



D3.2 European cybersecurity and privacy Research & Innovation Ecosystem

Author(s)	Mark Miller
Status	Review/Approval/Final
Version	V2.7
Date	31/05/2018

Dissemination Level

<input checked="" type="checkbox"/>	PU: Public
<input type="checkbox"/>	PP: Restricted to other programme participants (including the Commission)
<input type="checkbox"/>	RE: Restricted to a group specified by the consortium (including the Commission)
<input type="checkbox"/>	CO: Confidential, only for members of the consortium (including the Commission)

Abstract:



The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

Document identifier: Cyberwatching.eu – WP – D3.2	
Deliverable lead	CPT
Related work package	WP3
Author(s)	Mark Miller
Contributor(s)	CPT, Trust-IT Services, AON, ICTLegal, AEI
Due date	30/04/2018
Actual submission date	31/05/2018
Reviewed by	Trust-IT Services, UOXF
Approved by	
Start date of Project	01/05/2017
Duration	48 months

Revision history

Version	Date	Authors	Notes
0.1	14.02.2018	M. Miller/V. Menezes Miller (CPT)	TOC & sections assignment
0.2	19.02.2018	M. Miller/V. Menezes Miller (CPT)	Revisions
1	19.02.2018	M. Miller/V. Menezes Miller (CPT)	Revisions
1.1	02.03.2018	J. Tobal (AEI)	Contributions to section 4.1
1.2	02.03.2018	F. Manca (AON)	Contributions to sections 3.1, 3.2, 3.3
1.3	12.03.2018	M. Miller/V. Menezes Miller	Revisions
1.4	13.03.2018	F. Manca (AON)	Contributions to sections 3.4.1, 3.4.2, 3.5.1
1.5	13.03.2018	L. Senatore (ICT-Legal)	Contribution to section 2.2 and inputs to section 2.3.3
2	26.03.2018	M. Miller/V. Menezes Miller (CPT)	Revisions
2.1	26.03.2018	M. Miller/V. Menezes Miller (CPT)	Concertation Event addition
2.2	27.04.2018	M. Miller/V. Menezes Miller (CPT)	Concertation Event addition
2.3	04.05.2018	M. Miller/V. Menezes Miller (CPT)	Revisions overall
2.4	09.05.2018	Nick Ferguson, Niccolò Zazzeri (Trust-IT Services)	Contributions to section 2.6
2.5	18.05.2018	Nick Ferguson, Niccolò Zazzeri (Trust-IT Services)	Contributions to section 3.5, 3.6
2.6	23.05.2018	Nick Ferguson, Niccolò Zazzeri (Trust-IT Services)	Contributions to section 6.1 and inputs to section 6.2
2.7	31.05.2018	Nick Ferguson, Niccolò Zazzeri (Trust-IT Services)	Review of the

			document
2.8	31.05.2018	V. Menezes Miller (CPT)	Revisions to Concertation Event
2.9	31.05.2018	David Wallom, Michel Drescher (UOXF)	Review of the document
3.0	31.05.2018	Nick Ferguson, Niccolò Zazzeri (Trust-IT Services)	Final version ready for submission

Executive Summary

This document presents a view of the European cyber security and privacy research and innovation ecosystem with a view of getting input and feedback via a survey and the concertation meeting held on 26 April 2018 in Brussels.

A key component of developing this deliverable was to target research projects in the field of cyber security in the current cyber security framework. To this aim, a survey was sent out to projects in cyber security in the EU. All the projects were also invited to the First Concertation Meeting, which was held on 26 April 2018 in Brussels. Feedback from that first Concertation meeting is included in this deliverable.

The conclusions drawn demonstrate that there is a clear value in getting the European cyber security and privacy research and innovation ecosystems together in order to jointly discuss developments, findings, best practices and future directions. The Cyberwatching.eu Concertation Meeting has thus become a key forum for this exchange and we look forward to the next step in this process.

Table of Contents

1	Section 1 – Introduction	7
2	EU Cybersecurity Governance	7
2.1	NIS Directive	7
2.1.1	Brief introduction	7
2.1.2	First objective: improve national cybersecurity capabilities	8
2.1.3	Second objective: building cooperation	8
2.1.4	Third objective: cybersecurity risk management in key economic sectors	8
2.2	General Data Protection Regulation (GDPR)	9
2.2.1	Brief Introduction	9
2.2.2	Compliance and Principle of Accountability	9
2.2.3	Transparency	10
2.2.4	Where the NIS Directive meets the GDPR	10
2.3	EU Cybersecurity package	10
2.3.1	ENISA	11
2.3.2	Cybersecurity certification of ICT products and services	11
2.3.3	NIS directive, GDPR and Cybersecurity Act	11
2.4	European Cyber Security Organisation (ECISO)	12
2.5	National initiatives in Member States	12
2.6	How Research and Innovation is addressing governance needs	12
2.7	GDPR & Certification: Considerations from the Concertation meeting	17
3	Risk Management	18
3.1	Overview	18
3.2	Enterprise Risk Management Context	20
3.3	A cyber security risk management process	22
3.4	Risk Analysis	23
3.4.1	Relationship between residual risk and risk acceptance	25
3.4.2	Residual risk management	25
3.5	Addressing risk management needs using behavioural analysis	26
3.5.1	Risk sharing/insurance: Cyber Insurance	28
3.6	Addressing risk management needs through financial instruments (insurance)	30
3.7	Standards Overview in Risk management	31
3.8	A skilled workforce is essential – Considerations from the Concertation Meeting	32
3.9	An SME perspective on cybersecurity - Considerations from the Concertation Meeting	33
4	Standards and Certification Framework	33
4.1	Case Study: Cybersecurity certification in Spain by AEI	34
4.1.1	Background	34
4.1.2	Associated Evaluation Scheme and Governance	35
4.1.3	Process	35
4.1.4	Practice	35
4.1.5	Formal Status	35
5	Analysis of the Policy, Legal and standard framework	36
5.1	External Online Survey	36
5.1.1	Focus of the survey	36

5.1.2	Identification of stakeholders	36
5.1.3	Dissemination of the survey	37
5.1.4	Analysis of Response to the Online Survey.....	37
6	Research & Innovation	49
6.1	Clustering R&I projects	49
6.1.1	Applications and user-oriented services	50
6.1.2	Foundational technical methods and risk management for trustworthy systems 51	
6.1.3	Policy, governance, ethics, human aspects, trust and usability	52
6.2	Snapshot of the First cyberwatching.eu Concertation meeting	53
6.2.1	Objectives	54
6.2.2	Participants	54
6.2.3	Overall Feedback	55
7	Conclusions	55
Annex A.	ECISO “SOTA” – STATE-OF-THE-ART SYLLABUS (DECEMBER 2017)	56
Annex B.	ONLINE SURVEY - CYBER SECURITY POLICY AND REGULATORY FRAMEWORK.....	57
Annex C.	1ST CONCERTATION MEETING AGENDA	60
Annex D.	LIST OF PROJECTS AT THE 1ST CONCERTATION MEETING	63
Annex E.	LIST OF PARTICIPANTS AT THE 1ST CONCERTATION MEETING	68

GLOSSARY 71

LIST OF FIGURES

Figure 1: The Global Risks Landscape 2018 - World Economic Forum.....	19
Figure 2: Evolved approach to cyber risk management	22
Figure 3 Risk Assessment Matrix	24
Figure 4: Upcoming areas of concern in cyber security	41
Figure 5: Response highlighting concerns regarding cyber security	42
Figure 6: Where end users feel focus should be placed in regulator efforts in cybersecurity	43
Figure 7: User feedback on how harmonization can be achieved.....	45
Figure 8: User feedback on what role of certification in implementing policy and regulatory requirements	47
Figure 9: List of projects in Breakout Session 1	50
Figure 10: List of projects in Breakout Session 2.....	51
Figure 11: List of projects in Breakout Session 2.....	53

LIST OF TABLES

Table 1: Examples from the Online survey of regulations cited as relevant	39
---	----

1 Section 1 – Introduction

Cyberwatching.eu represents an opportunity to enable the European cyber security and privacy research and innovation ecosystem to exchange information and to learn from one another, ensuring that the concepts and conclusions do not become constant reinventions of the same developments. A close relationship with the European Cyber Security Organisation (ECSO) also facilitates the clear placement of the basic building blocks at the core of the efforts of cyberwatching.eu, while at the same time a certain synergy allows the results of both organization to be much greater.

Within this deliverable we have not only done certain basic analysis, building upon what is already existing, but we have also taken the opportunity to use a direct survey to get input and feedback as well, in addition to the Concertation event which is detailed herein. Indeed, the information gathered at the event from 48 CS&P projects has given us a vital window on how R&I is responding to the needs identified in the ecosystem. Throughout the document we will give examples of projects that are addressing needs in areas relating to governance such as the NIS directive, GDPR and certification; and market needs such as risk management and cyber insurance.

The first level conclusion is that we can make a difference by getting the best of the cybersecurity projects together in order to present and discuss their findings and developments on a regular basis.

2 EU Cybersecurity Governance

The EU Cybersecurity Ecosystem is governed by three key legislative/regulatory components consisting of the following:

- NIS Directive
- General Data Protection Regulation (GDPR)
- Cybersecurity Package

Within this deliverable we summarize the key and most relevant elements of these components, while at the same time we look at the practical aspects and analyse the current situation.

2.1 NIS Directive

2.1.1 Brief introduction

The first EU-wide source of legislation that was dedicated directly to the challenges of Cybersecurity is the Directive concerning measures for a high common level of security of network and information systems across the Union, commonly referred to as the “[NIS Directive](#)”. It was adopted in July 2016 and entered into force in August 2016. The EU Member States were given around two years to transpose the NIS Directive into their national laws, thus setting its implementation for **9 May 2018**. The Commission presented an additional and extensive deadline of November 2018, in order for the Member States to identify their country’s Operators of Essential Services. The Operators of Essential Services is a core term of the NIS Directive,

bringing upon higher standards of security of network and information systems. In view of these approaching deadlines, the Commission adopted a Communication on 13 September 2017, which they called the “NIS Tool Kit”, in order to aid the Member States’ efforts in implementing the NIS Directive in a timely and coherent manner across the EU (see Section 2.3). In this proceeding Communication, a more practical approach is offered to the Member States and the relevant organisations affected by presenting best practices from more advanced Member States as well as providing interpretations of provisions in terms of their feasibility.

The NIS Directive will be explained through its three main objectives. All three are stand at the cornerstone of the Directive in achieving a more secure Cyberspace and reaching a minimum level of harmonization within the 28 Member States.

2.1.2 First objective: improve national cybersecurity capabilities

The first priority of the NIS Directive is an overall improvement of national cybersecurity capabilities. More concretely, Member States will have to equip both public as well as private entities appropriately by having national Computer Security Incident Reponse Teams (CSIRTs). These teams would be responsible for handling risks and incidents of specific sectors, once identified as Operators of Essential Services according to Annex II of the Directive; including energy, transport, banking, health and more. The idea behind having CSIRTs dedicated to core sectors of a nation is that cybersecurity attacks could no longer cripple a country, or bring its citizens in a vulnerable position. Together with this, comes the implementation of a competent national NIS Authority. These Authorities would monitor the application of the NIS Directive, but also be part of a Cooperation Group (a group composed of representatives of the Member States, the Commission and ENISA) who will be the country’s person of contact in specific cases, such as those of incidents, or exchanging information. An example of the inter-connection between the competent Authorities and the CSIRTs would be once an incident occurred and the CSIRTs have identified a way to operate in order to issue early warnings of the incident. In this case, the CSIRTs would inform the competent Authority in order to pass this information onto the Member State level as well as to other competent Authorities that could potentially be influenced.

2.1.3 Second objective: building cooperation

To complete the first goal further, comes the second objective of the NIS Directive, which is to build cooperation at the EU level. Specifically, a CSIRTs network will be established; including every national response team as well as the Computer Emergency Response Team (CERT-EU) with the Commission as an observer. Notably, the CSIRTs network will be tasked with exploring principles and modalities for coordination to respond to cross-border risks and incidents. This action is needed, to ensure that no Member State is left alone in its efforts to achieve cybersecurity.

2.1.4 Third objective: cybersecurity risk management in key economic sectors

The third objective of the NIS Directive is to promote a culture of risk management and incident reporting among the key economic sectors; operators providing essential services (OES), such as energy, transport, banking. This is centered around the fact that without those OES the economic and societal activities cannot be maintained, thus protecting and preparing these sectors for cybersecurity risks is vital. Additionally, this Directive puts requirements on the Digital Service Providers (DSPs), such as search engines, cloud computing services and online markets, to

improve together with the technological market they belong to but also to comply with the risk management principles and techniques that have applied also to the OES.

2.2 General Data Protection Regulation (GDPR)

Web site: <https://www.eugdpr.org/>

2.2.1 Brief Introduction

The Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, better known as “[General Data Protection Regulation](#)” (GDPR) was voted by the EU Parliament on 14 April 2016, in force on 27 April 2016 and will be directly applicable in all Member States from **25 May 2018**. The GDPR is not the first European legislation on Data Protection, in reality it replaces and renews the Data Protection Directive 95/46/EC. Its goal is to further harmonise data privacy laws across Europe, by gathering the most highly respected standards or principles around the world and applying them to protect EU citizens’ data privacy.

The special element of GDPR is its extraterritorial scope. In fact, from 25th of May 2018, the GDPR will be effective in all 28 Member States of the European Union and applicable to all legal entities who:

- process personal data (e.g., name, surname, e-mail address, phone number, location, IP address) in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether or not the processing takes place in the European Union;
- offer goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the European Union.
- monitor the behaviour of data subjects as far as their behaviour takes place within the European Union.

Hence, this means that the GDPR may apply also to organizations that do not have an establishment in the European Union.

Non-compliance with the GDPR can result in heavy fines; such as in cases of infringements of basic principles for processing personal data, fines of 20 million EUR or 4% of worldwide annual turnover (whichever is higher).

The GDPR focuses on two main objectives, which are improved and clarified in comparison to Directive 95/46, increasing the level of compliance around Europe and strengthening the principle of transparency in the field of data privacy.

2.2.2 Compliance and Principle of Accountability

In the GDPR, there are constant references that eventually create a full compliance framework that must be created by organisations, depending on their activities and type of provision of services. The principle of accountability demands organisations not only to be compliant with the GDPR, but also to be able to demonstrate it. This principle requires organisations to document and record all their efforts to comply with data protection legislation.

2.2.3 Transparency

This is a concept that has not changed from Directive 95/46 but it has been further emphasized throughout the whole GDPR. The principle of transparency obliges organisations to be transparent about the purposes for which they process personal data, the means with which they collect this data, the period of storage of this data, and the recipients of this data. On top of this, when consent is the legal basis for processing, everything just mentioned must be communicated clearly and unambiguously to the data subjects and organisations must have proof of when this consent was received, when this consent was received pursuant to the principle of accountability mentioned above. Hence, in order to be able to follow through with the principle of transparency, a company must have great visibility of their data flows, and be able to show this to the outside world (both to customers, suppliers, and if needed to Supervisory Authorities).

2.2.4 Where the NIS Directive meets the GDPR

While the NIS Directive's scope is more generally the national critical infrastructure of Member States and specifically focusing on its main economic sectors, the GDPR is a legislation centered more around data subjects themselves and the relevant actors in processing activities. The NIS Directive covers general grounds and obligations that countries must apply in their national infrastructure, in order to ensure that all European Member States are approximately on the same page in terms of their capabilities to act in cases of cybersecurity attacks. Meanwhile, the GDPR covers the more specific principles and obligations related to personal data security and to protection of people's privacy. The two EU legislations work together to cover the gaps between Member States but to also ensure that national laws have a solid basis to protect both key economic actors as well as their citizens; since both legislations compile principles and best practices based on what is seen around the world. Furthermore, the GDPR and the NIS Directive are based on the concept of risk management, and for this reason they harmonise the most major issues while leaving to the discretion of the Member States the matters that are close to problems of national security.

2.3 EU Cybersecurity package

On 13 September 2017, The European Commission together with the High Representative issued a Joint Communication to the European Parliament and the Council on *Resilience, Deterrence, and Defence: Building strong cybersecurity for the EU*. In this Joint Communication, one of the key actions was to swiftly adopt the proposal on the so-called "EU Cybersecurity package". As a consequence of the EU Cybersecurity package, the so called "[Cybersecurity Act](#)" was proposed (*Regulation on ENISA, the "EU Cybersecurity Agency" and on Information and Communication Technology cybersecurity certification*). The present proposal repeals the Regulation 526/2013 (*Regulation (EU) 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004*) and seeks to give the European Union Agency on Network and Information Security (ENISA) a more central and specified role, together with establishing a European Cybersecurity Certification Framework for ICT products and services.

2.3.1 ENISA

In the Cybersecurity Act, ENISA gets the veil of a center of expertise, supporting Member States and the Commission on cybersecurity certification. Under this mandate, ENISA could perform functions to support the internal market and cover a cybersecurity 'market observatory' to analyse the trends of the cybersecurity market and then reflect that in the EU policy development in the ICT standardisation. ENISA would also be involved in the EU cybersecurity blueprint, in order to coordinate responses to large-scale cross-border cybersecurity incidents and crises at the EU level. This blueprint will be applicable only to cybersecurity incidents with extensive effects on two or more Member States and with political significance on the EU political level.

