WISER
Wide-Impact cyber SEcurity Risk framework

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

<D8.1 - MEDIA PLATFORM>

Work Package	WP8, Go to Market
Lead Author (Org)	Stephanie Parker (Trust-IT)
Contributing Author(s) (Org)	Ales Cernivec (XLAB), Roberto Mannella (REXEL), Paolo Lombardi (Trust-IT), Timea Biro (Trust-IT)
Due Date	M03
Date	31.08.2015
Version	1.0

Dissemination Level

☒ 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	Author	Notes
0.1	13.07.2015	Stephanie Parker (Trust-IT)	Table of Contents
0.2	20.07.2015	Stephanie Parker (Trust-IT)	Sections 2 and 3.
0.2	24.07.2015	Timea Biro (Trust-IT)	Sections 4 and 5
0.3	27.07.2015	Paolo Lombardi (Trust-IT)	Section 6 and general integration/review.
0.4	27.07.2015	Stephanie Parker (Trust-IT)	Final edit before 1st internal review done by Ales Cernivec (XLAB), Roberto Mannella (REXEL)
0.5	17.08.2015	Stephanie Parker, Timea Biro (Trust-IT)	Edit in answer to 1st review comments, before 2nd internal review Ales Cernivec (XLAB), Roberto Mannella(REXEL)
1.0	26.08.2015	Timea Biro, Stephanie Parker, Paolo Lombardi (Trust-IT)	Edit in answer to 2nd internal review; Final Version

Disclaimer

Table of Contents

List of Figures

Executive Summary

The main purpose of *Work Package 8 – Go to Market* is to help transform the innovation of WISER into tangible market uptake prospects. Adopting a market-driven approach from the very outset, this WP will develop a strong business case for the WISER risk management framework, widely promoting benefits for critical infrastructures and small firms based on their specific needs.

The WISER media platform, operated at www.cyberwiser.eu, plays a key role in communicating the WISER value proposition to key customer segments and stakeholders. Designed as a dynamic web platform, **cyberwiser.eu will stand out for** its **high-quality, highly relevant** and **practical content to inform and offer new services to increase resilience to cyber threats. The design and navigation** of the **website will evolve alongside the progress of the project, becoming increasingly market facing** and **service-oriented** (see Sec. 4).

The main focus of the WISER media platform is:

- Raise **awareness** and facilitate an understanding of the cyber threat/vulnerabilities landscape through “essential guides” and a dedicated Market Watch, showcasing findings & excellence in the field of cybersecurity.
- Offer a practical **entry point for potential customers of WISER services** based on specific needs. The approach will be hands-on, given the “Innovation Action” connotation of WISER and a key goal shall be driving WISER as a “trusted partner” when it comes to cyber security risk management.
- Be in-synch with the cyberwiser **social media** channels that are kept by the WISER consortium (Twitter & LinkedIn).
- Highlight **best practices (besides the WISER Full-Scale Pilots, FSPs, and Early Assessment Pilots, EAPs), relevant events,** as well as **career opportunities** through a dedicated Job Watch, which, besides interesting opportunities in the field, will also indicate potential sociological impact, e.g. eSkills, with advice also for employers on attracting and retaining specialised staff.

The social media channels will complement the media platform as a very effective means to attract relevant individuals, organisations, initiatives and associations (multipliers), thereby building a virtually connected community, leveraging partner networks and existing channels.

The main focus of the WISER social media channels is:

- Provide a channel for virtual engagement and dialogue, sharing of challenges and insights, news and events.
- Attract community members to WISER content and updates on the media platform.
- Build a virtually connected community, leveraging also WISER partner networks and with particular reference to the target markets identified.

1 Introduction

1.1 Purpose and Scope

The purpose of this document is to report on the WISER web presence, end-user engagement, including social media channel presence activation. In this context:

- ‘Web presence’ denotes the design and roll-out of the WISER media platform, evolving over the different phases of the project.
- ‘End-user engagement’ refers to actions conducted by WISER to promote the early assessment pilots (there are 10 EAPs), selected to field-test cutting-edge elements of the WISER risk management framework, and the full-scale pilots (there are 3 FSPs), selected to shape the innovative risk management framework, and develop a benchmarking support tool.

In this report, we detail the first roll-out of the Media Platform and describe plans for future developments as WISER prepares for market uptake. It also describes the activation of social media channels as one of the means for building the community and communicating WISER benefits.

Further updates on the media platform and social media channels will be provided in three iterations of the *Communication Plan* (D8.3), which are due in November 2015, May 2016, and November 2016 respectively.

1.2 Structure of the document

This document is structured as follows:

Section 1 presents the scope, purpose and structure of this document.

Section 2 outlines the WISER value proposition in terms of which problems and needs it seeks to tackle for different customer segments, explaining its core engagement activities. It also summarises the objectives of work package 8 (“Go to Market”) with particular reference to the media platform and social media networks.

Section 3 details the first roll-out of the media platform and social media channels. It includes examples of visibility and outreach, community building, information building, and the branding and design concept.

Section 4 focuses on the evolution of the media platform.

Section 5 offers a summary of key future actions serving mainly as a practical checklist.

