cyberwatching.eu

The European watch
on cybersecurity & privacy

Policy

Cybersecurity standard gap analysis

White Paper

October 2018

Disclaimer

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.

Executive Summary

The focus of this deliverable is to address the issue, with a white paper, of identifying the gaps in cybersecurity standards (and hence also certification). This is done using the methodology of focussed desk research first and foremost in order to gather together and to summarize all of the key efforts that have gone before. We thereafter survey the cybersecurity research, industry, public sector and user communities in order to get inputs into identifying the perceived gaps.

The main objective is that we do not want to “reinvent the wheel”, but rather we want to build upon all of the efforts that have gone before and the knowledge that has been developed around cybersecurity standards and certification.

It is interesting to note that some of the most important conclusions in this deliverable have already been identified previously, which only serves to reinforce the issues that are well known.

First of all, lack of mutual recognition and harmonization of cybersecurity standards are again identified as two of the most important (if not THE most important) gaps that currently exist. This has been noted and mentioned again and again, not only in earlier deliverables from the Cyberwatching.eu, but also in myriad ENISA and ECSO efforts and publications. Common Criteria and SOG-IS (Senior Officials Group-Information Systems Security) have been mentioned in the responses to our survey as really the only recognized area of mutual recognition and harmonization already accomplished but still further work is needed.

Second, and also very important is the fact that IoT is a sector that has been identified as having a notable lack of standards with the added challenges of the first issues of mutual recognition and harmonization.

Finally, the deliverable makes the recommendation that efforts such as ECSO Working Group 1 Meta-Scheme and ECSO WG1 Self-Assessment methodology should be strengthened and can be the path forward with a first approach to address the “low hanging fruit” with mutual recognition and harmonization on the mid to longer term horizon.

Recommendations in brief

1. The issues of **Mutual Recognition** and **Harmonisation** must be addressed due to the national nature of many standards and certification systems.
2. Further efforts must be made in order to raise awareness concerning the available **accepted standards and certification**, as well as the certification process in case of multi-party composition of products and solutions.
3. EC funding should be targeted toward **Raising Awareness and Education in Cybersecurity Standards and Certification** for both the Public and Private sectors.
4. **International Cooperation** is an area for opportunities to benchmark best practices and standards that may already exist as a way to not "reinvent the wheel", however, caution is urged in taking care not to immediately co-opt existing standards that may put European industry at a disadvantage.
5. The **cost issue for SMEs** looking toward standards and cybersecurity certification must be addressed. SMEs must be able to access standards and the related certification without breaking the bank. **Self-assessment** and other **low-cost solutions** must be explored.
6. The R&I community should look address the fast-evolving area of **Internet of Things (IoT)** with respect to cybersecurity standards and certification.
7. Elaborate a **common research agenda** across EU Member States (MS). Through the vehicle of the ERC, open specific calls for projects in the area of cybersecurity with clear aims and requirements in developing in areas of relevance to standards in cybersecurity.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

There have been numerous undertakings by various parties in the field of gap analysis in the EU cybersecurity standards framework.

This document takes into consideration the research already done by those key players in order to gather the knowledge, the findings and work already accomplished in this area.

- Chapter 2 looks at the general background and organizations involved highlighting the research already done and the recommendations proposed
- Chapter 3 looks at the international perspectives
- Chapter 4, 5 6 provides an insight into feedback from the user community
- Chapter 7 presents the Conclusions and Recommendations

2 Background and state of play

2.1 ENISA - Regulatory Body, the bridge between EC and MS

In September 2017, The European Union Agency for Network and Information Security (ENISA) was given a new and permanent mandate by the European Commission to contribute to enhancing resilience of European systems. The proposed mandate reinforces ENISA's role and enables the Agency to better support Member States in implementing the NIS Directive and to become a center of expertise on cybersecurity.

In the scope of cyber security standards and certification, ENISA has already over years engaged in a number of activities to support Member States and the Commission in this area of standards. As identified in its publication “Governance Framework for European Standardisation[1]”, the overall objective of a coordinated approach towards Cybersecurity standardisation should meet the following individual objectives as given below (taken from page 10 of ENISA publication[1]):

- *Cybersecurity standards should be developed through consensus;*
- *Cybersecurity standards should be approved in a recognised body;*
- *The distribution of mandated work for the development of Cybersecurity standards should be coordinated by the recognised bodies;*
- *Recognised bodies should make their development work programme public and coordinate with other recognised bodies to eliminate duplication and to minimise overlap.*

In working towards the above objectives by way of identifying gaps or improving recognition of relevant standards, significant research within the stakeholder community concerning cybersecurity and standards has been done by ENISA resulting in a series of ENISA publications in the field of standards and certification.