Specifically, ENISA will help to prepare the European cybersecurity certification schemes, which will then be adopted by the Commission through implementing acts. Additionally, if a cybersecurity certification scheme is needed, the Commission can also request from ENISA to prepare such a scheme for specific ICT products and services. These schemes will be jointly developed between ENISA and the European Cybersecurity Certification Group, consisting of national certification supervisory authorities of all Member States. The European Cybersecurity Certification Group is incorporated as a working group within the European Cyber Security Organisation (ECSO), which will be discussed more in depth in section 2.4.

2.3.2 Cybersecurity certification of ICT products and services

The Cybersecurity Act does not introduce any directly operational certification schemes *per se*, but it does create a system or framework to establish specific certification schemes, the termed "European cybersecurity certification schemes". The European cybersecurity certification schemes will allow certificates issued under those schemes to be recognized across all Member States and address the present market fragmentation. The general rationale behind the European cybersecurity certification scheme is to show that the ICT products and services are certified in accordance with a typical scheme that complies with specific cybersecurity requirements. A practical example of that could be the certification for a ICT product which includes the ability to protect personal data against unauthorized storage or processing. Thus, the European cybersecurity certification schemes would make use of existing standards of EU policies and regulations, that products need to comply with, in terms of technical requirements.

2.3.3 NIS directive, GDPR and Cybersecurity Act

Putting the three legislations discussed together, two of them to be implemented and one to be voted upon the European Parliament and the Council, it is clear that the EU is slowly building upon each policy to fortify different parts of or relating to cyberspace security.

Under the NIS Directive, there is a protection of the vital operators of the Member States' economy and society, which is enhanced by the proposal of the Cybersecurity Act. The proposal provides a tool for companies subject to the NIS Directive, to certify their ICT products and services against cybersecurity risks.

The GDPR itself, specifically lays down provisions to establish certification mechanisms with the objective of demonstrating compliance. For this purpose, this Cybersecurity Act could establish certification mechanisms that are directly tackling scenarios of data processing in ICT products and services and which could also

satisfy the requirements enlisted in article 42 of the GDPR. The support demonstrated through the Cybersecurity Act shows that the certification mechanisms will not be a way out of companies to show fake compliance, but a serious consideration in terms of marketing and promoting their ICT product or service.

2.4 European Cyber Security Organisation (ECSO)

The European Cyber Security Organisation (ECSO) is a key player in facilitating and enabling the collaboration between the private sector (including commercial companies, research organisations, and academic institutions) and the public sector, within the cybersecurity domain. ECSO is unique in that the organization includes members who are product & services providers, cybersecurity users and regulators in such a way that cooperation and implementation and harmonisation can be made possible across the European Union.

ECSO has 6 working groups covering the following areas:

- WG1: Standardisation, certification, labelling and supply chain management
- WG2: Market deployment, investments and international collaboration
- WG3: Sectoral demand
- WG4: Support to SMEs, coordination with countries (in particular East and Central EU) and regions
- WG5: Education, awareness, training, cyber ranges
- WG6: Strategic Research and Innovation Agenda (SRIA)

2.5 National initiatives in Member States

While the intention of this deliverable is not to catalog the national initiatives in Member States, we point to the ENISA website for this and note that a number of initiatives are currently in process. At the same time, the intention of Cyberwatching.eu is to ensure that we do not reinvent the wheel.

2.6 How Research and Innovation is addressing governance needs

As described above, Europe is taking key steps to harmonize cybersecurity legislation across the European Union through the NIS directive, GDPR and the Cybersecurity Package. EC-funded projects are a key part of the CS&P ecosystem in terms of both raising awareness and providing services and tools that can support SMEs, public administrations and other stakeholders in being compliant. In this section we highlight a number of these initiatives.

Protecting Critical Infrastructures

CIPSEC - Enhancing Critical Infrastructure Protection with innovative SECURITY framework
May 2016 – Apr 2019
www.cipsec.eu

CIPSEC develops an integrated framework composed by a heterogeneous set of products and services, providing high levels of protection for the whole critical infrastructure, considering both its IT (information technology) and OT (operational technology) networks. The outcomes are meant to be exploited in a wide range of verticals. CIPSEC brings use cases in railway, health and environment protection

contexts.

End-users

IT and OT for critical infrastructures including verticals such as chemical industry, ICT, energy, nancial services, food industry, health, transportation, water systems and facilities, nuclear, emergency services or manufacturing, amongst others.

The stakeholders group includes operators of critical infrastructures (whether public or private), large organizations, academia, SMEs (especially those being ICT-intensive), standardization groups, policy makers, public-private partnerships (PPPs), public authorities and people working on related European Projects, among others.

End-user benefits

CIPSEC contributes to the reduction of the capital investment in controlling and solving security threats for critical infrastructures. CIPSEC aims at increasing the confidence on the role of ICT in the daily operation of critical infrastructures, with positive impact in efficiency, quality of service and business profits.

CIPSEC also makes an impact by reducing the economic exposure linked to the consequence of cyber incidents and the likelihood of environmental disasters.

cyberwatching.eu Service Offer

<https://www.cyberwatching.eu/cipsec-enhancing-critical-infrastructure-protection-innovative-security-framework>

CITADEL - Critical Infrastructure Protection using Adaptive MILS

Jun 2016 – May 2019

www.citadel-project.org

CITADEL will provide innovative platform technology, methodology and tools for development, deployment, and certification of adaptive MILS systems for CI, which will be demonstrated in three industrial CI demonstrators. The solution enables robust and resilient CI through monitoring and adaptive self-healing mechanisms that respond to natural and malicious occurrences by intelligently reconfiguring hosts, functions, and networks, while maintaining essential functions and defences.

End-users

The project targets operators of critical infrastructures and providers of the underlying communication and computation technologies used for implementing for critical infrastructures. The project is focused on demonstrators addressing three different critical infrastructure domains: airspace control, process automation and subway transportation.

End-user benefits

Increased preparedness, reduced response time and coordinated response in case of a cyber-incident affecting communication and information networks of critical infrastructure operators. For each critical infrastructure domain demonstrated CITADEL will deliver uninterrupted availability of the most critical functions and core services operational under attack or failure scenarios. Savings potentials are substantial when compared to manually (re-)configured and maintained systems, among others by eliminating down-times in case of attacks or changes in the network architecture.

cyberwatching.eu Service Offer

<https://www.cyberwatching.eu/citadel-critical-infrastructure-protection-using-adaptive-mils>

Dealing with Data Privacy and Data Protection**SPECIAL - Scalable Policy-aware linked data arChitecture for privacy, trAnsparency and compLiance**

Jan 2017 – Dec 2019

www.specialprivacy.eu

SPECIAL reconciles Big Data and personal data protection via an innovative data handling solution and a transparency framework. SPECIAL will allow the acquisition of user consent at collection time and the recording of both data and metadata and make this information available at all stages of processing. Specifying purposes in the database and establishing an underlying communication link allows data controllers to handle personal data in accordance with the legal provisions and to demonstrate transparency and offering relevant choices to their customers.

End-users

The SPECIAL platform will ease industry's difficulties with GDPR compliance and to enable respectful treatment of personal information.

data subjects in their roles as customers, citizens, app-users, subscribers etc.; data controllers in particular big data scientists, technology companies and operational data owners, etc.; big data scientists and companies; entities providing infrastructure or software for data controllers that must be able to show that their product's GDPR-compatibility; policy makers, parliamentarians and the data protection community may provide the necessary encouragement to deploy the solutions; entities interested in providing data protection relevant information to data subjects based on the user interaction research driven within SPECIAL

End-user benefits

The application of SPECIAL will enable data subjects to gain more transparency and control over how their personal data is processed. Parts of the SPECIAL-results may support some of the features in the GDPR such as serving as a technical specification to exercise the right to object according to Art. 21 (5) GDPR.

cyberwatching.eu Service Offer

<https://www.cyberwatching.eu/special-scalable-policy-aware-linked-data-architecture-privacy-transparency-and-compliance>

OPERANDO - Online Privacy Enforcement, Rights Assurance and Optimization

May 2015 – April 2019

www.operando.eu/

The OPERANDO project will create a platform that will be used by independent Privacy Service Providers (PSPs) to provide comprehensive user privacy enforcement in the form of a dedicated online service, called "Privacy Authority".

OPERANDO will support a simple Privacy Dashboard allowing users to specify their preferences. These will be automatically compared with Online Service Provider (OSP) privacy policies and translated into personal data access control decisions by the PSP.

OPERANDO will also address OSP requirements for simplified privacy compliance checking and auditing, to verify that they will meet user expectations or to satisfy privacy regulators.

End-users

Privacy Service Providers, Users, Online Service Providers and Regulators, Public administrations, Healthcare.

End-user benefits

For end users OPERANDO provides the ability to manage all online privacy issues in an intuitive web-based dashboard. The user can set their User Privacy Policy (UPP) according to their preferences, which will be transparently enforced for each of the user's devices. The service will be free to users and simple to enrol.

For Service Providers consuming privacy services will grant the ability to benefit from:

- Cost-effective compliance with privacy regulations;
- Access to a lucrative user base and big data analytics reports;
- Avoid assumed consent, and inadvertent exposure of unsolicited information;
- Easy requests for information, allowing sharing between organisations for co-ordinated care;
- Sensitive Personal Data is held offsite;
- Compliance with evolving data protection legislation is ensured.

For Data Regulators OPERANDO will provide access to the human- and machine-readable privacy guarantees of the Service Providers, and the ability to input privacy regulations in a similar form. This will allow an automated audit for compliance with the relative regulations. The OPERANDO project has engaged consumer rights and standardization organizations, endorsed by the EU, as members of its Advisory Board, and will act to position the OPERANDO platform for endorsement by European governments.

cyberwatching.eu Service Offer

<https://www.cyberwatching.eu/services/catalogue-of-services/operando>

Certification

CERTMILS - Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats
Jan 2017 – Dec 2020

www.certmils.eu

certMILS will develop a MILS platform (Multiple Independent Levels of Security) within the cyber-physical system to dramatically reduce the complexity of the certification of cyber-physical systems.

The platform will be tested into three industrial CPS pilots (smart grid, railway, subway) with the aim of certifying security of critical re-useable components, and ensuring security certification for the pilots by certification labs in three EU countries with involvement of the authorities.

End-users

Certification Authorities, System Integrators

End-user benefits

As regards the cyber-physical systems, there are already in place safety methods as well as “safety certification stakeholders”, so the certification of cyber-physical systems must respect the existing safety certification processes.

Therefore, certMILS will generate rich interaction between developers, evaluation laboratories and certification authorities in three European countries resulting in:

- Validated modular Protection Profile
- Standardised and validated methodology for evaluating and certifying high assurance products
- Guidelines for compositional security for developers and evaluators

cyberwatching.eu Service Offer

<https://www.cyberwatching.eu/certmils-compositional-security-certification-medium-high-assurance-cots-based-systems-environments>

EU-SEC - The European Security Certification Framework

Jan 2017 – Dec 2019

www.sec-cert.eu

European Security Certification Framework (EU-SEC) is an innovation project with an aim to create a framework under which existing certification and assurance approaches can co-exist. Its main goal is to improve the business value, effectiveness and efficiency of existing cloud security certification schemes and to increase the level of efficiency and trustworthiness of the cloud market by offering solutions that makes the companies' compliance effort more cost-effective and high-level assurance.

End-users

Cloud service providers, Cloud users, Authorities

End-user benefits

The project EU-SEC will improve the effectiveness and efficiency of existing approaches for assurance and compliance by developing a specific framework that will equip stakeholders in the ICT security ecosystem with a validated governance structure, a reference architecture, and the corresponding set of tools to improve the efficiency and effectiveness of their current approach to security governance, risks management, assurance and compliance.

cyberwatching.eu Service Offer

<https://www.cyberwatching.eu/eu-sec-european-security-certification-framework>

2.7 GDPR & Certification: Considerations from the Concertation meeting

With cyberwatching.eu's Concertation Meeting taking place one month before the GDPR coming into force in May 2018, there was much discussion on the topic and a strong message that compliance should be seen as an opportunity for companies in particular to offer truly trusted services.

Some points covered at the event are summarized below.

- The GDPR has raised a lot of awareness about personal data and privacy. In this area, too, there is a need to create possible EU curricula with academics.
- The GDPR is not a catalogue nor a checklist. It requires investment and knowledge.
- GDPR is based on risk assessment which means that each organization/company is different. Unless a supervisory authority takes a stand to ensure GDPR compliance, there is the risk of being exposed to possible sanctions.
- From an international perspective, there is a perception that GDPR makes doing business with Europe more difficult; in other words, it could be perceived that there are additional barriers being created and some companies might feel discouraged in this respect to work with Europe. It was felt that what foreign companies required was to be accompanied in order for their business to be GDPR compliant.
- GDPR is not just about transparency. There is much more to it. It is about changing work flows, doing due diligence. The know-how and evaluation costs money and time. There should be a step forward by the EU governments to create a platform to help foreign companies to comply and also a platform for SMEs to comply.
- The GDPR is a serious concern for SMEs who do not have the resources to spend the time and money to be compliant. GDPR is a competitive disadvantage for SMEs. A "light" version of GDPR for SMEs could be a solution. Some guidelines at EU level for SMEs is required otherwise SMEs may be exposed to high risk of exposure.
- From an on-hands perspective of an end-user, a lot of time is spent in redefining policies resulting in long legal documents which are rarely fully read. Some guidance on how to be transparent and straightforward with customers would be very useful.
- There is a growing trend for data protection means, but for under 25 year olds, this sector is not aware. What are the impacts of GDPR that were not quite foreseen.
- Finally, a positive element is that if a service outside Europe does not comply, then, searching for a company which offers a compliant service within Europe is positive as a European business benefit and opportunity.

3 Risk Management

3.1 Overview

As the Fourth Industrial Revolution progresses, driven by widespread use of mobile technologies, cloud computing, corporate bring-your-own-device policies, big data analytics, and 3D printing, risks are evolving; so Cyber Risks has emerged as one of the fastest growing risks for governments and companies across the globe. Equally or perhaps even more important is the growing realization that cyber risk, in some instances more pervasive than traditional exposures, is present wherever organizations use technology to touch people, suppliers, customers, and governments.

In light of these changes, it is necessary to find out what large forward-thinking companies around the globe think about cyber risk and ascertain their attitude towards managing it.

The most relevant surveys¹ about risk management underline how cyber risk is perceived as arousing between relevant companies, and SMEs.

The Allianz risk Barometer 2018 defines cyber risk as the 2nd major risk for companies worldwide and new threats such as “cyber hurricanes”, increasing reputational risk and tougher data rules mean businesses and risk experts are more concerned than ever.

¹ Aon-Captive-Cyber-Survey-Interactive; Allianz risk barometer 2018; Aon Global Risk Management Survey 2017; IBM

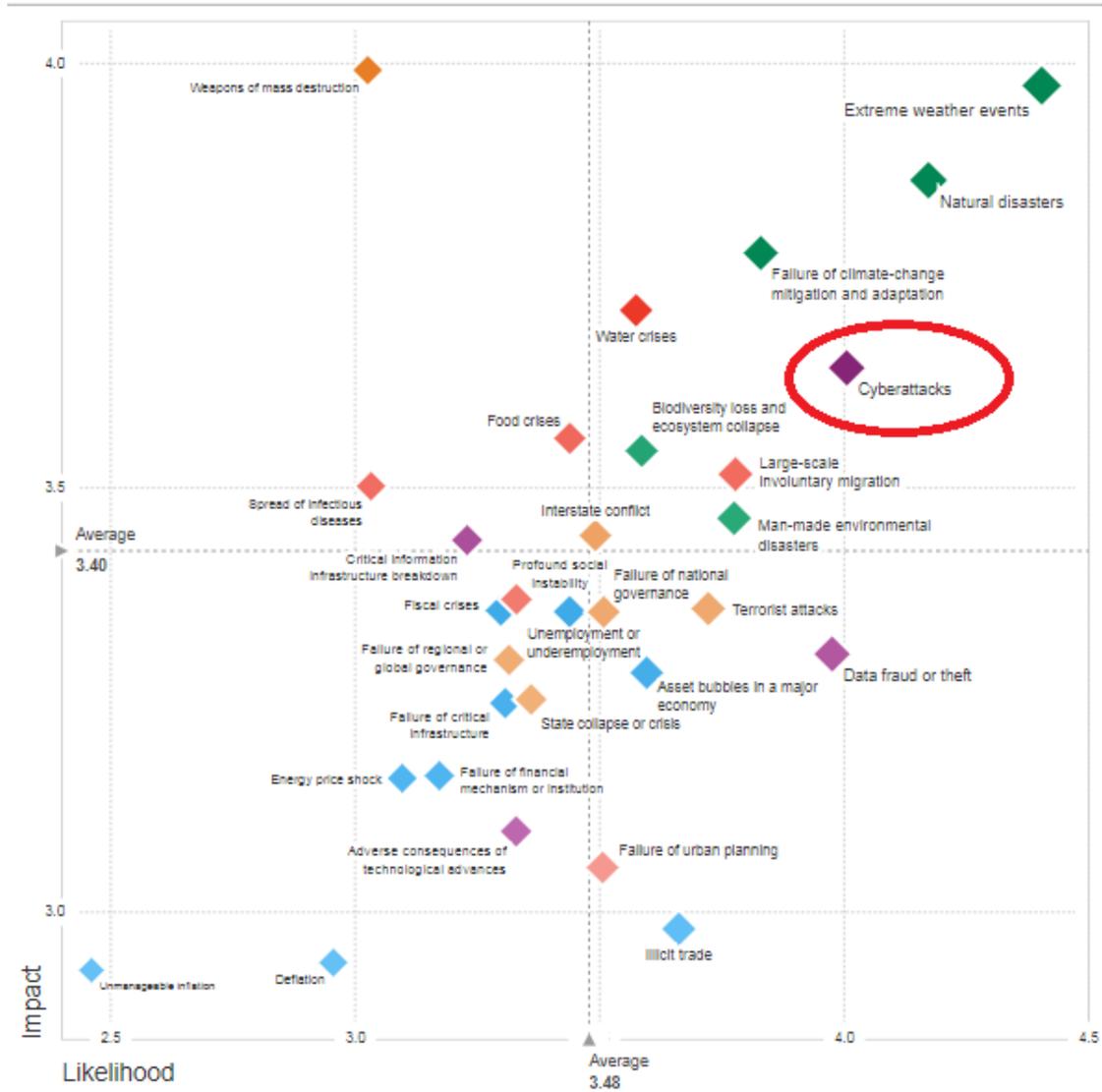


Figure 1: The Global Risks Landscape 2018 - World Economic Forum

The Aon Global Risk Management Survey (AGRMS 2017) defines the impact of Cyber risks due to data breaches occurred in the recent past, as “deadly”. For this reason, cyber crime/hacking/viruses/malicious codes are on the 5th place as the major risk perceived by companies and this risk entered the Top 10 list for the first time (at number nine) in 2015.