2 WISER Objectives, Value Proposition and Engagement

2.1 Objectives related to Go-to-Market Targets

The main purpose of *Work Package 8 – Go to Market* is to help transform the innovation of WISER into tangible market uptake prospects. It is not a standalone activity but leverages the commitment, expertise and insights of all partners in communicating benefits, and pursuing the most promising actions for disseminating and exploiting WISER outputs.

Adopting a market-driven approach from the very outset, the key objectives are to:

- Develop a strong business case for WISER and widely communicate benefits across verticals, to firms of all sizes and, where relevant, to public sector organisations (including research institutes).

- Conduct market analysis on a regular basis, ensuring the WISER consortium is well-informed of trends and potential competitors.
- Design and implement business models based on concrete market opportunities identified. The consortium will build on its initial market analysis and facilitate partners in defining market-facing/novel exploitation plans.
- Provide tools to facilitate socio-economic impact assessment, including cost-benefits analysis, and to showcase best practices in cyber security, also in socio-economic terms.

The WISER media platform plays a key role in communicating the WISER value proposition to key customer segments and stakeholders. Designed as a dynamic web platform, it will stand out for its high-quality, highly relevant and practical content to inform and offer new services to increase resilience to cyber threats. The design and navigation of the website will evolve alongside the progress of the project, becoming increasingly market facing and service-oriented.

The social media channels will complement the media platform as a very effective means to attract relevant individuals, organisations, initiatives and associations (multipliers), thereby building a virtually connected community, leveraging partner networks and existing channels.

The main focus of the WISER media platform is:

- Facilitate an understanding of the cyber threat/vulnerabilities landscape through “essential guides” and a dedicated Market Watch.
- Highlight career opportunities through a dedicated Job Watch, which will also indicate potential sociological impact, e.g. eSkills.
- Offer a practical hands-on approach for potential customers of WISER services based on specific needs. A key related goal is driving WISER as a “trusted partner” when it comes to cyber security risk management.
- Be in-synch with the cyberwiser **social media** channels that are kept by the WISER consortium (Twitter & LinkedIn).
- Highlight **best practices (besides the WISER Full-Scale Pilots, FSPs, and Early Assessment Pilots, EAPs) and relevant events**

The main focus of the WISER social media channels is:

- Provide a multimedia channel for virtual engagement and dialogue, sharing of challenges and insights, news and events.
- Attract community members to WISER content and updates on the media platform.
- Build a virtually connected community, leveraging also WISER partner networks and with particular reference to the target markets identified. Selected members of this community will form specific groups around which WISER will conduct dissemination and exploitation of results.

The Market Watch and the Job Watch are two innovative components to be be integrated to support the “go-to-market” approach.

The Market Watch is an online resource that tracks the rapidly changing cyber security landscape.

It identifies the most recent sources of information from tech and security channels and surveys. The information collected is edited for the cyber wiser community and published in a dedicated area. Currently this information is published as a news item but the next phase of the media platform development will feature a dedicated section branded as Market Watch.

The fast-track data collection feeds into the baseline market study that the consortium conducted prior to the start of Wiser.

The Job Watch on the other hand, is a open tool designed to provide support for both job seekers as well as employers by facilitating information exchange through a one stop area on the website highlighting career opportunities as well as addressing key issues related to the cyber security and risk management job market trends, as part of the sociological impact monitoring and analysis complementary to the WP8 “go-to-market” approach.

2.2 The WISER Value Proposition and Customer Segments

WISER places cyber-risk management at the very centre of business practices and responds to well-identified market needs for effective cyber security solutions. It therefore has the potential to benefit multiple industries, particularly:

- **Critical infrastructure organisations** and **highly complex cyber systems** that require real-time and cross-system assessment of vulnerabilities and threats.

  This group includes organisations of varying sizes, from big corporations to small firms across different verticals that fit the definition above. This may include public organisations that serve private or public customers or deal with highly sensitive data, including possible access to financial/insurance data.

  With WISER, these organisations benefit from being able to anticipate, identify, and reduce threats by embedding cyber security risk management into their business processes and assessing direct and indirect impact.

- **Small- and Medium-sized Enterprises or Businesses** (SMEs or SMBs), which typically comprise a small team (e.g. 9 out of 10 SMEs are micros), with little or no leadership at relevant C-Level (e.g. Chief Technology Officer – CTO, Chief Information Officer – CIO, Chief Information Security Officer – CISO).

  WISER mainly targets ICT-intensive SMEs and tech firms across the European Union and across verticals. Even the most highly skilled of these firms are ill-prepared for the cyber threats they potentially face and many do not understand compliance regulations. WISER identifies the most vulnerable verticals through continuous market assessment and specific firms through regular community building activities.

  WISER increases awareness of the threat landscape and lowers the entry barrier to cyber security risk management. WISER enables small firms to improve their IT security posture by anticipating, identifying and reducing risks, thus significantly increasing resilience against vulnerabilities.

  Equally importantly, WISER will enable interested SMEs/SMBs to use their limited resources (financial and human) more effectively and without the need to invest heavily in IT expertise.

  Given the importance of SMEs to the European economy and digital single market, WISER has the potential to generate significant socio-economic impact by targeting this group.