[1] ENISA Publication “Governance Framework” (December 2015) (https://www.enisa.europa.eu/publications/policy-industry-research)

2.1.1 Key Findings of ENISA in Cybersecurity Standards

In ENISA publication "**Improving recognition of ICT standards**"[2] (December 2017), research from the market indicated that the information security / cybersecurity standard development ecosystem is "healthy and fast moving". Member States have a high understanding of the NIS Directive and the responsibility to implement it both at the national and regional level.

The main assertions taken from the afore-mentioned ENISA publication "Improving recognition of ICT Standards" (page 4) were[3]:

- *Standardisation for compliance with the NIS Directive is essential;*
- *Recognition of standardisation in policy is low*
- *Utilisation of standards give value to Member States and their infrastructure;*
- *Utlisation of standards raises Cyber Security levels;*
- *Utilisation of standards provides sustainability and interoperability at European level.*

Following the results of the ENISA survey (by means of a form or interview) taken in connection with the publication "Improving recognition of ICT standards"[2], it was not conclusive to identify from Member States if there was actually a gap in the currently available standardisation. It would rather appear that there were a lot of standards but guidance on the role of standards and which standards to use in the NIS Directive Implementation process was lacking. Selecting the right standards to implement NIS was of "paramount importance." Furthermore, in order for the NIS Directive to be implemented effectively, organisations tasked with the technical compliance would need to be aware of the multiplicity of standards and guidelines available and Member States would need to adopt, where possible, **the same standards and guidelines**. This fragmentation at a national level was hindering the unified move of Europe towards a safe and trusted cyber world and raising issues such as challenges to interoperability, market fragmentation and increased cyber risk. In other words, **mutual recognition of standards and harmonisation is key to cybersecurity and economic development in Europe**.

Another major concern was that compliance with the **NIS Directive could not be limited geographically** or perceived as a national requirement within the EU. The reality is that in a global market, software and hardware will originate from beyond the European borders and

[2] ENISA Publication "Improving recognition of ICT standards" (December 2017) (https://www.enisa.europa.eu/publications/improving-recognition-of-ict-security-standards)
[3] Ibid ENISA

therefore the NIS compliance framework should provide for standards and guidelines to ensure that where international, cross-border, information sharing is required within Europe, that NIS Directive compliance is implemented in a harmonized approach.

An analysis of the NIS Directive was published in ENISA publication “Gaps in NIS Standardisation“[4] (November 2016) and is extracted hereafter as Table 1.

[4] ENISA Publication “Gaps in NIS Standardisation” (November 2016) (https://www.enisa.europa.eu/publications/gaps-eu-standardisation)

Article	Affected stakeholder	Responsibility	Reference standard	Observations
4	Member States	Member States shall ensure a high level of security of the network and information systems in their territories in accordance with this Directive	None	The term "high level of security" is undefinable. The affected systems are assumed to be those identified that support essential services.
5	Member States	Each Member State shall adopt a national NIS strategy defining the strategic objectives and concrete policy and regulatory measures to achieve and maintain a high level of network and information security.	See table in Annex C on national regulatory measures	Not a technical standards issue
6	Member States	[*The member states shall appoint a*] National competent authority on the security of network and information systems	None	Not a technical standards issue
7	Member States	Each Member State shall set up a Computer Emergency Response Team (hereinafter: "CERT") responsible for handling incidents and risks according to a well-defined process, which shall comply with the requirements set out in point (1) of Annex I. A CERT may be established within the competent authority	The ENISA report has cited 53 information sharing standards and 16 information management tools relevant to the concept of actionable information. The broad recommendation is to move towards STIX/TAXII/CyBOX for this domain.	Procedures for CERTs to interoperate are defined in general terms. Many EU MS have already identified their CERTs. ENISA has prepared reports on the general topic of data exchange but as noted they cite large numbers of standards and practices with no single harmonised specification. The number of cited standards is of itself a problem and pending a more detailed analysis it is highly likely that the overall picture leads to confusion and overlap. It is suggested that an initial response is a best practice guide that identifies specific standards for specific actions and that overall the number of citations is cut to the single best practice document to be agreed by all MS.