EY² declares in the 20th Global Information Security Survey that only 4% of organizations are confident that they have fully considered the information security implications of their current strategy, and that their risk landscape incorporates and monitors relevant cyber threats, vulnerabilities and risks.

The Evolving Risks Landscape, 2007-2017, describes as Cyber Risk Massive incident of data fraud/theft as the 5th Global Risks in Terms of Likelihood.

² EY GISS; Global Information Security Survey

If the current business environment is to be effective, it is essential to know how to manage and exploit huge amounts of data, as well as fully protect all the potential and the tools offered by the network.

Unfortunately, these elements - which will bring new opportunities - also bring on the other side a set of new risks to manage and mitigate.

As a consequence of the cyber threat evolution, it is necessary to adjust also the approach towards the IT assets protection of IT facilities and business processes, by passing from a static paradigm to a dynamic risk view. This vision is presented in the following paragraphs.

3.2 Enterprise Risk Management Context

The enterprise business is characterized by an indissoluble link with the risk. Risk is an intrinsic characteristic of company business and risk identification, evaluation and management capacities are at the base of a company's success.

The interest in risk management became very relevant assuming crucial importance since the nineties: gradually its value has increased, booming in recent years. However, initially risk was considered, in practice and in literature, merely as a secondary element within the enterprise management, as risk management was usually restricted to simple separated actions aimed at reducing the uncertainty derived from specific activities. The limits of this orientation became evident by the end of the nineties, when the greater uncertainty showed by the economic context and financial markets deeply changed the context in which the enterprise works. The increasing competitiveness, the new organization models, impacts derived from technical developments of business competitive dynamics, the financial collapses recently affecting some listed large enterprises, the increasing social, economic and political instability has increased the degree of instability, uncertainty and the set of variables impacting the achievement and maintenance of company results. Real estate markets, credit institutes, rating agencies and investors became aware of the increasing relevance of risk in company activities asking the companies to take more into account such issues as well as to take appropriate measures to manage risk, pointing out the need to improve internal control systems of the companies in order to anticipate and manage the change and, therefore, to strengthen and increase their capacity to create value for the stakeholders. The traditional risk-insurance approach is being given up in favor of an integrated management process related to generally accepted organization solutions shared by the whole organization. The crisis in 2008 contributed furthermore to spreading among companies the awareness about how even apparently irrelevant risks could cause serious damage, if not managed adequately, and this is even truer if various types of risk events interact.

The result is that a good risk management model should make it possible to understand the potential positive and negative aspects of all factors that can impact the organization, by increasing the likelihood of success in the strategy and thereby reducing the uncertainty of achieving the general objectives of the company. Therefore, risk management becomes a further productive factor in the company framework, to be managed according to common entrepreneurship practices.

According to the new COSO (Committee of Sponsoring Organizations of Treadway Commission) document (June 2017) "Enterprise Risk Management - Integrating with Strategy and Performance", ERM (Enterprise Risk Management) is defined as "The

culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value”.

The previous document - published in September 2004 - defines the Enterprise Risk Management (ERM) as a process put in place by the board of directors by the top management and other company staff; applied to develop the company strategy of the entire organization, planned to identify and manage events that could have a positive or negative impact on the company; focused on maintaining the company risk level within an acceptable risk appetite³ threshold; designed to provide a reasonable guarantee to the company related to the achievement of its objectives. In this model, risk management goes with a regular operative activity and becomes integral part of the company organization structure.

Furthermore, the ERM adopts a comprehensive risk vision that proves to be essential in order to identify the possible interconnections between the various risk types. In fact, only considering the company as a single entity, in which various areas and activities interconnected in organizational units, processes, etc., it is essential to apply a management model that provides the analysis and management of risk according to the different peculiarities applicable to the Organizational context (eg environmental risk, operational risk, cyber risk, financial risk). Therefore, the Enterprise Risk Management (ERM) model proposed by COSO has promoted the organic paradigm of integrated and holistic management of all types of business risk, in which ERM is aimed at the in-depth analysis of the company assessing the global risk profile. A complete and detailed company assessment is essential for a correct evaluation and selection of company strategies and related objectives.

Therefore, integrated risk management acquires a strategic tactic and competitive nature, able to positively influence the entire process of creating value for the company.

The **Cyber Security Risk Management process** should be embedded and perfectly integrated within the Enterprise Risk Management process (if already available in the organization), according to a common Framework that makes possible to put together information in order to obtain a systematic perspective of company risks as well as a selection of specific actions within the IT scope in terms of mitigation priorities. The Cyber Risk Management process in this sense has the aim to perform a unique reporting for the company management.

³ The broad-based amount of risk in different aspects that an enterprise is willing to accept in pursuit of its mission

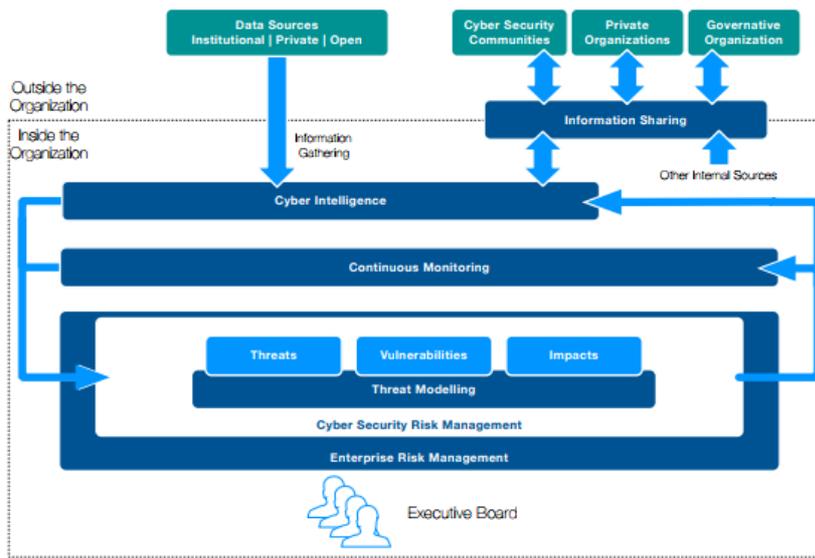


Figure 2: Evolved approach to cyber risk management⁴

A significant and niche approach, as it is specifically addressed to the cyber security aspects of small and medium enterprises, is represented by “A simplified approach to Risk Management for SMEs”, an initiative of 2007 promoted by the European Agency for the Security of Networks and Information (ENISA). As indicated in the title, the afore-mentioned European Union body decided to equip the management staff that are not expert in matters of security, with a simple tool to perform a guided and modular risk self-evaluation. In this regard, security aspects have been simplified and acceptable target security levels have been established, identifying a target risk profile to tend to.

In the following paragraphs, we describe with more detail the cyber security risk management process – as a part of the ERM process - and the related components.

3.3 A cyber security risk management process⁵

In defining the cyber security risk management process, the organization should achieve the following objectives:

- Establish univocal criteria for the evaluation and identification of cyber risks;
- Standardize a uniform analysis method in order to achieve comparable results over time;
- Be aware of the risk exposure level of each company information system component;
- Assess if the identified risk is acceptable or if, instead, it is necessary to plan appropriate processes to mitigate the risk.
- Provide an adequate and flexible method to identify technical-organizational protection needs in order to balance in the best way the possible preventive and detective security countermeasures;
- Allow the monitoring and analysis of security events in order to put in place improvement actions;

⁴ as described in the Italian National Cyber security Framework

⁵ http://www.cybersecurityframework.it/sites/default/files/CSR2015_ENG.pdf

- Assess all potential risks in defining and implementing new IT services; Identify a company function that coordinates all activities;
- Embed the cyber security risk management process within the Enterprise Risk Management process (if already available in the organization), according to a common Framework that makes possible to put together information in order to obtain a systematic perspective of company risks as well as a selection of specific actions within the IT scope in terms of mitigation priorities. perform a unique reporting for the company management.

The activation of the cyber security risk management process would allow the organization to achieve a set of benefits, among them, the following:

- Comply with national and international laws and regulations that expressly require that the organization is equipped with an IT risk Analysis method or process;
- Ensure the compliance of the IT governance with the company business objectives, in terms of sustainable evolution, operation excellence and cost competitiveness, through risk exposure reduction;
- Plan appropriate response actions to potential cyber-attacks in order to minimize possible impacts and therefore ensure the continuity of supplied services;
- Enable the organization to minimize security costs, ensuring an appropriate risk reduction at acceptable levels by the organization self. In other words, avoid the costs for implementing a security level, which could be higher than the appropriate one and which might apply to information system components with low impact for the organization.

With the aim of handling effectively cybersecurity risks, there will be an increasing demand for cyber security risk assessments, even to be compliant to a corresponding certification management system. Risk management has the aim to define coordinated activities to direct and control an organization with regard to risk. The activity to manage residual risk is, according to ISO 27001, “the risk remaining after risk treatment”.

The design and activation of the cyber security risk management process requires a series of initiatives that, even if strongly dependent on the initial situation, could imply a considerable amount of effort (human resources, time, IT security investments, etc.). Therefore, its implementation should take place at different stages of a project.

3.4 Risk Analysis

Risk Appetite and Risk Tolerance

In the risk management analysis, primary relevance is given to the definition of the internal environment and company strategic objectives. The internal environment represents the essential identity of an organization, establishes the modes in which the risk is considered and addressed by the company staff, the ethical values and the general working environment. In this framework, it is crucial to define the company risk management philosophy. This represents the common attitudes of the company’s risk approach, the way it is considered in all activities, identified and managed. It results then in the identification of the company’s Risk Appetite that is the inclination to the risk that reflects the way in which events are perceived and identified, what kinds of risk are accepted or not and how they are managed. Risk Appetite is identified and is the result of a dialogue between the management and

the board of directors, as it impacts both the strategic choices addressed to the board and the operative ones related to the directors of various units. The Risk Appetite choice is at the base of decisions taken related to the strategy to follow as well as the allocation of resources among the various business divisions. However, as said before, the ERM purpose is to give reasonable certainty of achieving the strategic objectives. It is therefore necessary to quantify such reasonability. The tolerable risk threshold is to be established according to the activity performed by the organization that implements it and according to a wide set of other variables. Such confidence threshold establishes the acceptable deviation levels compared to the objective achievement, it is called Risk Tolerance and is measurable with the same unit of measure chosen for other objectives.

Risk Assessment

The risk analysis process begins with the identification of risk events that could impact the achievement of a company's objectives. Each of them identifies risks as subject to two assessments: Before and after the mitigation actions put in place by management. The first assessment defines the inherent (or intrinsic) risk that is the maximum possible risk level, without any applied mitigation action. The second assessment defines the residual risk that is the part of risk remaining to the company after having put in place the existing control activities on the inherent risk. Mitigating actions are all the activities put in place to reduce the likelihood of risk events and/or linked impact.

Risk assessment regards two aspects: impact; likelihood.

Impact: The identification of the risk impact consists of defining the type of potential loss and measuring the size of the risk event. Considering that each risk is related to a specific objective and that this is qualitative as well as quantitatively measurable, risks may be quantified by using the same measurement of the referenced objectives. Typically, the criteria for the risk impact assessment are:

- **Economic:** The risk effect in terms of lower profit and higher costs is assessed. Such criterion is applicable to all those risks having a quantifiable effect on the income statement of the Company and they require the definition of specific thresholds based on a reference parameter (Costs, Revenues, Margin);
- **Market:** Possible loss of market shares as a consequence of risks related to inability to fulfill customer needs in terms of product/service quality;
- **Reputational:** Based on the occurrence of possible events that could damage the Company image;
- **Competitive advantage:** It measures the loss of competitive advantage acquired by a Company in case of occurrence of risk events.

Likelihood: The likelihood of risk occurrence is the possibility that an identified event/risk occurs in a given period of time. This aspect remains one of the most complex and controversial in the risk analysis process. Without precise quantitative [as underlined in 3.5.1] information that may derive from the analysis of similar previous experiences or from the specific analysis of relevant phenomena, it is possible to identify the

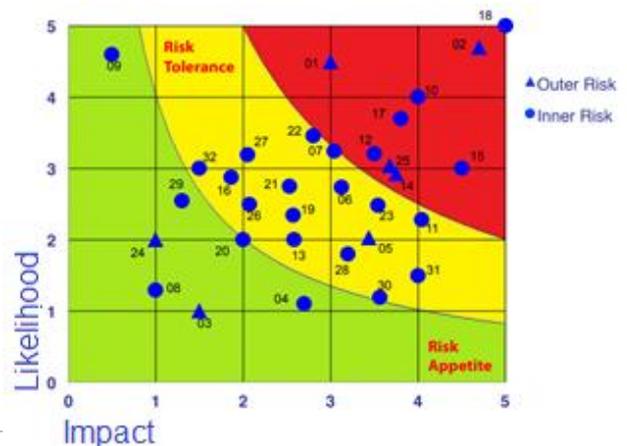


Figure 3 Risk Assessment Matrix

occurrence likelihood based on the staff sensitivity and experiences in their competence function scope. It is also possible to establish and create a risk matrix, similar to the one showed by Figure 1, that is a brief representation of the positioning related to single risks compared to the company's risk appetite and risk tolerance, enabling the management to identify action priorities and possible risk response strategies. Risk assessment, given by the multiplication of occurrence likelihood and impact, generates different risk levels.

3.4.1 Relationship between residual risk and risk acceptance

The purpose of residual risks is to find out whether the planned treatment is sufficient – the question is, how would you know what is sufficient? This is where the concept of acceptable level of risks comes into play – it is nothing else but deciding how much 'risk appetite' an organization has, or in other words whether the management thinks it is fine for a company to operate in a high-risk environment where it is much more likely that something will happen, or the management wants a higher level of security involving a lower level of risk.

Both approaches are allowed in ISO 27001 – each organization has to decide what is appropriate for its circumstances and for its budget. The former approach is probably better for high-growth startup companies, whereas the latter is usually pursued by financial organizations.

3.4.2 Residual risk management

After the risks are identified, an Organization⁶ needs to mitigate the risks deemed as unacceptable (through a mitigation plan). After the selected risks are addressed, it is impossible to eliminate all the risks because a risk is always >0 – therefore, some risks will remain at a certain level, and this is what residual risks are. The organization needs to know exactly whether the planned actions to address risk management are enough or not.

The company's management, once it has understood the residual risks, establishes how to align them with the target risk appetite level through a risk treatment plan. Possible answers to risk may be classified according to the following categories⁷:

- **Risk acceptance:** If the level of risks is below the acceptable level of risk, the management needs to formally accept those risks.
- **Risk reduction:** If the level of risks is above the acceptable level of risk, the Organization needs to find out some new (and better) ways to mitigate those risks, through the implementation of the actions described in the risk treatment plan – that also means the need to reassess the residual risks (typically the what-if analysis).
- **Risk sharing/insurance:** If the level of risks is above the acceptable level of risk, and the Organization decides to pursue the path of not investing to mitigate the risks, it could opt for risk transfer through a cyber liability policy, colloquially named as “the last line of defense”
- **Risk avoidance:** If the level of risks is above the acceptable level of risk, and the costs of decreasing such risks would be higher than the impact itself, than the Organization needs to propose to the management that it accepts these

⁶ <https://advisera.com/27001academy/knowledgebase/why-is-residual-risk-so-important/>

⁷ ISO 31000

high risks. In this case, it is not possible to find a valid option that reduces risk impact and likelihood to an acceptable degree, therefore the source of risk is eliminated.