Other groups targeted by WISER are:

- **Public sector organisations** with a focus on the most vulnerable ones identified through the WISER market analysis. WISER will increase awareness of cyber risks, help identify best practices and develop a roadmap for risk management implementation, and ultimately, measure the resulting socio-economic impact.
- **European and international initiatives**: WISER is part of the drive, in Europe and globally, to improve cyber security by sharing insights and best practices. These efforts are firmly rooted in policy and investments, both in Europe and worldwide, such as the European Strategy for Cyber Security, existing national cyber security strategies in

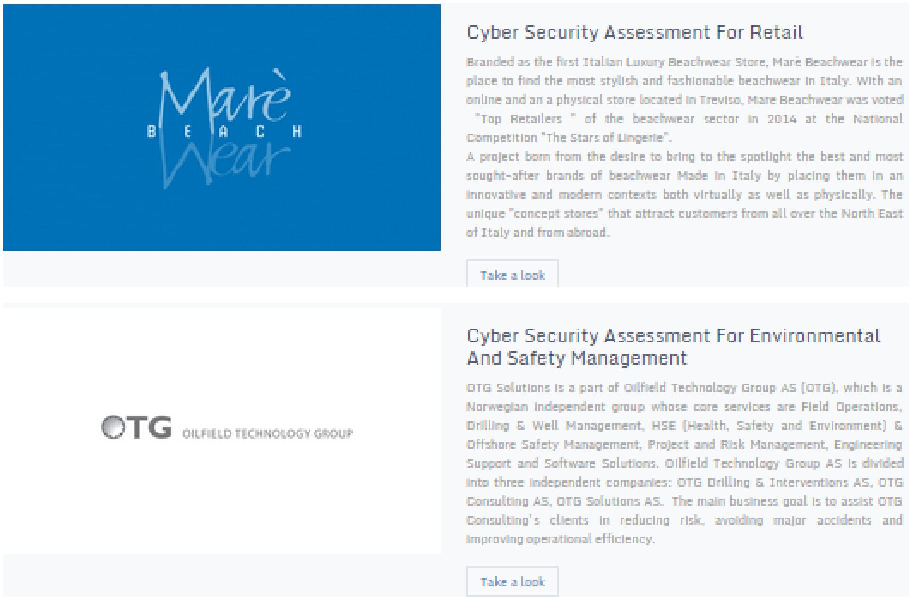
Europe and globally[1] and reference documents like the ENISA framework for evaluating cyber security strategies[2], and the NIST Cyber Security Framework[3].

Common benefits include greater awareness of the portfolio of services, tools and products emerging from investments and consensus on best practices, market conditions and policy perspectives, and tools to assess socio-economic impact.

Internet trust and security are vital to a vibrant digital society, as stated in the Digital Agenda for Europe[4]. WISER will contribute to this goal through its risk management framework and by establishing synergies with relevant initiatives. Such synergies will aim to increase overall awareness of cyber security and compliance with European Union legislation, such as the proposed Network and Information Security (NIS) and General Data Protection Regulation (GDPR). The NIS directive will impose new security and incident reporting requirements on a broader range of private sector companies. However, several studies show that many organisations in Europe are not prepared for the changes and are challenged by the cost and complexity of complying with the legislation[5][4].

2.2.1 Engagement with end-users: Early Assessment Pilots

WISER engages with selected early assessment pilots in order to field-test cutting edge elements of its framework. WISER targets 10 such pilots spanning different verticals, domains, and countries. Below is an illustration of how the Early Assessment Pilots are presented on the Cyberwiser.eu media platform:



