the WISER JobWatch is not so much to excel in timely collection and publishing of the requests for cyber security profiles, which is outside of the remit of the WISER work plan, rather providing the cyber wiser visitors a first overview of what opportunities are shaping up across Europe, thereby contributing to the development of a full awareness of the cyber security field, also in terms of impact on the human resources themes and career opportunities.

Having said that, a first attempt to gauge available figures on the cyber security job market is an extremely valuable exercise as it can be assumed as a proxy indicator for the wider cyber security market. Then, provided below are some of the main highlights concerning the cyber security job market:

- CISCO estimates there are more than 1 million unfilled security jobs worldwide[43];
- Demand is expected to rise to 6 million globally by 2019, with a projected shortfall of 1.5 million, says Michael Brown, CEO at Symantec[44];
- As for the US cyber security job market a Peninsula Press analysis of numbers from the Bureau of Labor Statistics reports that more than 209,000 cyber security jobs in the U.S. are unfilled, and postings are up 74 percent over the past five years[45];
- Again, in so far as the US is concerned, experts at $(ISC)^2$ are reported to expect the demand for cyber security professionals to spike by 10.8 percent each year from 2014 to 2019, with the supply only increasing by 5.6 percent over the same time range[46];
- Lastly, again a rather comprehensive analysis of the US cyber security job market provides insights on how the demand for certificated cyber security talent is outstripping supply by noting that such job postings took 8% longer to fill than IT job postings overall and advertised an average 9% salary premium in comparison with other IT job postings.

In conclusion we believe it can be safely assumed that the above shown data provide additional evidence of a larger and blooming cyber security market.

[42] *The Business of Cybersecurity: 2015 Market Size, Cyber Crime, Employment, and Industry Statistics*, Morgan, S.,Forbes Tech, available at: http://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics last accessed on Jan. 29, 2016]
[43] *Mitigating the Cybersecurity Skills Shortage Top Insights and Actions from Cisco Security Advisory Services*, pg. 2, Cisco, 2015, available at http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf [last accessed on Jan. 29, 2016]
[44] *One Million Cybersecurity Job Openings in 2016*, Morgan,S., Forbes Tech, Jan 2 2016, available at http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#422b5c227d27[last accessed on Jan. 29, 2016]
[45] *Demand to fill cybersecurity jobs booming*, Setalvad A., March 31 2015, Peninsula Press, Stanford Journalism, available at: http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/ [last accessed on Jan. 29, 2016]
[46] *Inside Cybersecurity's Booming 2016 Job Market*, PYMNTS, Jan 5, 2016, available at: http://www.pymnts.com/news/security-and-risk/2016/inside-cybersecuritys-booming-2016-job-market/ [last accessed on Jan. 29, 2016]

3.10 Innovation potential

The main elements of innovation brought forward by WISER that are still relevant vis-à-vis the market conditions at the time of writing the present report are:

- Develop a truly dynamic, scalable and flexible monitoring infrastructure with plug-and-play mechanisms for dynamic registering of signalling components to adapt to modern dynamic technological contexts
- 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.
- Wide coverage of cyber threats and vulnerabilities monitored and analysed, by supporting new signalling technologies, event formats and semantics
- Real-time security analytics to correlate fast-growing and increasingly complex data generated in current and emerging cyber ecosystems
- Improve situational awareness with regards to cyber risk exposure, both in terms of performance (real-time, high volumes) and coverage of target infrastructures (enterprise-wide and inclusive of both physical and IT security, and all sub-services that depend on a given ICT system at risk.)
- Real-time assessment of the trade-off between societal and economic impact associated to the application of cyber risk mitigation strategies at different levels (basic ICT system, its supported services and the wider scope), in view of the economics of mitigating or eliminating the risk, in a manner inspired by advanced insurance models.
- Target a wider range of organizations, allow for two modes of operation of the service (Cyber WISER Light, Cyber WISER Essential, Cyber WISER Plus) provisioning :
    - (i) Basic risk management: delivered as a pre-packaged solution, targeting SMEs and ICT systems in general which can have basic needs for RM, would provide the user the necessary information for risk management, in real time, highlighting to the user the basic vulnerabilities and threats to consider.
    - (ii) Advanced mode: delivered as on-demand services by a Risk Platform as a Service, intended for critical infrastructure or highly complex cyber systems requiring the implementation of special controls within the ICT system to be monitored, to allow for the real time and cross-system assessment of vulnerabilities and threats.

4 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.

Figure 3 – Current offerings and WISER positioning

4.1 Value chain

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

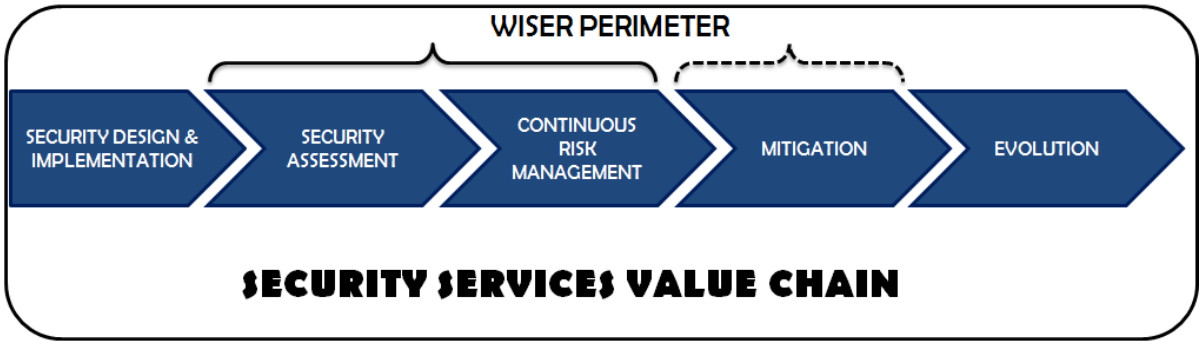

Figure 4 – The security services value chain and WISER

4.2 SWOT

A preliminary SWOT analysis for WISER is reported below.

STRENGTHS	WEAKNESSES
• Assets delivered by WISER partners • Innovation potential of the WISER concept (risk management applied to cyber security) • Awareness of the market • Multi-industry approach	• WISER relatively limited investments • Limited visibility of the WISER initiative • Support needed for integration of WISER components in basic/advanced mode
OPPORTUNITIES	**THREATS**
• Rapidly expanding market • PA and Large Enterprises increasingly aware • More funding from local governments soon available • Forthcoming NIS Directive • WISER targets specific target segments (i.e. SMEs) that cannot afford IT consultant fees but will be able to assess risks.	• 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

Figure 5 – SWOT analysis for WISER

5 Conclusions

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

- Currently there is a big market opportunity to be seized
- Continuous risk management can be the differentiating asset
- On the demand side a considerable opportunity is emerging
- The latent demand is particularly relevant for SMEs, also in terms of awareness & 'light-weight' services (see Cyber WISER Light)
- On the supply side a few large players are already present with industrial approach, but still a lot is consultancy-based, hence high-cost projects are entailed
- Some online tools are emerging, but a lot of opportunities there
- Governments are currently playing a decisive role in stimulating the economy
- There is a need to move away from the current mindset, where cyber security is associated only with costs, to one that acknowledges that a proper cyber security risk management actually *saves* costs and enables organizations to make full use of digital opportunities.