Such a systematic approach ensures that management is involved in reaching the most important decisions, and that nothing is overlooked.

Top management needs to be involved and to know which risks their company will face even after various mitigation methods have been applied. After all, top management is not only responsible for the bottom line of the company, but also for its viability.

3.5 Addressing risk management needs using behavioural analysis

A number of projects are providing services and solutions for stakeholders such as SMEs and public administrations in order for them to be better prepared for how they manage risks. In this section we look at four projects which address these issues: HEREMENEUT, CS-AWARE, SAINT and DOGANA.

HERMENEUT - Enterprises intangible Risks Management via Economic models based on simulation of modern cyber-attacks

May 2017 – Apr 2019

www.hermeneut.eu

Hermeneut project aims at developing modelling of cyberattacks, measuring their intangible impacts both at micro and macro levels and developing simulation approaches to cyber risks management.

End-users

SMEs, Large companies, CISOs, CIOs, Insurers, Analysts especially in the Healthcare, Financial sectors and overall in all IP intensive industries.

End-user benefits

The project will develop a holistic risk assessment model able to support decisions on cyber-security investments for possible hard and soft mitigation measures, integrating also dedicated elicitation approaches and a Benefit-Harm Index (BHI). This will help to give an estimation of the enterprise's vulnerabilities for both the humans and technology, to assess the corresponding tangible and intangible assets at risk against cyber-attacks and cyber-crime.

cyberwatching.eu Service Offer

<https://www.cyberwatching.eu/hermeneut-enterprises-intangible-risks-management-economic-models-based-simulation-modern-cyber>

SAINT - Systemic Analyser in Network Threats

May 2017 – Apr 2019

www.project-saint.eu

SAINT proposes to analyse and identify incentives to improve levels of collaboration between cooperative and regulatory approaches to information sharing in order to enhance cyber-security and mitigate (a) the risk and (b) the impact from a cyber-attack, while providing, at the same time, solid economic evidence on the benefit from such improvement based on solid statistical analysis

and economic models.

End-users

Academic researchers, cyber security practitioners, market agents, law enforcement authorities, policy makers, regulators, governmental authorities

End-user benefits

SAINT will collect important information, regarding cyber-threats and relevant vulnerabilities, tangible (assets) and intangible (reputation) risks in order to identify the most relevant indicators and metrics.

SAINT will analyse these cyber security data metrics with a multidisciplinary methodology, employing analytic frameworks from various scientific disciplines (IT, Economics, Psychology, Law), resulting in a new empirical science consisting of novel analytic methods and models for cyber-security.

cyberwatching.eu Service Offer

<https://www.cyberwatching.eu/saint-project-cybersecurity>

CS-AWARE - A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis

Sep 2017 – Aug 2020

www.cs-aware.eu

The main objective for this project is to provide a cybersecurity situational awareness solution for small- to medium-sized IT infrastructures. This solution enables detect, classify and visualise cybersecurity incidents in real-time, supporting the prevention or mitigation of cyber attacks. The solution will be a big step towards automation of cyber incident detection, classification and visualisation, and will be based on mature big data analysis tools and methodologies provided by consortium partners.

End-users

Public administrations and small- to medium-sized IT infrastructures.

End-user benefits

Increased competitiveness of European ICT security products and services catering to the needs of SMEs, local public administrations and individuals.

Increased resilience against widespread cybersecurity threats facing SMEs, local public administrations and individuals.

Increased effectiveness of cybersecurity solutions through usability advancements and increased automation.

cyberwatching.eu Service Offer

<https://www.cyberwatching.eu/cs-aware-cybersecurity>

DOGANA - Advanced Social Engineering and Vulnerability Assessment Framework

Sep 2015 – Aug 2018

www.dogana-project.eu

DOGANA will leverage both on regularly performed Social Vulnerabilities Assessments (SVAs), and on an efficient framework to help deploy effective mitigation strategies and lead to reducing the risk created by modern Social Engineering 2.0 attack techniques.

End-users

SMEs and Large organizations in energy, finance, transport, utilities sectors as well as public authorities

End-user benefits

The main DOGANA aim is to provide enterprises with a complete framework to assess their exposure and consequently adopt secure countermeasures. On a practical level DOGANA will deliver a complete toolset to detect and prevent social-engineering cyber-attacks at 4 levels:

- technological: develop an integrated tool-chain to assist social vulnerability assessments and evolve on the existing tools
- legal: supply a legal framework to assist enterprises to perform internally this type of assessments
- education: study and experiment new awareness methodologies to improve the education of employees with the aim of a lasting and efficient training.
- risk management: measure the risks consistently

cyberwatching.eu Service Offer

<https://www.cyberwatching.eu/dogana-project>

3.5.1 Risk sharing/insurance: Cyber Insurance

A recent publication from ENISA “Cyber Insurance: Recent Advances, Good Practices and Challenges” underlines the “last line of defense” as one of the ways to manage risks.

In fact Cyber insurance was created to address risk that cannot be reasonably mitigated by remediation plans and technological, organizational or security measures. Whilst it initially started in a limited form, it developed to cover more and more types of cyber risk. In comparison with other insurance sectors, cyber insurance appears to have a lower adoption rate, while the growth projections remain high. Projections estimate that the global cyber insurance coverage is expected to double or triple over the next few years⁸, growing from its current estimated \$1.5 billion to \$3 billion in U.S. premiums. Some predict sales could soar to \$ 7.5 billion in annual sales by 2020 and over \$ 20 billion by 2025.

Cyber insurance products have been around since the late 90s. The demand originated from the technology, media and telecom (TMT) sector and professional services firms which needed coverage to protect themselves against inadvertent transfer of malware (cyber liability cover) and loss of confidential client information (privacy breach cover). Initially developed as add-on coverage or bundled into

⁸ The wall street journal, Cyber Insurance: How to Address Obstacles to Growth

existing liability or professional indemnity policies, these early products were a first attempt by insurers to offer traditional risk transfer solutions to help their clients with an emerging risk.

With the global strengthening of regulations on loss of personally identifiable information (PII), the costs related to the handling of a breach (cyber security incident in general) increased: i.e. the costs of reporting a breach to the regulator, customer notification, PR costs and legal expenses.

Awareness of cyber threats also started to reach the boardroom. A study conducted by Aon and Aon Inpoint estimated the 2015 global standalone cyber market to be worth \$1.7bn in annual gross written premium. Although cyber insurance has been around for over 25 years, the market has grown tremendously in recent years, achieving annual growth rates of 30% between 2011 and 2015; levels not seen in traditional lines of business.

In Europe and in the US, due to the established cybersecurity & privacy related legislation, there is a higher adoption of cyber insurance than in regions that have recent or no formal legislation.

According to a recent Aon Benfield report, there has been a significant uptick in demand for cyber insurance, particularly in the wake of high-profile cases.

On the other hand, the “last line of defense”, could be seen as an instrument to support the defense strategy within the organization with higher insurance premium in the short term, decreasing it due to a combination of the implementation of remediation plans to mitigate the risks identified through a process of finding, and recognizing the possible events.

Actually, many Member States are recognizing the importance of addressing cyber risk, and have taken relevant actions by publishing national cyber security frameworks⁹. Furthermore, insurance federations have also taken a great interest in cyber insurance, with actions taking place on both European and national levels. Among others, insurers are facing challenges around the lack of cyber-security incident data supporting risk assessments, but mainly to estimate the likelihood of the occurrence.

On the other hand, gathering information on cyber security management within organizations is not easy, and the uncertainty around accumulating risk underlines the growing need for specific services in cyber security and cyber insurance.

Further to the reported good practices, ENISA had some relevant recommendations, directed at policy makers, insurers, and customers, for the improvement of cyber insurance constituency.

Cyber insurance is a product that has been created to counter residual risk associated with the information systems of asset owners. Despite the large number of developments that have taken place over the last few years, the cyber insurance market is yet to receive the anticipated adoption rate. While some regions have

⁹ <http://www.cybersecurityframework.it/>
https://www.ssi.gouv.fr/uploads/2016/10/list-of-security-measures_anssi.pdf

made progress on the basis of supportive legislation, it is found that in comparison with other insurance sectors, the state of cyber insurance is at a less mature stage. With the general data protection regulation (GDPR) being adopted on April of 2016, and network and information security (NIS) directive on July 2016, the need for cyber insurance is anticipated to grow.

Insurers, brokers are challenging a deep revolution in the market with the aim to run pre-policy risk assessments. Those services have the aim to support the clients to define a tailor-made policy, calculating the first-party and third party risks related to a data breach or, more in general to a “data breach”. The methodologies are evolving and generally could be classified as:

- Qualitative risk analysis, The process of prioritizing individual risks for further analysis or action by assessing their likelihood of occurrence and impact as well as other characteristics¹⁰
- Quantitative risk analysis; The process of numerically analyzing the combined effect of identified risks and other sources of uncertainty on overall project objectives.¹¹
- Standard based risk analysis, with the aim to comply to laws, regulations or best practices, as prescribed by the ISO 27001;
- Technologic, product assisted assessments (e.g. Starlings soar <https://www.rheagroup.com/starlings-soar>; panoptesec, <http://www.panoptesec.eu/> ; wiser <https://www.cyberwiser.eu/>; Archer <https://www.rsa.com/en-us/products/governance-risk-and-compliance>)
- Cyber risk self assessment

Future work could focus on individual study findings, or evaluate the pre-policy risk assessment from a pure customers’ perspective. A current theme would be to examine the post-insurance effects on a customers’ environment, or in-depth on market growth and check any possible relation to the industries affected by the NIS Directive.

3.6 Addressing risk management needs through financial instruments (insurance)

Cyberinsurance can fulfill a key role in improving cybersecurity within companies by providing incentives for them to improve their security, requiring certain minimum protection standards. Unfortunately, so far cyberinsurance has not been widely adopted. The CYBECO project specifically addresses the issue of cyberinsurance to fill this gap by including cyberthreat behaviour through adversarial risk analysis to support insurance companies in estimating risks and setting premiums as well as using behavioural experiments to improve IT owners’ cybersecurity decisions.

CYBECO therefore facilitate risk-based cybersecurity investments and progress beyond information security economic models, supporting insurers in their cyber offerings through a risk management modelling framework and tool.

¹⁰ PMBOK® Guide Sixth Edition

CYBECO - Supporting Cyberinsurance from a Behavioural Choice Perspective

Sep 2015 – Aug 2018

www.cybeco.eu

CYBECO will research, develop, demonstrate, evaluate and exploit a new framework for managing cybersecurity risks, one that is focusing on cyberinsurance, as key risk management treatment including a rigorous framework for cyber insurance, with appropriate pricing and segmentation, benefitting from Structured Expert Judgment (SEJ) methodologies to cope with lack of attack data and Multi-Attribute Utility Theory (MAUT) methods to properly value assets

End-users

Insurance companies, brokers, consulting companies, SMEs, large companies, public administrations.

End-user benefits

On the supply side, end-users benefit from better founded and designed cyberinsurance products and cyber risk management frameworks. On the demand side, end-users benefit from a well-founded tool that allows them to determine their optimal cyber security investments, including the appropriate cyber insurance product.

cyberwatching.eu Service Offer

<https://www.cyberwatching.eu/cybeco-supporting-cyberinsurance-behavioural-choice-perspective>

3.7 Standards Overview in Risk management

In order to enforce Cyber Security effectively, there is a need for harmonized standards, a corresponding certification system to ensure compliance, that in some cases needs a Risk Management process and Risk Assessment activities to enable risk-based thinking decision-making.

Sometimes organizations are implementing preventive actions mainly as a requirement to be in compliance with the most relevant standards and best practices¹² and not as a reason for improvement.

The ISO 27001:2013 is a risk-based standard approach for the information security management system. This implies adopting a global vision of business, process, people and technology risks and top management is actively involved in the entire risk mitigation process.

Risk-based thinking goes far beyond preventive actions because it involves analyzing the context and processes to identify risks, take note and record actions to eliminate them or reduce the likelihood of it occurring.

As prescribed by the ISO 31000 and ISO 27001, the level of adoption of the risk-based approach are the coordinated activities to direct and control the organization with regard to risk (effect of uncertainty on objectives).

¹² (e.g. Data protection Risk assessment / impact assessment as prescribed by EU 679/2016 ISO 9001; ISO 27001; ISO 27005; NIST 800-30; ISO31000; ISO22301 etc.)

The main drivers for risk management include providing:

- Stakeholders with substantiated and consistent opinions over the current state of risk throughout the enterprise
- Guidance on how to manage risk to levels within the enterprise's risk appetite
- Guidance on how to set up the appropriate risk culture for the enterprise
- Wherever possible, quantitative risk assessments enabling stakeholders to consider the cost of mitigation and the required resources against the loss exposure, so the risk management process has the aim to build an End-to-end guidance on how to manage risk; through the definition of common and sustainable approach for assessment and response.
- A more accurate view of significant current and near-future risk throughout the enterprise—and the impact of this risk on the enterprise
- Understanding how effectively IT risk management optimizes value by enabling process effectiveness and efficiency
- Opportunities for integration of IT risk management with the overall risk and compliance structures within the enterprise
- Promotion of risk responsibility and its acceptance throughout the enterprise

Companies worldwide, as described in EY Global Information Security Survey 2017-18 are facing threats and vulnerabilities to have most increased the risk exposure in the last years, (2013–2017).

The Benefits to start-up a risk management process, a systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analyzing, evaluating, treating, monitoring and reviewing the cyber risk are various. This process [3.3] in one of the instruments, to address threats and vulnerabilities, if assisted by Vulnerability assessments or penetration tests within the Organizations' infrastructure. The process has the aim to give a more accurate view of significant current and near-future risk throughout the enterprise—and the impact of this risk on the enterprise. Through the analyses companies could understand how effective IT risk management optimizes value by enabling process effectiveness and efficiency, giving the opportunity to define an overall risk and compliance structure within the enterprise providing the risk responsibility and its acceptance throughout the enterprise.

3.8 A skilled workforce is essential – Considerations from the Concertation Meeting

The risk management market was also a topic discussed at the cyberwatching.eu Concertation meeting. A key aspect was what the future holds bearing in mind the current lack of skills in the cybersecurity field and the dearth in fully trained and qualified cybersecurity experts.

With a global shortfall of 3.5 million experts by 2021 with this profile there is a strong need to create technical capabilities in the area of cybersecurity and to change the societal view. The situation is further compounded by a current lack of trainers who also need to be educated themselves. One way to address this is to focus on raising awareness of cybersecurity and to provide simple tools that can do this. In addition,

improving the societal understanding on issues such as private data, will also help improve this situation.

A first target for this should be management-level individuals in companies and organizations, for it is these people who make the decisions. This can cause a drip-down affect can really ensure that a cybersecure culture exists in their organizations.

A final consideration was that Cybersecurity is multidisciplinary and the problem needs to be examined and addressed in order to keep pace with the increasing need to have a cybersecure Europe.

3.9 An SME perspective on cybersecurity - Considerations from the Concertation Meeting

From an SME and micro-SME perspective, cybersecurity is a real challenge and in many ways, skills, resources, investment and the additional requirements are extremely burdensome. SMEs just don't have the same resources for certification or compliance and feel that they are at a competitive disadvantage.

On the other hand, there is a need to conform to be at the same level of quality in order to compete in the market place. Compliance should be seen as a business advantage for companies and well-worth the investment in order to deliver trusted services on the market.

4 Standards and Certification Framework

Within Europe the following three European Standards Organizations cooperate to try and minimize duplication of standards:

- CEN,
- CENELEC, and
- ETSI.

The relevant ISO Standard ISO 27001 risk assessment and risk mitigation in the broadest sense and is considered the baseline standard for cybersecurity.

In order for cybersecurity to be enforced effectively, there is a need for harmonized standards a corresponding certification system to ensure compliance. A recent publication from ENISA "Challenges of security certification in emerging ICT environments"¹³ (February 2017) aims to pave the way towards a common approach to security certification by examining five different critical business sectors. The ENISA publication "Recommendations on European Data Protection Certification"¹⁴ further identifies and analyses the challenges and opportunities of data protection certification mechanisms.

¹³ <https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments>

¹⁴ <https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification>

ECOSO's WG1 on "Standardisation, certification, labelling and supply chain management" has produced a publication "State-of-the-Art Syllabus"¹⁵ which lists all standards and specifications related to cybersecurity. We have attached a copy of this living document as ANNEX A to this deliverable.

The need to harmonize certification was a point raised at the cyberwatching.eu Concertation Meeting in April 2018. In addition, greater awareness around certification and what it means is also required as certification does not automatically mean that a company is "cybersecure".

4.1 Case Study: Cybersecurity certification in Spain by AEI

The Seal of Cybersecurity certification (AEI Seal of Cybersecurity for Organizations) is a certification scheme developed by the 'Spanish Cybersecurity Innovation Cluster' (AEI Ciberseguridad). It includes the technical and management security requirements that any organization should comply with to demonstrate it has implemented in a secure way physical and logical systems and measures to protect their assets against cyber threats.