Cyber Security Assessment For Retail

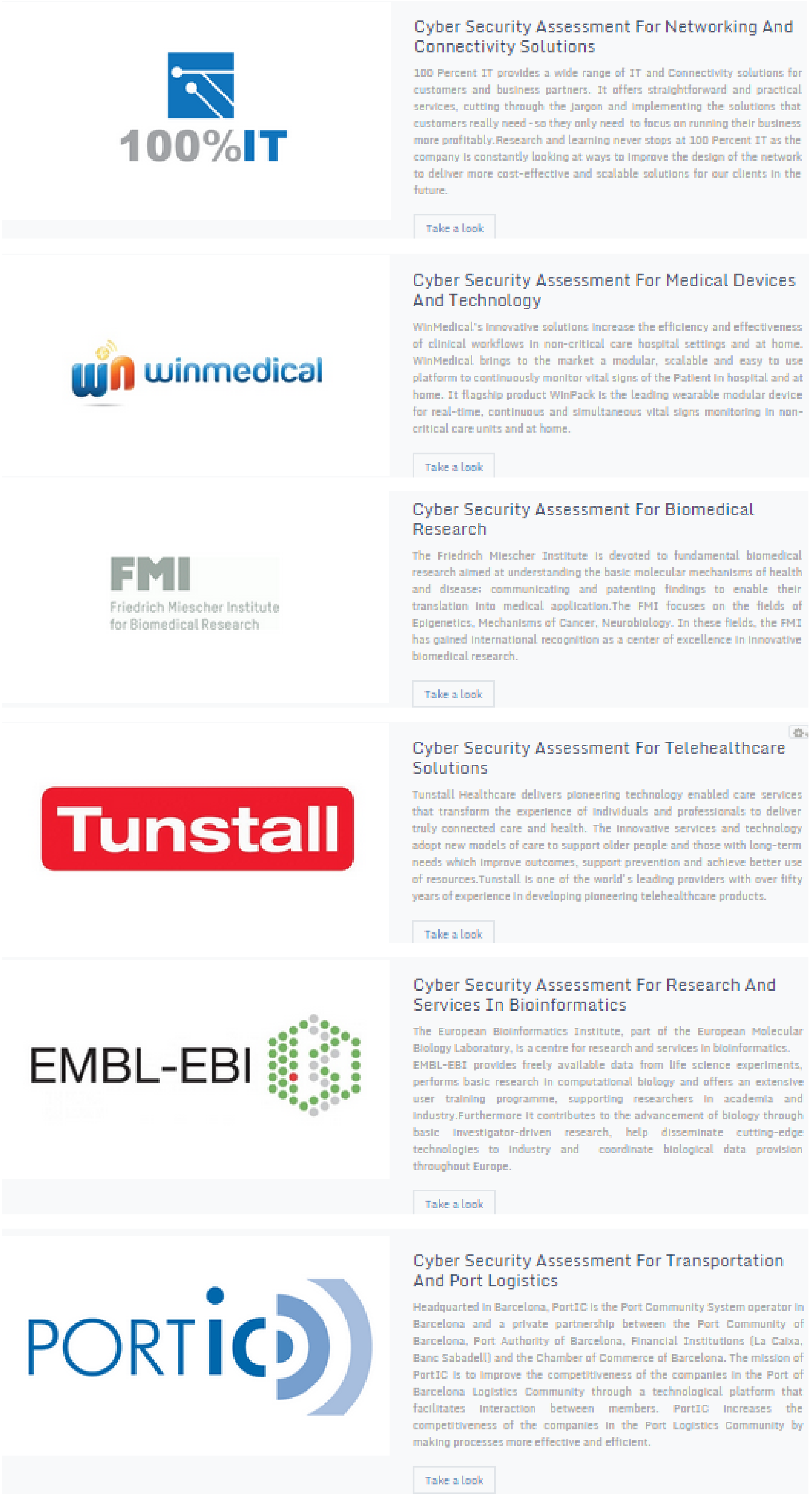
Branded as the first Italian Luxury Beachwear Store, Marè Beachwear is the place to find the most stylish and fashionable beachwear in Italy. With an online and an a physical store located in Treviso, Mare Beachwear was voted "Top Retailers " of the beachwear sector in 2014 at the National Competition "The Stars of Lingerie".

A project born from the desire to bring to the spotlight the best and most sought-after brands of beachwear Made in Italy by placing them in an innovative and modern contexts both virtually as well as physically. The unique "concept stores" that attract customers from all over the North East of Italy and from abroad.

Cyber Security Assessment For Environmental And Safety Management

OTG Solutions is a part of Oilfield Technology Group AS (OTG), which is a Norwegian independent group whose core services are Field Operations, Drilling & Well Management, HSE (Health, Safety and Environment) & Offshore Safety Management, Project and Risk Management, Engineering Support and Software Solutions. Oilfield Technology Group AS is divided into three independent companies: OTG Drilling & Interventions AS, OTG Consulting AS, OTG Solutions AS. The main business goal is to assist OTG Consulting's clients in reducing risk, avoiding major accidents and improving operational efficiency.

[1] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world
[2] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1
[3] http://www.nist.gov/cyberframework/
[4] https://ec.europa.eu/digital-agenda/en/cybersecurity.
[5] 'Latest EU Cyber Security Laws Leave Businesses Baffled', CWEurope, March 2015, http://www.computerweekly.com/ezine/CWEurope/CW-Europe-March-2015-Edition



Cyber Security Assessment For Networking And Connectivity Solutions

100 Percent IT provides a wide range of IT and Connectivity solutions for customers and business partners. It offers straightforward and practical services, cutting through the jargon and implementing the solutions that customers really need - so they only need to focus on running their business more profitably.Research and learning never stops at 100 Percent IT as the company is constantly looking at ways to improve the design of the network to deliver more cost-effective and scalable solutions for our clients in the future.

Cyber Security Assessment For Medical Devices And Technology

WinMedical's innovative solutions increase the efficiency and effectiveness of clinical workflows in non-critical care hospital settings and at home. WinMedical brings to the market a modular, scalable and easy to use platform to continuously monitor vital signs of the Patient in hospital and at home. It flagship product WinPack is the leading wearable modular device for real-time, continuous and simultaneous vital signs monitoring in non-critical care units and at home.

Cyber Security Assessment For Biomedical Research

The Friedrich Miescher Institute is devoted to fundamental biomedical research aimed at understanding the basic molecular mechanisms of health and disease; communicating and patenting findings to enable their translation into medical application.The FMI focuses on the fields of Epigenetics, Mechanisms of Cancer, Neurobiology. In these fields, the FMI has gained international recognition as a center of excellence in innovative biomedical research.

Cyber Security Assessment For Telehealthcare Solutions

Tunstall Healthcare delivers pioneering technology enabled care services that transform the experience of individuals and professionals to deliver truly connected care and health. The innovative services and technology adopt new models of care to support older people and those with long-term needs which improve outcomes, support prevention and achieve better use of resources.Tunstall is one of the world's leading providers with over fifty years of experience in developing pioneering telehealthcare products.

Cyber Security Assessment For Research And Services In Bioinformatics

The European Bioinformatics Institute, part of the European Molecular Biology Laboratory, is a centre for research and services in bioinformatics.
EMBL-EBI provides freely available data from life science experiments, performs basic research in computational biology and offers an extensive user training programme, supporting researchers in academia and industry.Furthermore it contributes to the advancement of biology through basic investigator-driven research, help disseminate cutting-edge technologies to industry and coordinate biological data provision throughout Europe.