The AEI Seal of Cybersecurity distinguishes three different types of organizations (A, B and C) that can be certified, depending on the access level to the information systems of other organizations through their products or services. This ranges from software developers to general cleaning services, lawyers or system integrators. The Seal has a special category for Critical Infrastructure operators, for which several specific technical and management requirements are applicable.

The standard includes technical and management requirements in the following categories:

- Communication protocols: configurations and implementations.
- Software development: web and desktop, distributed applications, etc.
- Data Protection: national regulations and European General Data Protection Regulation.
- Infrastructure: both physical and logical.
- Human Resources: experience and training.
- Suppliers: SLAs, Cybersecurity awareness, etc.
- Services: digital signature, cryptography, key storage, etc.

The requirements are listed in the Seal of Cybersecurity Industry Standard. This document is available upon request to any interested organization via AEI or any of the accredited consultant organizations.

4.1.1 Background

Spanish Cluster of Cybersecurity (AEI Ciberseguridad Association) detected that none of the certifications schemes available covered technical requirements for IT security at technical level, as well as at organizational level. Most of the existing certificates cover management processes only, missing the required level of detail in technical, specific aspects.

¹⁵ SOTA is available on the ECOSO web site at <https://www.ecs-org.eu/working-groups/wg1-standardisation-certification-labelling-and-supply-chain-management>

The aim of the seal is to complement existing certificates (e.g., ISO 27001) covering the lack of specific technical details.

4.1.2 Associated Evaluation Scheme and Governance

The Seal of Cybersecurity is a third-party certification scheme. It is owned by the Spanish Cluster of Cybersecurity (AEI Ciberseguridad Association), who is acting as the Accreditation Body and Certification Authority, guaranteeing the quality of the scheme and the different associated services. AEI Ciberseguridad is a national non-profit Cybersecurity and advanced technologies association with more than 80 private and public members.

4.1.3 Process

Any organization can freely implement the requirements of the certification scheme and ask for certification.

All information regarding the certification process is public available on the Association's website: https://www.aeiciberseguridad.es/index.php/Sello_AEI. This website also contains a list of (four) approved consultants delivering implementation services for the Seal of Cybersecurity, as well as a list of accredited audit/evaluation entities, for which currently (Feb 2018) only one organization is listed.

The website also offers information on the expected number of working days an audit will take. Depending on the size and complexity of the organization and its products/services, this may range from a couple of days to a few weeks. Estimates for maintenance evaluations and renewal evaluations are included as well.

4.1.4 Practice

AEI Ciberseguridad has grown from 40 members in 2015 to +80 by the end of 2017. The Seal of Cybersecurity was launched in June 2016. Since then, around 60 organizations –public or private- were certified or are in the process of being certified. This includes companies from Spain, Italy, Switzerland and France. The Seal has been implemented and certified in several sectors: financial, cloud providers, consultant companies, public sector contractors, data centers, etc.

Any consultant firm, member of the AEI Ciberseguridad association, can become a “approved consultant for the Seal of Cybersecurity”.

4.1.5 Formal Status

Currently there is no official mandate from the (Spanish) government that operators of critical infrastructure or other organizations must obtain the Cybersecurity Seal. However, some operators and companies are requesting the Seal to suppliers when issuing tenders. Therefore, the seal simplifies selecting and contracting certified suppliers in order to maintain the required cybersecurity along the whole supply chain.

Organizations that are certified under the Seal of Cybersecurity can show the Logo of the Seal in their communications, website, stationery, etc.

5 Analysis of the Policy, Legal and standard framework

The Cyber Act (Cybersecurity Package) represents the first step to address harmonization of the cybersecurity legislation across the European Union. With 28 different approaches to cybersecurity regulations currently, this presents a significant issue especially for SMEs that provide cybersecurity products or services.

5.1 External Online Survey

In order to obtain feedback from the previous and ongoing EU cybersecurity projects, cybersecurity users (public and private sectors), and cybersecurity products and services providers, a survey was prepared on the use and application, and implementation of cybersecurity standards. The results and the analysis of those results of this survey are included as part of this deliverable.

5.1.1 Focus of the survey

The focus of the survey was to benefit from the experiences of ongoing projects and efforts in understanding what is the current landscape in cybersecurity, including certification, harmonization and standardization as well as the range of products and services offered. Furthermore, as our intention is to insure that we don't "reinvent the wheel" we would like to benefit from the knowledge already developed and used within the European projects. We are genuinely grateful to those projects who have participated in the survey and in the discussions during our first Cyberwatching.eu concertation meeting.

5.1.2 Identification of stakeholders

In order to identify the group of stakeholders for the online survey, and the format and approach, a lengthy discussion took place at the Face-to-Face meeting in Brussels, on 22 November 2017. Several discussions followed by conference calls to fine-tune the survey and to ensure that it was brief, to the point and not more than 5 questions with a user friendly survey approach. The stakeholder group was identified as public sector, private sector (large and small and medium-sized enterprises), EU projects. Each partner made significant efforts to disseminate the survey to a widespread number of contacts, as follows:

- AEI and CITIC sent the survey to 424 subscribers to their cybersecurity-focused mailing lists,
- TRUST-IT to the Concertation list (\pm 43 contacts)
- TRUST-IT to the contacts from H2020 projects database, some \pm 150 project contacts
- TRUST-IT to the SEREN3 project network
- AEI to WP4 clusters, some 65 e-mails
- Digital SME through their social network
- Digital SME through recent conferences they attended
- CONCEPTIVITY to ECSO partners to \pm 230 companies via their newsletter
- CONCEPTIVITY to the Anastacia project (to the Coordinator for distribution to all the partners)
- CONCEPTIVITY to the ARMOUR project (to the Coordinator for distribution to all the partners)
- CONCEPTIVITY through LinkedIn, 7000 contacts

- CONCEPTIVITY to EOS - published in the EOS newsletter
- CONCEPTIVITY through personalized messages
- Cybersecurity.eu web site's portal contained the survey for three months

5.1.3 Dissemination of the survey

The online survey (ANNEX B) was disseminated by e-mail, social media (twitter, LinkedIn), and published on the cyberwatching.eu website in early December 2017 with the objective to solicit feedback from stakeholder communities on the current legal and policy framework in the European Union.

The survey was launched in December 2017. Due to an initially limited response, in January 2018, a second reminder was sent to the afore-mentioned contacts requesting that the survey be completed. A further effort was made by sending individual reminders on a personalized basis in February.

With the wide distribution as described above and several reminders to the large number of recipients of the survey communication, 33 replies were received from the following countries: Spain (18 replies), Switzerland (3), Italy (3), France (2), Austria, Finland, Greece, Ireland, Luxembourg, Mexico, UK (1). The replies covered 9 EU countries providing a response. The breakdown category of the responses was:

- 7 were from the industry,
- 6 SMEs,
- 6 non-for-profit,
- 4 governmental
- and 10 others were not specified.

The following sections summarize the responses received, results and analysis of answers to the questions set forth in the survey:

5.1.4 Analysis of Response to the Online Survey

Although the survey was completed by only 33 people, the responses provided an insight into understanding concerns in cybersecurity and related issues. The open-ended type questions allowed the end user to freely respond to the questions asked.

5.1.4.1 Survey Question No. 1

Question 1:

Has your project catalogued and/or tracked EU policy and regulatory elements related to cybersecurity?

- 76% (25 out of 33 submissions) responded affirmatively

This result is **important to note** as it indicates that cybersecurity is taken seriously and projects are tracking EU policy and regulatory information.

5.1.4.2 Survey Question No. 1A

Question 1A:
List which policies and regulatory elements have been tracked?

The most frequently tracked policies and regulations were:

- Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and related data privacy regulations and/or privacy protection directives
- NIS
- European Cybersecurity package

Given the impending implementation of GDPR on 9 May 2018, it is no surprise that this regulation is closely being tracked. The same applies to the European Cybersecurity package which was announced on 13 September 2017.

Examples of other regulations and standards which were cited of relevance to the projects are listed below:

Regulation/Standard	Title
Regulation (EU) N° 910/2014	Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation)
Regulation (EU) 2016/679	General Data Protection Regulation (GDPR)
	Directive on privacy and electronic communications (e-privacy directive)
Implementing Regulation (EU) N° 2016/68	Commission Implementing Regulation on common procedures and specifications necessary for the interconnection of electronic registers of driver cards
ISO/IEC 15408:2009	Security techniques -- Evaluation criteria for IT security
ISO/IEC 17030:2003	Conformity assessment – General requirements for third-party marks of conformity
ISO/IEC 17065:2012	Conformity assessment -- Requirements for bodies certifying products, processes and services
ISO/IEC 18045:2005	Security techniques -- Methodology for IT security evaluation

ISO/IEC 27000:2016	Security techniques -- Information security management systems -- Overview and vocabulary
ISO/IEC 27001:2013	Security techniques -- Information security management systems – Requirements
ISO/IEC 29100:2011	Security techniques -- Privacy framework
ISO/IEC 29190:2015	Security techniques -- Privacy capability assessment model
ISO/IEC 40500:2012	(W3C) Information technology -- W3C Web Content Accessibility Guidelines (WCAG)
ITU-T X1208 (01/2014)	A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies
ITU-T Y2060 (06/2012)	Overview of the Internet of things
ITU-T Y3051 (03/2017)	The basic principles of trusted environment in information and communication technology infrastructure
ITU-T Y3052 (03/2017)	Overview of trust provisioning for information and communication technology infrastructures and services
ITU-T Y4050 (07/2012)	Terms and definitions for the Internet of things
ITU-T Y4100 (06/2014)	Common requirements of the Internet of Things
ETSI TR 103 304	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services
ETSI TR 103 305	CYBER; Critical Security Controls for Effective Cyber Defence
NIST SP 800-53 R4	Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-122	Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
	Swiss Federal Act on Data Protection (FADP)
	Swiss Ordinance on Data Protection Certification
	Code for drug use on humans

Table 1: Examples from the Online survey of regulations cited as relevant

5.1.4.3 Survey Question No. 1B

Question 1B:

How are they (policies and regulatory elements) relevant for what your project is doing?

The results concerning the relevance of policies and the regulatory framework to projects indicated that overall cybersecurity was “highly relevant”, “very relevant”, or “important” to a project, that **compliance and building trust** in order to serve members was a priority. On the other hand, identity management and protecting the personal data stored in IT systems is crucial to preventing misuse of data, fraud and cybersecurity breaches. **Cybersecurity** (encompassing a regulatory framework, compliance and certification) would be the foundation for **privacy and trust**.

Additional comments specifically related to the projects were:

- “In the case of ARIES project <http://www.aries-project.eu/> affects the solution to generate virtual identities and how they can be managed in the border and access solution for boarding in airport scenarios. In the case of ARMOUR and ANASTACIA, the Cybersecurity Act affects the approach to the creation of a EU certification framework for ICT security”
- “Very relevant, this is one of the tasks of the CANVAS project (see www.canvas-project.eu)”
- “The project aim is to build a cyber-security protection infrastructure. Therefore, aspects related to cyber-security assume a crucial role.”
- “Inclusion in the overall ANASTACIA project framework to secure complex IoT and CPS architectures.”
- “SECURITYMADEIN.LU covers all aspects of cybersecurity and/or data protection (which is kind of the same area anyway) from reactive services like incident response, CERT, etc. ; organisational aspects: risk mgmt, security policy and certification to human awareness, skills and competences.”
- “Policies are fundamental in projects related to cyber security as sensitive and private data are often treated, we need policies to protect data used in IT systems.”
- “They are a fundamental basis for our activities. We discuss in the CSP (PPP between Austrian Government and Critical Infrastructure Providers) about concrete measures for national implementation.”

5.1.4.4 Survey Question No. 2

Question 2:

Are there upcoming policy and regulatory elements that are of concern to the partners in your project?

- 58% (19 responded affirmatively)
- 42% (14 responded negatively)

5.1.4.5 Survey Question No. 2A

Question 2A:
Indicate which elements are of concern.

The upcoming areas of concern were GDPR, an EU-wide cybersecurity legislation, compliance and certification, security standards, lack of training, misuse of digital signature and other areas included health, transport, communications and ethics.

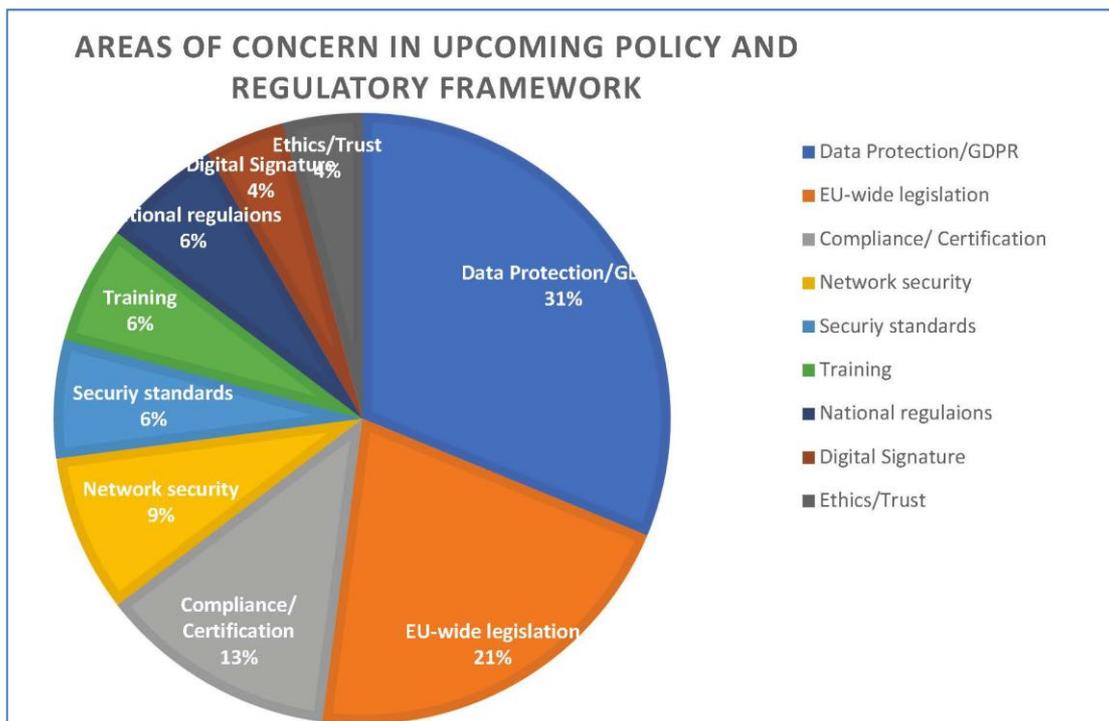


Figure 4: Upcoming areas of concern in cyber security

Data protection/GDPR is clearly a primary concern given the implementation of the upcoming GDPR on 9 May 2018. Following the Communication on 13 September 2017, by the European Commission and the High Representative to the European Parliament and the Council (JOIN(2017) 450 final), bearing the title “Resilience, Deterrence and Defence: Building strong cybersecurity for the EU” introducing an a comprehensive plan to improve cybersecurity throughout the EU, it is clear that an EU-wide legislation is in demand. The fact that compliance and certification follow as a concern is because there should be a mechanism to enforce the regulation and, therefore, professional competencies in this respect are crucial.

Some pertinent comments with respect to upcoming concerns were:

- “Service providers must adhere to our commitments regarding compliance. Additionally, our customers demand us to be compliant with the regulatory requirements.”
- “We participate in several projects and proposals that need good knowledge on the recent policy and regulations in the area of ICT and critical infrastructures.”

- “Lack of training for employees and companies in prevention and threats in continuous advance.”
- “For example, regulation of our profession. Spain needs to regulate the exercise of the profession of a computer science engineer. Also, the role of data responsible in the organizations, as the policies from EU have changed, and in Spain there must be adapted to these EU policies. Moreover, some other concerns of regulation like bitcoins, smart cities, etc.”
 “ethical aspects of apps that allow unintended disclosure/access to more info than is necessary for a transaction starting with eIDs”

5.1.4.6 Survey Question No. 2B

Question 2B:
 Why are they of concern to you?

In summary, the response was that the following main areas were a priority: compliance, trust, security, harmonization, ethics, costs related to non-compliance.

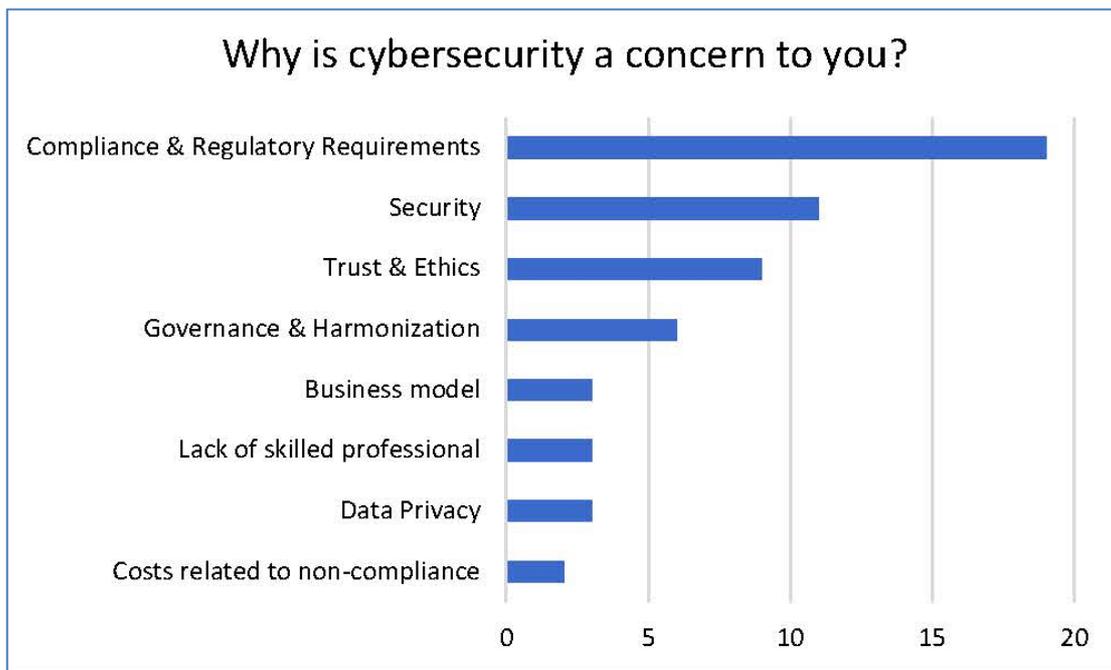


Figure 5: Response highlighting concerns regarding cyber security

Whilst compliance to regulatory requirements was the main theme, the underlying concern expressed was trust in ICT products and IoT. People feel vulnerable if they cannot trust the ICT products put at their disposal. Therefore, governance and harmonization combined with certification and compliance play an important part. Some of the concerns expressed are quoted below:

- “Trust systems to fit into the regulations are essential on the market domains that we are working on.”
- “We need to ensure our partners comply (self-assessments, 2nd and 3rd party audits) while we proof our end-to-end compliance (internal and external audits, regulation authority inspections).”

- “Missing harmonization across regulatory topics, Missing baseline security requirements”
- “Because cybersecurity is a problem that affects you and can affect everyone including me”
- “security, privacy, ethical use and limiting linkage are essential to sustaining public trust in using eIDs across all potential e-activities. Our project ARIES in which we are a partner has highlighted many areas where citizens have concerns. Too often it is assumed that governments are not trusted. Increasingly, there is scepticism from citizens about the commercial intentions of industry and suppliers mining (covertly) their data for imprcise purposes, outsourcing and public private partnerships that elude EU control.”
- “The concern to the existence of our profession. We would like that our politicians take care of our role in the society. In Spain, everyone can do "IT" tasks. Software is placed everywhere, and there are places affected by critical security or privacy aspects, where regulatory aspects should have been put in place some years ago.”

5.1.4.7 Survey Question 3

Question 3:
 Given that regulatory efforts will continue in cybersecurity and data protection, can you list the areas which you believe should be the focus (in the order of priority)?

The response to this question raised many interesting and diverse areas requiring attention. The most frequent concerns are indicated below in Figure 6 below.

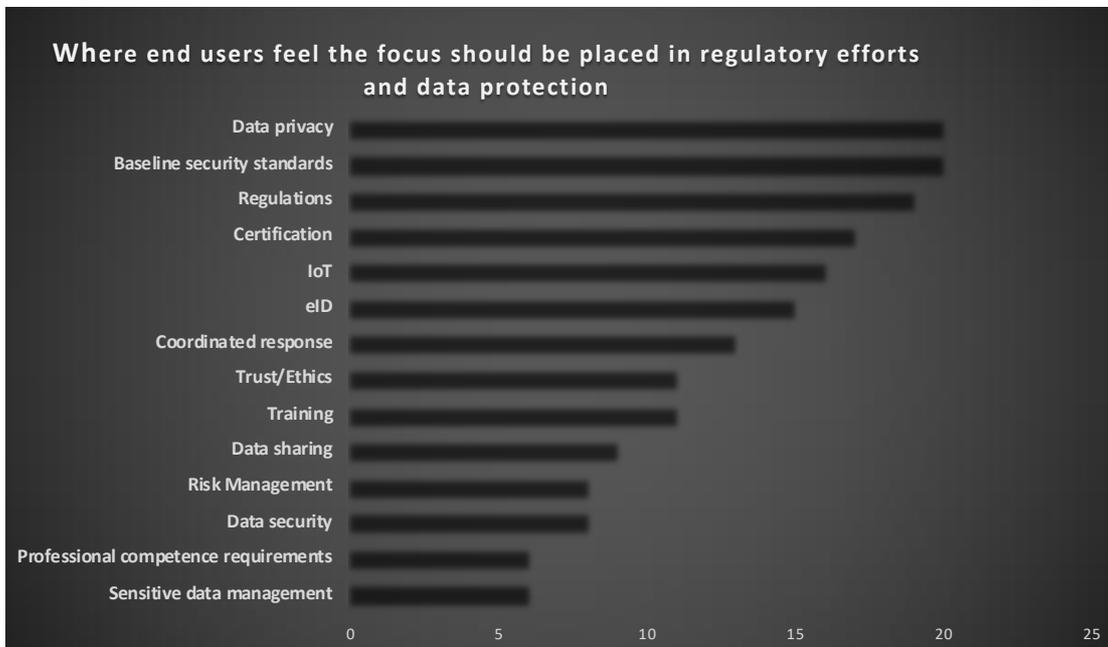


Figure 6: Where end users feel focus should be placed in regulator efforts in cybersecurity

From this question, it was revealed that:

- as an individual or an owner of data, data privacy, data security and data sharing were of concern.
- as a user of IoT, trust in devices and protection of network infrastructure were a priority.
- as an owner of data and as a user of IoT, it was clear that the framework to regulate the underlying concerns was necessary, specifically to address data privacy, enforce baseline security standards, including compliance, certification, best practices and guidelines, training, which required professional competencies and not just a passion for the subject matter, in order to enable trust and a secure environment.
- as a concerned citizen, a coordinated response to mitigate the impact of cyber attacks and for the better protection of Europe as a whole was necessary.

Poignant quotes from the survey:

“Coordinate actions in each country, and between each at the European level, by defining best practices, fixing responsibilities, improving the organization and data sharing, providing the necessary budget, and giving the organisations legal power to impose proactive actions.”

“We consider most important the introduction of baseline security standards for every kind of ICT that is produced, delivered, procured or used in Europe, especially considering the increasing number of cheap IoT devices that go into broad usage without any minimum security.”

Some interesting quotes in this respect were:

- “We consider most important the introduction of baseline security standards for every kind of ICT that is produced, delivered, procured or used in Europe, especially considering the increasing number of cheap IoT devices that go into broad usage without any minimum security.”
- “Trust certification schemes for devices and applications. Training courses on the regulations and their technical adaptation
- “Certification of devices”
- “Having only one framework to work with, well defined and common to all EU members”
- “Knowledge of the person that is involved in cybersecurity. Not only a course or passion on computer science is a guarantee for secure a system. A minimum requirement on a university degree and a professional habilitation should be taken into account”
- “Coordinate actions in each country, and between each at the European level, by defining best practices, fixing responsibilities, improving the organisation and data sharing, providing the necessary budget, and giving the organisations legal power to impose proactive actions.”

5.1.4.8 Survey Question 4

Question 4:
 In your opinion, how can harmonization of the policy and regulatory requirements be achieved?

In summary, a combination of stakeholder engagement with EU leadership using compliance and certification schemes were expressed in order to achieve cybersecurity. The main outcomes are presented below:

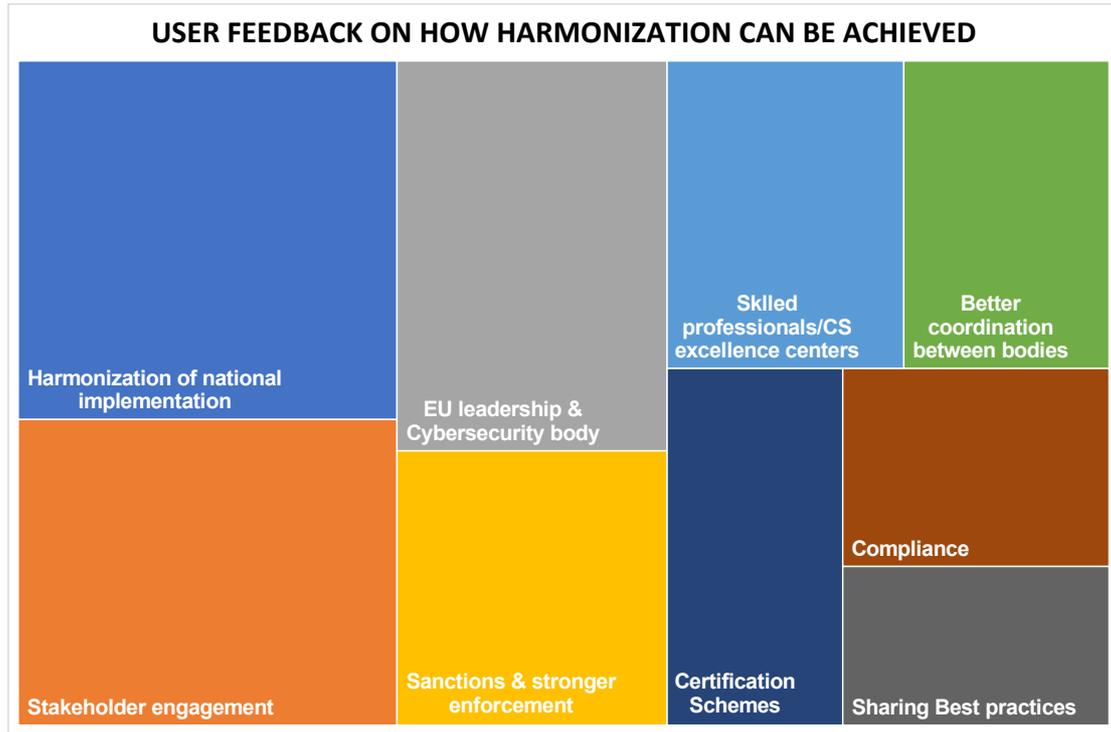


Figure 7: User feedback on how harmonization can be achieved

Harmonization is clearly necessary but so is stakeholder engagement. Without stakeholder engagement from industry and the public sector, it is difficult to move forward. The EU leadership is necessary to act as the umbrella managing better coordination between current bodies and to implement cybersecurity across borders. With a clear governance, a stronger enforcement mechanism should be put in place to contain compliance to certification, raising awareness, and professional capacity.

Some interesting comments from this question are quoted below:

- “It is challenging, policy and regulation makers must achieve a strong stakeholder engagement across verticals”
- “There needs to be a dedicated European body who assures coordination and harmonization of legal and regulatory matters with regards to cybersecurity and data protection.”
- “leadership from EU is crucial, and EU setting standards in line with EU values (rather than what international/US corporations want). EU consultation with industry and citizens is important and should be ongoing BUT clear

political vision and determination to set an EU model is vital. Openness and accountability about what the EU wants to do, why and how. The role of the EU data protection supervisor is crucial, not just from the point of view of review after something has happened but the EDPS should be consulted and heeded at the point new algorithms/apps are likely to be developed. Industry needs training in ethics.”

- “Input from all stakeholders shall be gathered and considered.”
- “Set up of international fora and joint working group, with strong participation of industry and device manufacturer to ensure compliance and interoperability of products.”
- “Through legislation and certification”
- “Two main areas of work 1) Better coordination of the different fora, for example actually ENISA, JRC, ECSC, AIOTI are working in parallel and in some cases with different views. It is necessary to better envision a EU strategy. 2) The creation of excellence center at national/regional level that coordinate and provide support to SMEs in the management of cybersecurity”
- “Preparing candidate European cybersecurity certification schemes for ICT products and services. Compiling and publishing guidelines and developing good practices concerning the cybersecurity requirements of ICT products and services, in cooperation with national certification supervisory authorities and the industry.”
- “Especially cybersecurity and/or data protection are areas that are very well suited to be harmonized, especially inter-sector. Indeed, in many of today's sectoral regulations (e.g. banking, telecom, etc.) one can identify cybersecurity relevant aspects. By defining a common and underlying framework of requirements specific for cyber and independent of sector-specificities, a huge harmonization effort can be achieved”
- “The policy and regulatory requirements will be achieved after we can ensure all the communication processes are supervised.”
- “Please, push Spain politicians to comply these requirements: a software system that controls life or security or important data of persons, must be designed, implemented and assured by experts in this area, not by persons who are only passionate of computer science, or that have done a course. There must be a regulation of which persons can do these tasks, the same if someone wants to be a medician or architect, there must be a guarantee for the consumer.”
- “Preparing candidate European cybersecurity certification schemes for ICT products and services. Compiling and publishing guidelines and developing good practices concerning the cybersecurity requirements of ICT products and services, in cooperation with national certification supervisory authorities and the industry.”

5.1.4.9 Survey Question 5

Question 5:

5 - What role could certification play in implementing policy and regulatory requirements?

The role of certification was expressed overall as a “main role”, “very relevant”, “essential”, “important” and “key”. The response from the survey provided : regulatory framework, promoting trust and certification mechanism

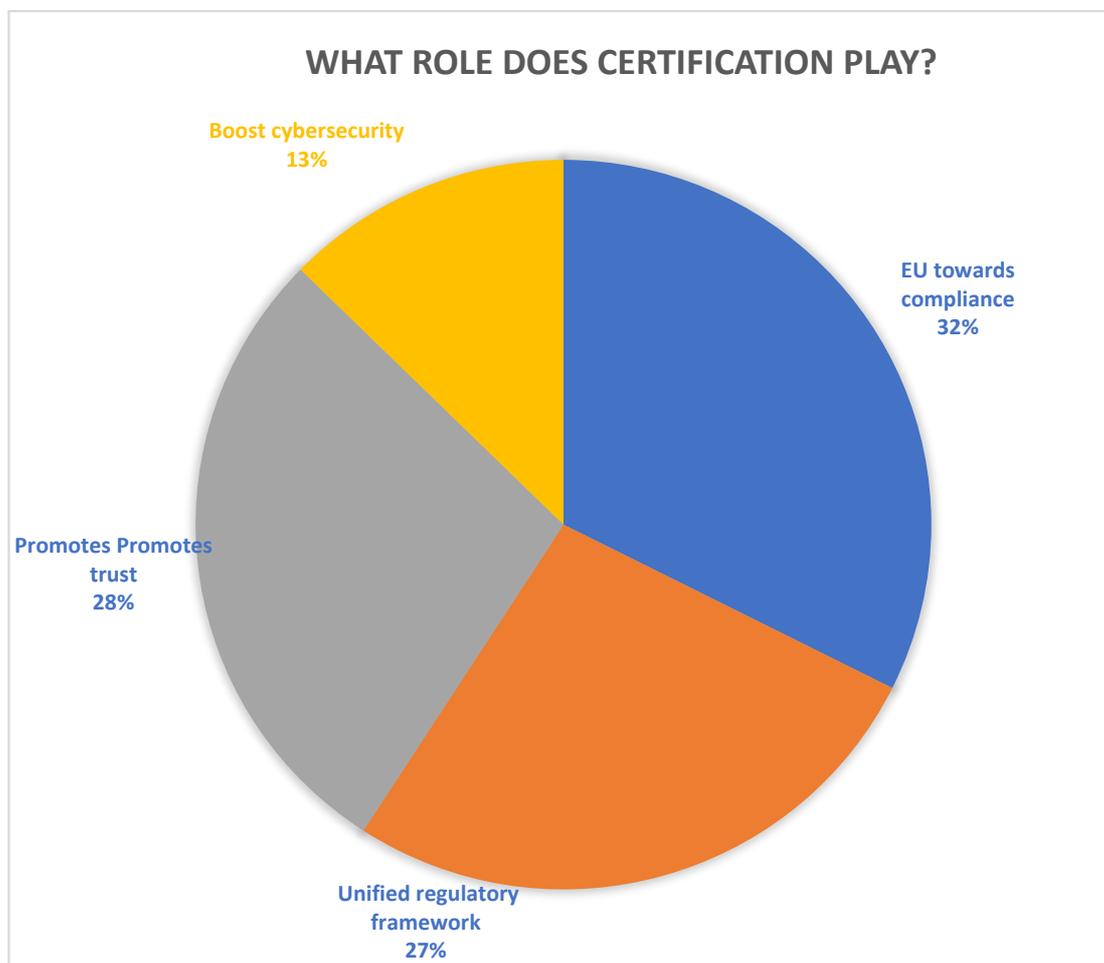


Figure 8: User feedback on what role of certification in implementing policy and regulatory requirements

5.1.4.9.1 Regulatory Framework

With respect to the policy and regulatory requirements, implementing certification would provide several advantages as follows:

- a unified approach to cybersecurity in Europe
- a rise in the expected level of maturity for regulatory requirements

- a harmonized approach to normative requirements in Europe
- a common reference

5.1.4.9.2 EU towards Compliance

Certification would lead to compliance at the European. A uniform or common reference certification scheme would be necessary in order to avoid a proliferation of certificates. Further, skilled ICT professions were necessary and also skilled and independent verifiers.