Cyber Security Assessment For Transportation And Port Logistics

Headquarted in Barcelona, PortIC is the Port Community System operator in Barcelona and a private partnership between the Port Community of Barcelona, Port Authority of Barcelona, Financial Institutions (La Caixa, Banc Sabadell) and the Chamber of Commerce of Barcelona. The mission of PortIC is to improve the competitiveness of the companies in the Port of Barcelona Logistics Community through a technological platform that facilitates interaction between members. PortIC increases the competitiveness of the companies in the Port Logistics Community by making processes more effective and efficient.

Cyber Security Assessment For Cloud Computing Software Development

Koofr d.o.o. is a young start-up company, founded in 2013 engaged in software development for cloud computing. Their application Koofr enables online storage for private and business data.The company also offers software solution for domestic and foreign Internet service providers. Only a year after establishing the company, Koofr has already built up a reputation of a complete software solution provider for Cloud storage targeted at Internet service providers in the European area.

Figure 1 - Illustration of the Early Assessment Pilots on cyberwiser.eu

Risk management approaches will be tested among these organizations based on defined cyber security scenarios. Each organisation will be benchmarked against a set of metrics such as risk mitigation effectiveness, residual risk, and cost-benefits.

The early assessment pilots are showcased through the media platform with updates coming from direct interaction and collaboration. The social media channels are used to raise awareness and help build a virtual community specifically targeting organisations facing similar challenges over time.

2.2.2 Engagement with end users: Full-scale Pilots

WISER carries out three full-scale pilots from the private sector managing critical infrastructures, enabling them to anticipate threats and comply with new European Union regulations for reporting serious attacks. Each of the 3 pilots targets the private sector.

- **Financial Services & Insurance**: AON plc, UK[6]. Leading global provider of risk management, insurance and reinsurance brokerage, and human resources solutions and outsourcing services.

  Pilot: **cyber secure assessment processes of financial institutions**. The pilot focuses on finding countermeasures for a subtle and hard-to-track form of frauds, such as the leakage of confidential information in assessment processes, especially in remote. WISER will offer near real-time risk assessment to quickly identify risk factors and drastically reduce events with high impact on businesses.

- **Energy Management and distribution**: REXEL, France[7]. Part of a group specialising in the distribution of electrical supplies to professional users, e.g. automation, technical supply and energy management.

  Pilot: **global energy solutions procurement**. The pilot focuses on testing the effectiveness of the WISER approach when applied to the procurement of energy products, especially risks from a global supply network configuration. Events are both low and high impact. The pilot will validate WISER real-time platform capabilities end-to-end for the entire service value chain.

- **Energy Management and distribution**: DOMOTECNICA, Italy. An SME that markets smart meters to both businesses and households.

  Pilot: cyber secure, innovative smart energy meters solution. The pilot focuses on testing the effectiveness of the WISER approach applied to energy distribution, with the testing of an innovative solution of energy consumption/production monitoring. It will assess the adaptability and scalability of WISER signalling and real-time monitoring to cope with highly distributed and dynamic infrastructures and their capability to process and analyse massive amounts of data that needs to be cyber secure.

[6] http://www.aon.com/.
[7] http://www.rexel.com/en/.

3 First Roll-out of WISER Media Platform & Social Media Channels

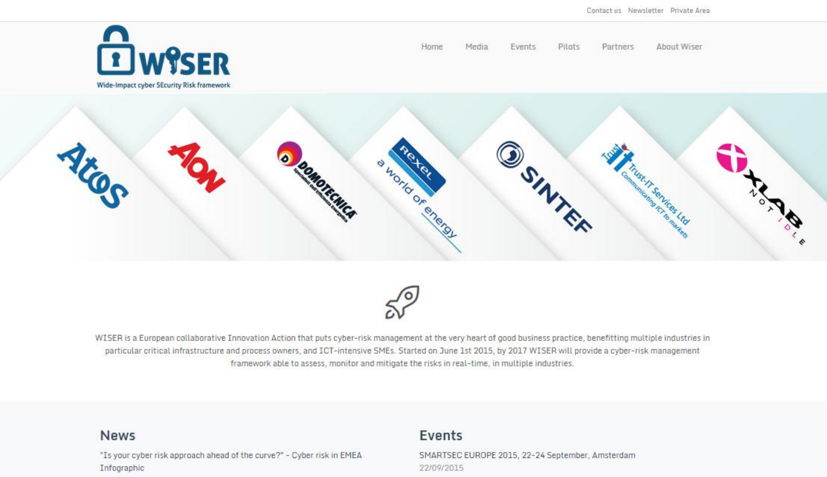
The term “community” has been at the heart of the Internet since very early on, when mainly scientists and students used it to share data, collaborate on research, and communicate. Although the Internet usage trends are impressive, and businesses have not only picked up but are now in the driving seat, it is also very clear that simply putting up a website does not necessarily mean that the entity which has invested in that website is granted an audience.

For this purpose building a website needs to be closely tied to a communication and dissemination strategy. The strategy envisioned for WISER is based on a service oriented approach to communication and community building.