5.1.4.9.3 Secure environment promotes Trust

By implementing a certification mechanism according to the regulations in place, the industry would provide ICT products which end users could trust and therefore improve the level of cyber security.

5.1.4.9.4 Boost cybersecurity in Europe

The goal to reach a cybersecure Europe could be attained by compliance to the policies and regulations set forth at the European level. Certification would be the gateway to producing a level of cybersecurity as long as the mechanism applied is standard and the certification scheme is

Interesting comments in response to question 5 of the survey were

- “Key role to create awareness, encourage and boost cybersecurity adoption.”
- “Certification can help raising the expected level of maturity for regulatory requirements. Being a market oriented and voluntary process, a huge effort in harmonization and communication is needed to avoid proliferation of certificates, incompatibilities and confusion among consumers.”
- “An important role, especially with regards to baseline security standards. As a first step a self-certification could be used, but mid-long term only certified ICT should be allowed to use in Europe. This affects the whole supply chain.”
- “Certification will be key in order to provide trust to the Digital Single market and the end users. Also it is key the support to the SME in the way to increase their policies and procedures.”
- “It could play a very important role because by setting standards for certification, it would ensure that all infrastructures are aligned on the same implementation and use the same judgment metric.”
“Pivotal role - as soon as a certification framework is issues, manufacturers will start align to it in order to keep/maintain market shares, finally improving the level of cybersecurity.”
- “certification is only as good as the independence of the verifier, regular independent audits and compliance checks. This must be stringent and not tick box. Given the speed with which apps develop and new processes come to the fore, an annual certification is needed if citizens are to trust suppliers and users and if industry is to trust each other. Governments must not be lured into buying obsolete systems so needed training and expertise inhouse as well, may be via special EU level updating regularly”

6 Research & Innovation

Cybersecurity is critical to both our prosperity, security and public safety. Malicious cyber activities not only threaten our economies and the drive to the Digital Single Market, but also the very functioning of our democracies, our freedoms and our values. EU cyber preparedness is therefore central and needs a collective and wide-ranging approach.

The precursor FP7 programme and the current Horizon 2020 programme form the basis of the Research & Innovation Ecosystem, recognizing that there are many projects and consortia that are involved.

The existing projects in the European research and innovation ecosystem have been identified and classified within WP2 according to their content and domain and as such are part of the group that we had identified as targets for the survey. The projects form the first version of the Cyberwatching.eu R&I CS&P observatory¹⁶.

Furthermore, these projects were also invited to the 1st Cyberwatching.eu Concertation Meeting held in Brussels on 26 April 2018. A catalogue of service offers¹⁷ was created based on service offers provided by 48 projects, mainly in the EC's Unit H1 Cybersecurity and Privacy.

This catalogue demonstrates how European research priorities have adapted to a fast-moving and rapidly evolving threat landscape, which is increasingly in the public eye. Research and Innovation (R&I) projects have spearheaded the development of novel architectures and technologies across the EU & Associated Countries (ACs) to help protect our European Digital Society against cybersecurity & privacy threats. The offers in the catalogue give us a clear understanding of how projects are assessing and addressing end-user needs and the status of developments.

The catalogue is also the result of the first step in cyberwatching.eu's comprehensive observation and clustering of national and pan-European R&I initiatives. Our goal is to provide a cross-pollination platform of both non-technical, policy, experiences and best practice findings, as well as deeper technical specifics that concentrate on specific issues in smaller and more tightly focused groups.

The projects contained in the service offer catalogue cover a number of fields related to the themes of this deliverable and we feature a select number of those in this document where relevant.

6.1 Clustering R&I projects

Work Package 2 will provide a series of deliverables (D2.2, 2.5, 2.7 Technology radar reports) in which CS&P projects will be mapped according to a pre-defined taxonomy outlined in D2.1 Cybersecurity and Privacy ecosystem model report.

The taxonomy identified in D2.1 has been used to cluster 150 projects based on three high-level definitions. The clustering has been published on the R&I CS&P observatory and the catalogue of services. This represents the first level of clustering to be carried out by the project based on three high-level definitions¹⁸.

¹⁶ <https://www.cyberwatching.eu/observatory>

¹⁷ <https://www.cyberwatching.eu/services/catalogue-of-services>

¹⁸ *Foundational technical methods & risk management for trustworthy systems in cybersecurity and privacy; Applications and user-oriented services to support cybersecurity*

The first cyberwatching.eu Concertation meeting in April 2018, saw clusters of projects on these come together to identify R&I challenges, cross cutting themes and collaboration opportunities.

6.1.1 Applications and user-oriented services

This first cluster includes projects focusing on the development of technologies that are directly associated with cybersecurity capabilities or features and methods by which the confidence in the technical capabilities of a system may be validated.

The following projects are included in this cluster and took part in the discussions at the Concertation meeting.



Figure 9: List of projects in Breakout Session 1

The complete Service Offers of the projects which participated in Breakout Session 1 are available on the [cyberwatching.eu website here](http://cyberwatching.eu).

All the presentations from the projects which participated in Breakout Session 1 are available on the [cyberwatching.eu website here](http://cyberwatching.eu).

Top R&I challenges
<ol style="list-style-type: none"> 1. Business modelling and commercialisation 2. Context integration – integrating a few security products at the same time and together 3. Scalability - when there are overlapping solutions, projects to resolve similar problems but using different solutions and standards 4. Standardisation and certification. Standardization takes time, to see the maturity of the solution also takes time. The new way of communication between devices makes it even more complicated. 5. Users’ data protection and legal compliance – this has multiple dimensions, from the service-provider to the user. Frequently, one operates in a controlled testing environment so you do not see the real environment 6. Supporting SMEs in cybersecurity and privacy – this is very difficult for SMEs

The top cross-cutting themes
<ol style="list-style-type: none"> 1. e-Health (KONFIDO; SHIELD) 2. Security for SMEs (SMESEC; FORTIKA)

and privacy; Policy, governance, ethics, trust, and usability, human aspects of cyber security & privacy

3. Trust assurance for Critical Infrastructures (CITADEL; CIPSEC; SCOTT)
4. Anonymous access (ReCred; CREDENTIALS)
5. Open Innovation Frameworks

Top new collaboration opportunities and new ideas

1. Identity management and network communication anonymisation
2. Improvement of Users' awareness of data use

6.1.2 Foundational technical methods and risk management for trustworthy systems

This second cluster includes projects focusing on specific capabilities or services which directly interact with system users and are developed with capabilities that are directly about how to improve the inherent capabilities and user experiences of cybersecurity and privacy in consumed services.

The following projects are included in this cluster and took part in the discussions at the Concertation meeting.



Figure 10: List of projects in Breakout Session 2

The complete Service Offers of the projects which participated in Breakout Session 2 are available on the [cyberwatching.eu website here](https://www.cyberwatching.eu).

All the presentations from the projects which participated in Breakout Session 2 are available on the [cyberwatching.eu website here](https://www.cyberwatching.eu).

Top R&I challenges	
Group 1	Group 2
<ol style="list-style-type: none"> 1. Usability of products and services 2. Interoperability on top of heterogeneous landscapes 3. Package results (to make it digestible for industry) 4. Security protocol re-engineering for constrained devices 5. Unattended devices and services 6. Landscape too fragmented 	<ol style="list-style-type: none"> 1. Dynamic risk assessment (impact and attack) probability on impact 2. Data Governance / Privacy preserving / Data Sharing (Trust) 3. CTI tsunami (OSINT) 4. Get crypto ready for post-Quantum 5. Threat models for emerging infrastructures

--	--

The top cross-cutting themes	
Group 1	Group 2
<ol style="list-style-type: none"> 1. Features sell, not security → the time to market problem 2. GDPR compliance for EC projects 3. Privacy and GDPR compliance built into SW design 4. Increase maturity of SW process towards true engineering 5. Digitisation & equal opportunities for rural areas 6. Device security and “European sovereignty” 	<ol style="list-style-type: none"> 1. Risk Models 2. Governance 3. CTI sharing

Top new collaboration opportunities and new ideas	
Group 1	Group 2
<ol style="list-style-type: none"> 1. How to use project results – “project snippets” 2. European landscape for projects 3. Open Source and IPR collaboration 4. Make the Cybersecurity atlas an online tool 	<ol style="list-style-type: none"> 1. Sharing CTI and risk models between projects 2. Need to better facilitate the collaboration between business and academia to synergise research e.g. development of Impact Models 3. Open labs & tools 4. Education and training/ raising awareness 5. Develop database of best practises

6.1.3 Policy, governance, ethics, human aspects, trust and usability

This third cluster includes projects focusing on aspects of cyber security that are overwhelmingly driven by the human interaction, understanding and dependency on how secure systems are or have been designed to be.

The following projects are included in this cluster and took part in the discussions at the Concertation meeting.



Figure 11: List of projects in Breakout Session 2

The complete Service Offers of the projects which participated in Breakout Session 2 are available on the [cyberwatching.eu website here](http://cyberwatching.eu).

All the presentations from the projects which participated in Breakout Session 3 are available on the [cyberwatching.eu website here](http://cyberwatching.eu).

Top R&I challenges
<ol style="list-style-type: none"> 1) Certification 2) Education & Awareness 3) Social & Ethical (social pressure) 4) European Values (how to address these) 5) Global Cooperation

Further consideration
<ol style="list-style-type: none"> 1. Everyone does his own risk analysis (one objective of trust) with society pressures 2. Usability is a key factor in the personal risk analysis 3. Security is also a matter of perception 4. It is easy to trust a large company with many users 5. 28 EU Member States – this presents a challenge of languages 6. Harmonisation is key

6.2 Snapshot of the First cyberwatching.eu Concertation meeting

A key output of cyberwatching.eu is four Concertation Meetings to be convened during the life time of the project.

The first Concertation Meeting was held in Brussels on 26 April 2018.

The meeting took place later than foreseen; therefore, in view of the timing of the meeting, submission of this deliverable D3.2, due in M12, was delayed by one month to M13.



6.2.1 Objectives

As explained in D3.1 (“Concertation Plan”), the overarching objective of cyberwatching.eu is to reduce barriers to CS&P across the EU. The aim of this first meeting was to showcase ongoing EU projects in the area of cybersecurity, what is being done, what services are offered, how this affects the lives of end users, and what challenges and opportunities are available. The approach of this first Concertation Event was to

- make the event a dynamic and interactive platform,
- bring together projects in the domain of cybersecurity so that they collaborate, interact and generate synergies between them
- open an opportunity for networking,
- provide a platform for clustering and convergence between projects on common themes and challenges

6.2.2 Participants

Whilst the event was open to all, i.e., to a variety of stakeholders, from SMEs to R&I teams, public sector organisations and policy makers, the main focus was on the EU projects (involved in some way or another in cybersecurity) and bringing them together so that common themes and challenges could be discussed. A total of 74 registered participants included:

- 40 projects (although one project did not present itself at the meeting)
- EU officials
- representatives of the following companies:
- partners in cybersecurity.eu

In addition, for this first event, a hard copy of the **R&I Catalogue of Services** of projects was compiled and distributed to each participant. As stated earlier in this report, each project provided a service offer with short and attractive texts covering what user needs the project services could solve or how it would improve or is improving the lives of end-users.

The detailed agenda of the Concertation Meeting is attached as ANNEX B and the approach to the Concertation Meeting is available in D3.1. A summary of the main agenda is provided in Annex C.

6.2.3 Overall Feedback

The breakout sessions and panel discussions were lively and presented the opportunity to discuss areas of concern. Some of the main concerns were emphasized in the following areas and which have been covered in separate sections of this document:

- GDPR and Certification, see section 2.7
- A skilled workforce is essential, see section 3.8
- An SME perspective on cybersecurity, skills, certification, see section 3.9

7 Conclusions

The first results are very promising, first from the input and feedback coming from the survey and second from the actual concertation event. The opportunity for information sharing and exchange presents an important element in ensuring that the results from projects are capitalized upon and not just lost once the project has ended. The key element of being able to learn from what has come before is very significant in this context with project results being at the core of the sharing process at the concertation meetings. The feedback from the meeting was excellent and the summarized results can also be seen here in this deliverable.

The next steps are to build upon the first concertation event, as there are two further events planned during the life of this project. There were certain “no shows” of projects who had promised to attend and present, so our intention would be to have even a better attendance than the first event. Furthermore, we have learned from the challenges of the first survey in that we will need to spread the net very wide even from the start in order to get a reasonable number of responses to our survey request.

Finally, we would like to say a big “thank you” to all of the projects and companies and persons who attended the 1st Concertation Event making it a resounding success, with a special thank you to the European Commission for their participation and discussions. Another big “thank you” goes out to those who contributed to responding to the survey as this was not only enlightening, but actually confirmed most of the current wisdom and knowledge concerning cybersecurity.

Again, we look forward to the next concertation events in the near future.

ANNEX A. ECSO “SOTA” – STATE-OF-THE-ART SYLLABUS (DECEMBER 2017)

ECSO State of the Art Syllabus – Overview of existing Cybersecurity standards and certification schemes v2 [publicly available on the ECSO website](#).

ANNEX B. ONLINE SURVEY - CYBER SECURITY POLICY AND REGULATORY FRAMEWORK



[LOGIN \(/USER/LOGIN\)](#)

[REGISTER \(/USER/REGISTER\)](#)



SURVEY ON CYBER SECURITY POLICY AND REGULATORY FRAMEWORK IN THE EU & ASSOCIATED COUNTRIES

SURVEY TO GATHER INFORMATION FROM THE PERSPECTIVE OF SUPPLY & DEMAND

REGARDING CYBER SECURITY POLICY AND REGULATORY FRAMEWORK

IN THE EUROPEAN UNION & ASSOCIATED COUNTRIES

This survey is to gather information from the perspective of supply (provider/regulator) and demand (consumer) regarding the cyber security policy and regulatory framework in the European Union and Associated Countries. Your contribution is important and necessary as it will contribute to analysing the EU policy framework with the objective to provide recommendations to protect public and private organisations from cyber attacks. These recommendations may result in supporting efforts to develop new EC Communications, new directives and even assist in providing input to implementing regulations in cybersecurity, data protection and data privacy. At the First Concertation Meeting to be held in Spring next year, the results of this survey will be shared. A public deliverable containing the results of this survey will be published in 2018.

By participating in this survey, you will be able to obtain early access to the results of the survey at the First Concertation Meeting to be held in Spring next 2018.
Please note that all fields marked with * are mandatory.

Please note that all fields marked with * are mandatory.

Annex B, page 2

First Name *
<input type="text"/>
Last Name *
<input type="text"/>
Title *
<input type="text"/>
Company/Organization *
<input type="text"/>
Company/Organisation type * <input type="text" value="- Select -"/>
Country * <input type="text" value="- Select -"/>
Please indicate the EC funded project you represent *
<input type="text"/>
Select your geographical scope of operations *
<input type="text" value="- Select -"/>
E-mail (optional)
<input type="text"/>
Website
<input type="text"/>
1 - Has your project catalogued and/or tracked EU policy and regulatory elements related to cyber security? *
<input type="radio"/> Yes
<input type="radio"/> No
2 - Are there upcoming policy and regulatory elements that are of concern to the partners in your project? *
<input type="radio"/> Yes
<input type="radio"/> No
Thank you for accepting cookies
<small>You can now hide this message or find out more about cookies.</small>
<input type="button" value="Hide"/> <input type="button" value="More info"/>

3 - Given that regulatory efforts will continue in cybersecurity and data protection, can you list the areas which you believe should be the focus (in the order of priority)? *

4 - In your opinion, how can harmonization of the policy and regulatory requirements be achieved? *

5 - What role could certification play in implementing policy and regulatory requirements? *

Please take the time to read and review the cyberwatching.eu web platform Terms and Conditions of Use (<https://www.cyberwatching.eu/terms-of-use>) and Privacy Policy (<https://www.cyberwatching.eu/privacy-policy>).

Accept Privacy Policy and Terms and Conditions of Use *

Having read and understood the Privacy Policy above, I provide my free, specific and informed consent to the processing of personal data described under section c) of Purposes of the processing and legal basis and under section d) of Purposes of the processing and legal basis.