3.1 Visibility & Outreach

Awareness raising activities for WISER target stakeholders & general public on the WISER mission, vision, upcoming services and main results and promotion of events & synergies built with relevant initiatives, including liaison with the CSP Forum as the reference Coordination and Support Action.

In its first release, the website homepage was designed as a gateway to all dedicated web sections including News, Events, highlight of the WISER vision and partners.



WISER is a European collaborative Innovation Action that puts cyber-risk management at the very heart of good business practice, benefitting multiple industries in particular critical infrastructure and process owners, and ICT-intensive SMEs. Started on June 1st 2015, by 2017 WISER will provide a cyber-risk management framework able to assess, monitor and mitigate the risks in real-time, in multiple industries.

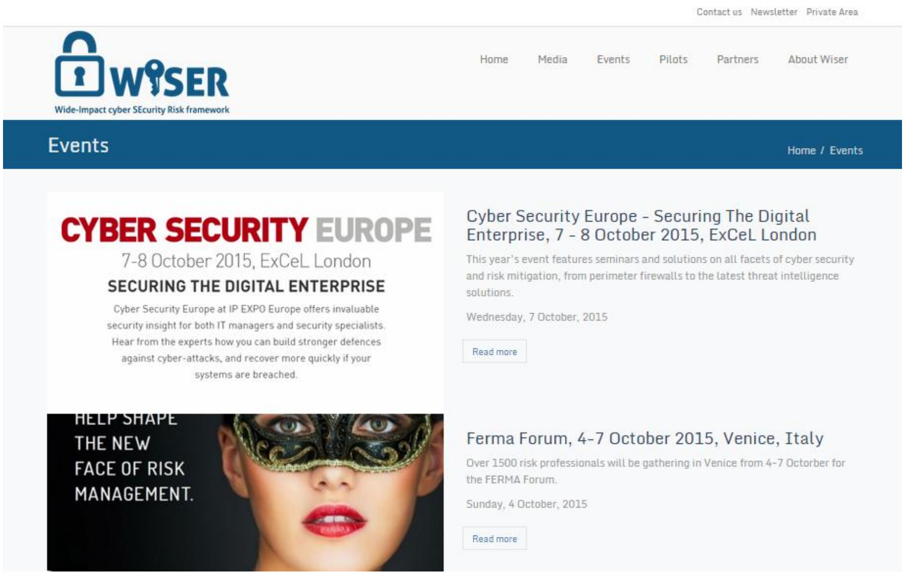
News

"Is your cyber risk approach ahead of the curve?" - Cyber risk in EMEA Infographic

Events

SMARTSEC EUROPE 2015, 22-24 September, Amsterdam
22/09/2015

Figure 2 Cyberwiser.eu homepage sample highlighting the project vision and partners



CYBER SECURITY EUROPE

7-8 October 2015, ExCeL London

SECURING THE DIGITAL ENTERPRISE

Cyber Security Europe at IP EXPO Europe offers invaluable security insight for both IT managers and security specialists. Hear from the experts how you can build stronger defences against cyber-attacks, and recover more quickly if your systems are breached.

Cyber Security Europe - Securing The Digital Enterprise, 7 - 8 October 2015, ExCeL London

This year's event features seminars and solutions on all facets of cyber security and risk mitigation, from perimeter firewalls to the latest threat intelligence solutions.

Wednesday, 7 October, 2015

Ferma Forum, 4-7 October 2015, Venice, Italy

Over 1500 risk professionals will be gathering in Venice from 4-7 Octorber for the FERMA Forum.

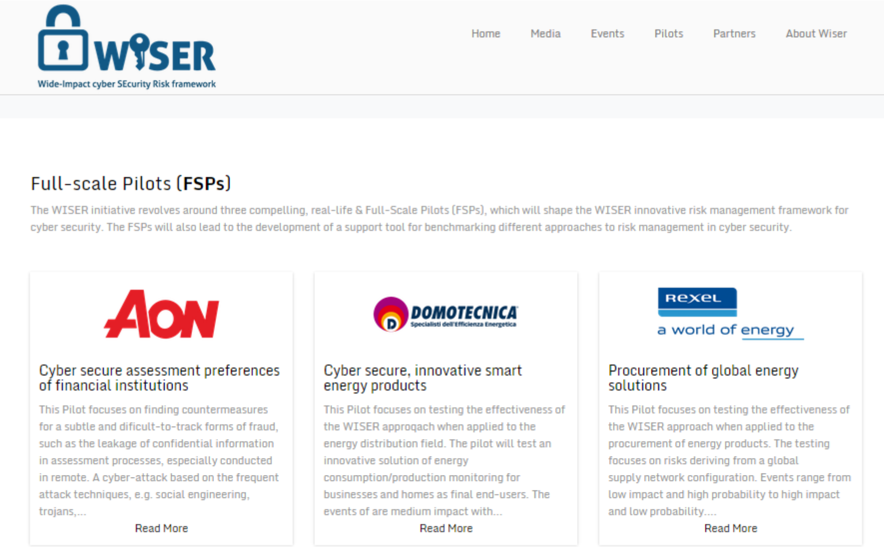
Sunday, 4 October, 2015

Figure 3 Sample of the Events dedicated web section

3.2 Community building and engagement

Identifying key target stakeholders and engagement in WISER activities and events particularly focusing on the engagement of Early Assessment Pilots and Full Scale Pilots as well as an extended pool of potential end-users

The WISER EAPs and FSPs are fundamental for the project concept and approach as the pilot activities will first support the definition of the WISER framework and later the validation of the resulting outputs.
The importance of these activities is emphasized on the homepage as well as the navigation structure through quick access areas and dedicated menus.