Yes

No

Sign up for our newsletter *

Yes

No

Submit

ANNEX C. 1ST CONCERTATION MEETING AGENDA



The First cyberwatching.eu Concertation Meeting Cybersecurity and Privacy Services Home-grown in Europe

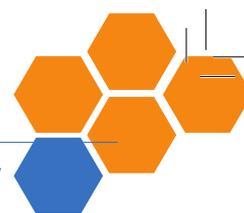
26 April 2018 | Brussels, Belgium

The Agenda of the day

10:00 – 10:30	Registration & Networking Coffee
10:30 – 10:50	<p>Introduction Chair: Nicholas Ferguson, Trust-IT Services & Cyberwatching.eu Coordinator</p> <ul style="list-style-type: none"> » Welcome and a perspective from the EC - Martin Ubelhor, Head of Sector, European Commission » Cyberwatching.eu overview and objectives of the meeting - Nicholas Ferguson, Trust-IT Services
10:50 – 11:40	<p>Piecing together the Cybersecurity & Privacy ecosystem Chair - David Wallom, University of Oxford</p> <p>An introduction on the Cybersecurity Atlas - Nineta Polemi, European Commission</p> <ul style="list-style-type: none"> » Roberto Cascella, ECSO » Afonso Ferreira, CNRS » Helmut Fallman, Fabasoft » Andrei Kelemen, Cluj IT <p>Introduction to the cluster break-out sessions - David Wallom, University of Oxford</p>
11:40 – 12:00	Quick networking break
12:00 – 13:30	<p>Breakout Sessions - Lightning talks and Top fives</p> <p>Room: Studio 1 Break-out 1 – Applications & user-oriented services Chair: Bharadwaj Pulugundla, Verizon & Re-CRED Representatives from: CITADEL - CREDENTIAL - CIPSEC - FORTIKA - KONFIDO - PRIVACY FLAG - Re-CRED - SCOTT - SHIELD - SMESEC - SpeechXRays - YAKSHA</p> <p>Room: Studio 4 (plenary room) Break-out 2 – Foundational technical methods and risk management for trustworthy systems Chair: Brian Lee, Athlone IT & PROTECTIVE Representatives from: ANASTACIA - ATENA - C3ISP - CYBECO - DiSIEM - FENTEC - GHOST - HERMENEUT - PRISMACLOUD - PROTECTIVE - REASSURE - SAINT - SPECIAL - VESSEDIA</p>

www.cyberwatching.eu | [@cyberwatchingeu](https://twitter.com/cyberwatchingeu) | www.linkedin.com/in/cyber-watching

Annex C, page 2



Room: Studio 5	Break-out 3 – Policy, governance, ethics, human aspects, trust and usability Chair: Linda Strick , Fraunhofer FOKUS & EU-SEC Representatives from: PROTASIS - AEGIS - CANVAS - certMILS - COMPACT - CS-AWARE - DOGANA - E-SIDES - EU-SEC - EUNITY - FutureTrust - LIGHTTest - TRUESSEC.eu
13:30 – 14:30	Networking Lunch at Restaurant Midtown Grill
14:30 – 14:50	ECSC WG6 Strategic Research & Innovation Agenda – Identifying the future R&I landscape and future priorities - Fabio Martinelli , National Research Council of Italy
14:50 – 15:30	Reporting back to base on Top fives – Interactive panel discussion on cross-cutting themes and future collaboration opportunities Chair: David Wallom , University of Oxford Break-out 1 – Applications & user-oriented services Chair: Bharadwaj Pulugundla , Verizon & Re-CRED Break-out 2 – Foundational technical methods and risk management for trustworthy systems Chair: Brian Lee , Athlone IT & PROTECTIVE Break-out 3 – Policy, governance, ethics, human aspects, trust and usability Chair: Linda Strick , Fraunhofer FOKUS & EU-SEC Opportunities for projects to collaborate with EU Cybersecurity clusters - Jorkin Garatea , GAIA
15:30 – 16:10	International policy and standards evolution Chair – Mark Miller , CPT & Cyberwatching.eu » Gregory Blanc, IMT & EUNITY » Yolanda Ursa, Inmark Europe & AEGIS » Helmut Fallman, Fabasoft » Sebastiano Tofaletti, Digital SME Alliance » Poalo Balboni, ICT Legal Consulting
16:10 – 16:30	Future Cybersecurity & privacy challenges and funding opportunities Nineta Polemi , European Commission
16:30	Meeting Close

www.cyberwatching.eu | [@cyberwatchingeu](https://twitter.com/cyberwatchingeu) | www.linkedin.com/in/cyber-watching

- An **Introduction to cyberwatching.eu project and the Concertation Meeting** by Nicholas Ferguson (Trust-IT Services & Cyberwatching.eu Coordinator)
- A **Welcome address and a perspective from the EC** by Martin Ubelhor (Head of Sector, European Commission) who underlined the immense opportunity of the Concertation meeting to bridge the gap in learning about other projects, learning from each other, reaching out to other projects and continuing to support cybersecurity in years to come
- A panel session entitled “**Piercing together the Cybersecurity & Privacy ecosystem**” chaired by David Wallom (University of Oxford & Cyberwatching.eu partner) who used three high level areas to describe the ecosystem:
 - tools and services,
 - foundational technical methods and risk management and
 - social and policy matters
- “**An introduction on the Cybersecurity Atlas**” by Nineta Polemi (European Commission).

Between 12h00 to 13h30, there were three break-out sessions with thought provoking sessions, specifically:

1. Applications and user-oriented services
2. Foundational technical methods and risk management for trustworthy systems
3. Policy, governance, ethics, human aspects, trust and usability

Each Breakout-session began with a lightning talk from each project attending that session. This “lightning” talks were scheduled for a couple of minutes per project and during which time the project presented itself, its top challenges and/or opportunities, followed by smaller group discussions concerning the top challenges.

After lunch, a session on “Identifying the future R&I landscape and future priorities” chaired by Fabio Martinelli, National Research Council of Italy.

This was followed by a session during which each Chair of the Breakout Sessions reported back on the top five challenges of each theme.

A panel discussion on “International policy and standards evolution” chaired by Mark Miller (CONCEPTIVITY & Cyberwatching.eu partner) followed.

The day ended with a closing address on the theme of “Future Cybersecurity & privacy challenges and funding opportunities” by Nineta Polemi (EC).

ANNEX D. LIST OF PROJECTS AT THE 1ST CONCERTATION MEETING

Project	Full name / Description	Call / Type	End of Project	Web site
AEGIS	Accelerating EU-US Dialogue in Cybersecurity and privacy	DS-05-2016 / CSA	Apr 2019	http://aegis-project.org/
ANASTACIA	Advanced Network Agents for Security and Trust Assessment in CPS/IOT Architectures	DS-01-2016 / RIA	Dec 2019	http://www.anastacia-h2020.eu/
ATENA	Advanced Tools to AssEss and mitigate the criticality of ICT compoNents and their dependencies over Critical InfrAstructures	DS-03-2015 / IA	Apr 2019	https://www.atena-h2020.eu
CANVAS	Constructing an Alliance for Value-driven Cybersecurity	DS-07-2015 / CSA	Aug 2019	https://canvas-project.eu/canvas/
certMILS	Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats	DS-01-2016 / IA	Dec 2020	https://certmils.eu/
CIPSEC	Critical Infrastructure Protection with innovative SECURITY framework	DS-03-2015 / IA	Apr 2019	http://www.cipsec.eu
CITADEL	Critical Infrastructure Protection Using Adaptive MILs	DS-03-2015 / IA	May 2019	http://www.citadel-project.org
COMPACT	Cybersecurity for Public Administrations	DS-02-2016 / IA	Oct 2019	https://www.compact-project.eu/en
CREDENTIAL	Secure Cloud Identity Wallet	DS-02-2014 / IA	Sep 2018	https://credential.eu/
CS-AWARE	A cybersecurity situational awareness and information sharing	DS-02-2016	Aug 2020	https://cs-aware.eu/

Project	Full name / Description	Call / Type	End of Project	Web site
	solution for local public administrations based on advanced big data analysis	/ IA		
CYBECO	Supporting Cyberinsurance from a Behavioural Choice Perspective	DS-04-2016 / RIA	Apr 2019	https://www.cybeco.eu/
C3ISP	Collaborative and Confidential Information Sharing and Analysis for Cyber Protection	DS-04-2015	Sep 2019	https://www.digitalcatapultcentre.org.uk/project/c3isp/
DiSIEM	Diversity Enhancements for Security Information and Event Management	DS-04-2015 / IA	Aug 2019	http://disiem-project.eu
DOGANA	aDvanced sOcial enGineering And vulNERability Assessment	DS-06-2014 / IA	Aug 2018	http://www.dogana-project.eu
e-Sides	Ethical and Societal Implications of Data Sciences	ICT-18-2016 CSA	Dec 2019	http://www.e-sides.eu
EUNITY		DS-05-2016 / CSA	May 2019	http://eunity-project.eu/
EU-SEC	European Security Certification Framework	DS-01-2016/ IA	Dec 2019	http://www.sec-cert.eu/
FENTEC	Functional ENcryption TECHNOLOGIES	DS-06-2017	Dec 2020	http://fentec.eu/
FORTIKA	Cyber Security Accelerator for trusted SMEs IT Ecosystem	DS-02-2016/ IA	May 2020	http://fortika-project.eu/
FUTURETRUST	Future Trust Services for Trustworthy Global Transactions	DS-05-2015/ IA	May 2019	https://www.futuretrust.eu/home/
GHOST	Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control	DS-02-2016 / IA	Apr 2020	http://www.ghost-project.eu
HERMENEUT	Enterprises intangible Risk Management via Economic models	DS-04-2016	Apr 2019	http://www.hermeneut.eu/

Project	Full name / Description	Call / Type	End of Project	Web site
	based on simulation of modern cyber attacks	/ RIA		
KONFIDA	Secure and Trusted Paradigm for Interoperable eHealth Services	DS-03-2016/ RIA	Oct 2019	http://www.konfido-project.eu/konfido/
LIGHTest	Lightweight Infrastructure for Global Heterogeneous Trust management in support of an open Ecosystem of Stakeholders and Trust schemes	DS-05-2015/ IA	Aug 2019	http://lightest.eu
MITIGATE	Protecting Maritime Supply Chain IT Infrastructure	DS-06-2014/ IA	Feb 2018	http://www.mitigateproject.eu
PANORAMIX	Platform for the operation and Optimization in Real-time of MIXed autonomous fleets	DS-01-2014 IA	Aug 2018	https://panoramix-project.eu/
PRIVILEG E	PRIVacy-Enhancing Cryptography in Distributed LEDGERS	DS-06-2017 /	Dec 2020	
PRISMA CLOUD	PRIVacy and Security MAintaining services in the CLOUD	ICT-32-2014 / RIA	July 2018	https://prismacloud.eu/
PRIVACY FLAG	A European research project on personal data protection	DS-01-2014 / IA	Apr 2018	http://privacyflag.eu/
PROTASIS	Police Training Skills		April 2020	https://protasis-project.eu/
PROTECTIVE	Proactive Risk Management	DS-04-2015 / RIA	Aug 2019	https://protective-h2020.eu/
REASSURE	Robust and Efficient Approaches to Evaluating Side Channel and Fault Attack Resilience	DS-01-2016 / RIA	Dec 2019	http://reassure.eu/
RECRE D	Real-world Identities to	DS-	Apr	http://www.recred.eu/

Project	Full name / Description	Call / Type	End of Project	Web site
	Privacy-preserving and Attribute-based CREDentials for Device centric Access Control	02-2014 / IA	2018	
SAINT	S ystemic A nalyzer In N etwork T hreats	DS-04-2016 / RIA	Feb 2021	https://project-saint.eu/
SCOTT	Secure Connected Trustable Things	ECSE L-2016/ IA	Jun 2020	https://scottproject.eu/
SHIELD	European Security in Health Data Exchange	DS-03-2016/ RIA	Dec 2019	http://www.project-shield.eu/
SPECIAL	S calable P olicy-aware L inked D ata A rchitecture For P rivacy, T ransparency and C ompliance	ICT-18-2016 / RIA	Dec 2019	https://www.specialprivacy.eu/
SMESEC	Cybersecurity for Small and Medium-Sized Enterprises	DS-02-2016/ IA	May 2020	https://smesec.eu/
SpeechXRays	Multi-channel biometrics combining acoustic and machine vision analysis of speech, lip movement and face	DS-02-2014 / IA	Apr 2018	http://www.speechxrays.eu/
TRUESSEC.EU	CSA on Certification and Labelling of Trustworthiness Properties from a Multidisciplinary SSH-ICT Perspective and with Emphasis on Human	DS-01-2016 / CSA	Dec 2018	https://truessec.eu/
VESSEDIA	Verification Engineering of S afety and S ecurity Critical Industrial A pplications	DS-01-2016 / RIA	Dec 2019	https://vessedia.eu/
YASHKA	Cybersecurity Awareness and Knowledge Systemic High-level Application»			http://project-yaksha.eu/

Project	Full name / Description	Call / Type	End of Project	Web site

ANNEX E. LIST OF PARTICIPANTS AT THE 1ST CONCERTATION MEETING

Name	Surname	Organization	Project
Stefania	Aguzzi	IDC	e-SIDES
Amelia	Alonso	AEI	cyberwatching.eu
Matthieu	Aubigny	Ittrust Consulting	ATENA
Mari Kert-Saint	Aubyn	Guardtime	PRIVILEGE
Paolo	Balboni	ICT Legal Consulting	cyberwatching.eu
Jorge Bernal	Bernabe	University of Murcia	ANASTACIA
Alysson	Bessani	University of Lisbon	DiSIEM
Justina	Bieliauskaitė	Digital SME Alliance	cyberwatching.eu
Gregory	Blanc	IMT	EUNITY
John	Bothos	NCSR	SAINT
Ahmed	Bounfour	Paris-Sud University	HERMENEUT
James	Caffrey	European Commission	
Roberto	Cascella	ECSO	
Ioannis	Chochliouras	Hellenic Telecommunications Organization	Privacy Flag
Alberto	Crespo	ATOS Spain	FENTEC
Danilo	Delia	ECSO	
Jean-Loup	Dépinay	IDEAMIA France SAS	SpeechXRays
Claudia	Diaz	KU Leuven	PANORAMIX
Christos	Douligeris	University of Piraeus Research Center	MITIGATE
Christos	Douligeris	University of Piraeus Research Center	MITIGATE
Michel	Drescher	Oxford University	cyberwatching.eu
Helmut	Fallman	Fabasoft	
Nicholas	Ferguson	Trust-IT Services	cyberwatching.eu
Afonso	Ferreira	CNRS	European Alliance for Innovation
Jokin	Garatea	GAIA	
Francesca	Giampaolo	Engineering Ingegneria Informatica S.p.A.	DOGANA
Martin	Griesbacher	University of Graz	TRUESSEC.eu
Jassim	Happa	University of Oxford	PROTECTIVE
Carmen	Ifrim	European Commission	
Uros	Janko	Independent consultant	
Andrei	Kelemen	CLUJ IT	
Ismail	Khoffi	Digital Catapult	C3ISP,

			HERMENEUT
Klaus Michael	Koch	TECHNIKON	CERTMILS, VESSEDIA
Francois	Koeune	Université catholique de Louvain	REASSURE
Ioannis	Komnios	EXUS Software Ltd	KONFIDO
Helmut	Kurth	Atsec Information Security	CITADEL
Xabier	Larrucea	Tecnalia	SHIELD
Brian	Lee	Athlone IT	PROTECTIVE
Michele	Loi	University of Zurich	CANVAS
Luis	Lozano	AEI	cyberwatching.eu
Francesco	Manca	AON	cyberwatching.eu
Laurent	Manteau	ECSO	
Evangelos	Markatos	FORTH	PROTASIS
Fabio	Martinelli	CNR	C3ISP, NeCS
Blanca	Martinez de Aragon	PwC Luxembourg	
Victoria	Menezes Miller	Conceptivity	cyberwatching.eu
Mark	Miller	Conceptivity	cyberwatching.eu
Nineta	Polemi	European Commission	
Armand	Puccetti	CEA	VESSEDIA
Bharadwaj	Pulugundla	Verizon	ReCRED
David	Rios	ICMAT-CSIC	CYBECO
Rodrigo Diaz	Rodriguez	ATOS Spain	CIPSEC, SMESEC, YAKSHA
Juha	Röning	University of Oulu	CS-AWARE
Jon	Shamah	EEMA	FutureTrust
Daniel	Slamanig	Austrian Institute of Technology	PRISMACLOUD
Marco	Steger	Virtual Vehicle	SCOTT
Linda	Strick	Fraunhofer FOKUS	EU-SEC
Cristoph	Striecks	Austrian Institute of Technology	CREDENTIAL
Lorenzo	Sutton	Engineering Ingegneria Informatica S.p.A.	COMPACT
Rafael	Tesoro	European Commission	
Karantjias	Thanos	Singular Logic	
Sebastian	Toffaletti	Digital SME Alliance	cyberwatching.eu
Aristotelis	Tzafalias	European Commission	
Dimitrios	Tzovaras	Centre for Research & Technology Hellas - Information Technologies Institute	FORTIKA
Martin	Übelhör	European Commission	
Yolanda	Ursa	INMARK	AEGIS

Valerie	van Roost	European Commission	
Alejandro	Varas Galves	CITIC	cyberwatching.eu
Kostaninos	Votis	Centre for Research & Technology Hellas - Information Technologies Institute	GHOST
David	Wallom	Oxford University	cyberwatching.eu
Agnieszka	Wawrzyk	European Commission	
Simon	Weidler	European Commission	
Niccolò	Zazzeri	Trust-IT Services	cyberwatching.eu
Harald	Zwingelberg	ULD	SPECIAL

GLOSSARY

Term/Abbreviation	Explanation
COSO	Committee of Sponsoring Organizations of Treadway Commission
CS&P	Cyber Security & Privacy
DSP	Digital Service Providers
ECSO	European Cyber Security Organization
ENISA	European Agency for the Security of Networks and Information
ERM	Enterprise Risk Management
GDPR	General Data Protection Regulation
PII	Personally identifiable information