Full-scale Pilots (**FSPs**)

The WISER initiative revolves around three compelling, real-life & Full-Scale Pilots (FSPs), which will shape the WISER innovative risk management framework for cyber security. The FSPs will also lead to the development of a support tool for benchmarking different approaches to risk management in cyber security.

Cyber secure assessment preferences of financial institutions

This Pilot focuses on finding countermeasures for a subtle and dificult-to-track forms of fraud, such as the leakage of confidential information in assessment processes, especially conducted in remote. A cyber-attack based on the frequent attack techniques, e.g. social engineering, trojans,...

Cyber secure, innovative smart energy products

This Pilot focuses on testing the effectiveness of the WISER approqach when applied to the energy distribution field. The pilot will test an innovative solution of energy consumption/production monitoring for businesses and homes as final end-users. The events of are medium impact with...

Procurement of global energy solutions

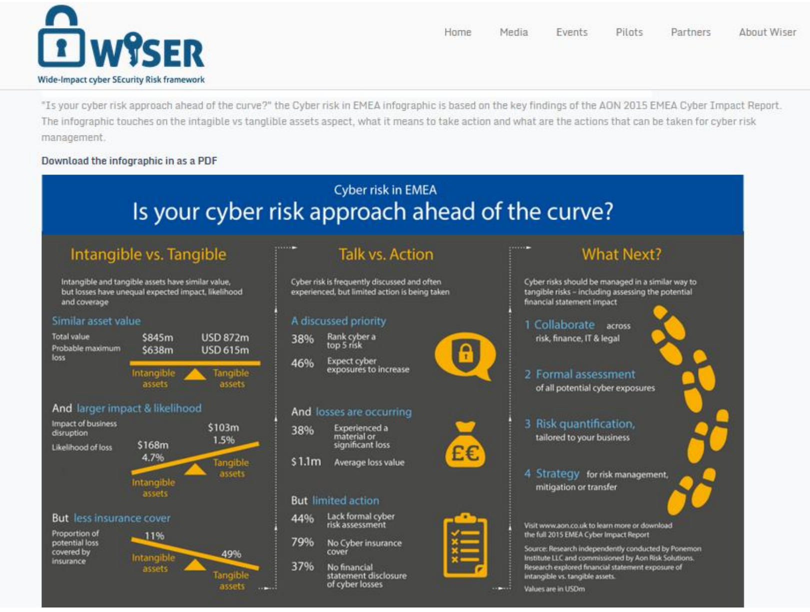
This Pilot focuses on testing the effectiveness of the WISER approach when applied to the procurement of energy products. The testing focuses on risks deriving from a global supply network configuration. Events range from low impact and high probability to high impact and low probability....

Figure 4 Homepage sample of WISER Full-Scale Pilots spotlight

3.3 Information provisioning

Timely communication of practical information serving a two-fold goal: facilitating an understanding of the cyber threat/vulnerabilities landscape (e.g. "essential guides"; dedicated Market Watch) and showing what vulnerabilities WISER services and tools address for each target group with a focus on benefits gained.

The Cyberwiser.eu website will stand out through its high–quality, highly relevant and practical content delivered in an interactive and engaging manner:



"Is your cyber risk approach ahead of the curve?" the Cyber risk in EMEA infographic is based on the key findings of the AON 2015 EMEA Cyber Impact Report. The infographic touches on the intagible vs tanglible assets aspect, what it means to take action and what are the actions that can be taken for cyber risk management.

Download the infographic in as a PDF

Cyber risk in EMEA

Is your cyber risk approach ahead of the curve?

Intangible vs. Tangible

Intangible and tangible assets have similar value, but losses have unequal expected impact, likelihood and coverage

Similar asset value

	Intangible assets	Tangible assets
Total value	$845m	USD 872m
Probable maximum loss	$638m	USD 615m

And larger impact & likelihood

	Intangible assets	Tangible assets
Impact of business disruption	$168m	$103m
Likelihood of loss	4.7%	1.5%

But less insurance cover

	Intangible assets	Tangible assets
Proportion of potential loss covered by insurance	11%	49%

Talk vs. Action

Cyber risk is frequently discussed and often experienced, but limited action is being taken

A discussed priority

38% Rank cyber a top 5 risk

46% Expect cyber exposures to increase

And losses are occurring

38% Experienced a material or significant loss

$1.1m Average loss value

But limited action

44% Lack formal cyber risk assessment

79% No Cyber insurance cover

37% No financial statement disclosure of cyber losses

What Next?

Cyber risks should be managed in a similar way to tangible risks – including assessing the potential financial statement impact

1 Collaborate across risk, finance, IT & legal

2 Formal assessment of all potential cyber exposures

3 Risk quantification, tailored to your business

4 Strategy for risk management, mitigation or transfer

Visit www.aon.co.uk to learn more or download the full 2015 EMEA Cyber Impact Report

Source: Research independently conducted by Ponemon Institute LLC and commissioned by Aon Risk Solutions. Research explored financial statement exposure of intangible vs. tangible assets.

Values are in USDm

Figure 5 Sample of the "Cyber risk in EMEA" infographic published on the cyberwiser.eu website

Hot off the press updates and in-depth analysis as well as hand-on practical guidance are provided in a variety of formats written articles, detailed graphics and videos to make sure the right information is readily available and easy to grasp.

3.4 Branding and Design Concept

The project branding is aimed at ensuring a distinctive look and feel across a broad set of communication tools. The WISER logo highlights two concepts that are fundamental to the project vision: the padlock that is a symbol for security and the key that relates to the concept of a provided solution.

The logo symbolism is further stressed by the accompanying project payoff "Wide-Impact cyber Security Risk framework".

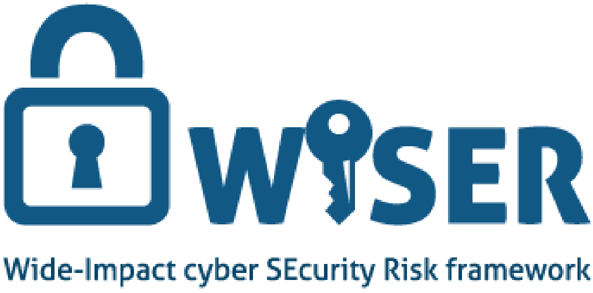


Figure 6 WISER logo and pay-off

The logo and colour branding has been replicated on the website and has also used to produce different templates including project documents and will also be used in all project dissemination tools, materials (poster, flyers, booklets etc.), other web graphics and the newsletter layout.

To improve search engine results and support awareness, the toponym “**cyberwiser**” has been adopted and will be leveraged as a keyword throughout the project. The #cyberwiser account name has been created for twitter and linkedIn, and the www.cyberwiser.eu is the official URL of WISER.

3.5 Terms of use

Based on the current platform structure appropriate Privacy Policy & Terms of Use are documented and available on the website, encompassing a section on “Website content” and one on “External Links and Document”. As the service offer will extended the policies and practices will be updated and properly documented, articulating benefits as well as responsibilities of the subjects and entities involved. Finally, a section on “Security” of the website will be added, reflecting as much as possible the WISER’s credo.

4 Evolution of the Media Platform

Enhanced versions of the platform will be progressively released to accommodate for advanced features and tools, as they will be delivered by the Project, for the various stakeholders.

In the subsequent releases the WISER Media Platform will be especially enriched in the following directions, with a service-delivery focus:

- ➢ Build a risk assessment framework that operates in real time, providing an updated view on the risk level that a given ICT system poses.
- ➢ Provide real-time cyber risk monitoring tools that give access to real-time information necessary for decision makers to manage risk.
- ➢ Provide decision support tools to facilitate selection of mitigation options based on risk impact and different levels.

Specifically, the web platform will be configured as a service platform providing a full set of tools for self assessment as well as decision support. In particular the 3 “service delivery operating models” of WISER (viz. “Non-intrusive”, “Basic” and “Advanced”, see Deliverable D2.10) will all be supported, at different levels of engagement with the related end-users & stakeholders, by the cyberwiser.eu media platform. This fact will be reflected in the future, progressive releases of the platform anticipated above.

By all means, the WISER Media Platform will provide a user-friendly interface for the complete set of tools and services, addressing the needs of all WISER stakeholders.

Cyberwiser.eu will be the gateway to reach the area of tools and services that will be developed during the project, ensuring access to users already registered on the media and Platform and services possibly through a single sign-on solution. Particular attention will be paid to the security measures related to access and data exchange protocols, authentication system as well as firewalls and back-up systems.

Ultimately, cyberwiser.eu will help strengthen WISER's commitment to offer a practical hands-on approach for potential customers and in consolidating itself as a "trusted partner" when it comes to cyber security risk management.

5 Summary of Future Actions

WISER website cyberwiser.eu, will be an interactive meeting point and a key element, during the lifecycle of the project and beyond to raise awareness around cybersecurity and to gather interest and develop opportunities for potential customers in this field. WISER, through its media platform, aims to progressively consolidate itself as a "trusted partner" when it comes to cyber security risk management.

The media platform will undergo, during the entire project duration (i.e. up to project completion in November 2017) 2 types of evolutions:

- Continuous content update (through the CMS): this will essentially be a daily activity. Content will also include the public WISER deliverables, which will be downloadable from the web platform;
- Progressive publication of new functionalities/access to services: this will be an activity with a coarser progression timeline (e.g. monthly or two-monthly);
- Continuous update of the "Terms of use" section

Among the major platform evolutions to be envisaged in the "services" direction, are the following ones:

- Project public repository.
- Online surveys.
- Online self-assessments.
- Risk framework.

The present document will be periodically be updated to report about inclusion of the aforementioned services/functionalities on the cyberwiser.eu platform.

6 References

[1] ENISA and Cyber Security Strategies: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss

[2] NIST Cybersecurity Framework: http://www.nist.gov/cyberframework/

[3] European Commission's Digital Agenda for Europe - Cybersecurity: https://ec.europa.eu/digital-agenda/en/cybersecurity

[4] 'Latest EU Cyber Security Laws Leave Businesses Baffled', CWEurope, March 2015, http://www.computerweekly.com/ezine/CWEurope/CW-Europe-March-2015-Edition

[5] Deliverable D2.1: Requirements, WISER consortium, confidential report of, Aug. 2015