Article	Affected stakeholder	Responsibility	Reference standard	Observations
8	Competent authorities, European Commission	To form a *permanent* network ("cooperation network") to cooperate against risks and incidents affecting network and information system	As for article 7 the preference would be to share data using a format and transfer function as defined for STIX/TAXII/CyBOX ratified within a European SDO (work is underway on this in ETSI TC CYBER).	This article stipulates: "*The Commission shall establish, by means of implementing acts, the necessary modalities to facilitate the cooperation between competent authorities and the Commission referred to in paragraphs 2 and 3. Those implementing acts shall be adopted in accordance with the consultation procedure referred to in Article 19(2)*" which may imply standards need to be developed and cited
9	Competent authorities, European Commission	The "cooperation network" to be intrinsically secure	As for article 7 the preference would be to share data using a format and transfer function as defined for STIX/TAXII/CyBOX ratified within a European SDO (work is underway on this in ETSI TC CYBER).	Implementing acts may be required
10	Competent authorities, European Commission	To use the "cooperation network" to exchange information of the form "early warning"	As for article 7 the preference would be to share data using a format and transfer function as defined for STIX/TAXII/CyBOX ratified within a European SDO (work is underway on this in ETSI TC CYBER).	Delegated acts may be required
11	Competent	To give assurance based on	As for article 7 the	Responses will be made at national level and

Article	Affected stakeholder	Responsibility	Reference standard	Observations
	authorities, European Commission	information from the early warnings received via the "cooperation network" of a coordinated response	preference would be to share data using a format and transfer function as defined for STIX/TAXII/CyBOX ratified within a European SDO (work is underway on this in ETSI TC CYBER). The impact here extends to working practice and policy and not to technical specifications.	coordinated but the cooperation model needs policy development.
12	European Commission	To adopt, by means of implementing acts, a Union NIS cooperation plan	Extends the technical and policy framework from articles 7 through 12.	Policy not technical.
13	European Union	Shall allow for harmonised international cooperation	This may be more easily fostered if the programme of standards supporting the "cooperation network" are also in common use internationally	Adopting the STIX/TAXII/CyBOX approach in close cooperation with international partners may achieve this goal more easily, notwithstanding the political issues that may need to be negotiated.
14	Competent authorities, Member States, Market operators, Public Administration	To deploy risk managed secure networks and infrastructure	The standards track identified by the EU ERNCIP programme applies with additional attention paid to specific controls under the ISO 27000 family of	ISO 27001 in particular is not very precise and has a cost burden to implement for SMEs who although excluded for now from the NISD may be in the overall supply chain and this requires that the entities they supply to take responsibility for all entities in the supply chain

Article	Affected stakeholder	Responsibility	Reference standard	Observations
			management standards.	
15	Member states, Competent authorities	Powers to enforce compliance and investigate non-compliance	The suggestion is that market operators need to prove the security of their networks. This could imply Common Criteria (recommended) or some other assurance scheme. Current standards do apply including ISO/IEC 15408 and NIST SP 800	Target of what is to be complied to needs to be stated. This should be a stated NIS Protection Profile or close equivalent.
16	Member States	Encourage implementation of article 14 by use of implementing acts	As noted there are a number of existing standards to undertake risk analysis and the sharing of the results of such analysis.	The notes from Article 14 apply
17	Member States	Harmonised sanctions for failure to implement	None	Not a technical standards issue but requires harmonisation of sanctions. It is noted that attacks may arise from outside the EU and other international laws may need to be invoked
18	Member States	Power to adopt delegated acts	None	Not a technical standards issue
19	European	To establish a NIS Committee	None	Not a technical standards issue
20	European Commission	To establish a review process	None	Not a technical standards issue
21	Member States	Transposition of NISD to provisions in	None	Not a technical standards issue

Article	Affected stakeholder	Responsibility	Reference standard	Observations
		national law		
22	Member States	To establish NISD as national law within 20 days of publication of NISD in official journal	None	Not a technical standards issue. However compliance without a sound standards basis may be difficult to enforce
23	Member States	Intended audience of NISD	None	Not a technical standards issue

Table 1: Analysis of NIS Directive taken from ENISA Publ. "Gaps in NIS standardisation"[5]

[5] Ibid ENISA

From the above analysis by ENISA of the NIS Directive, the following articles 4, 7, 8, 9, 13, 14, 15, 16, 17 and 22 indicate where some gaps occur related to standards "generalisation" (i.e., lack of criteria), harmonisation, overlap. The first two columns of Table 2 (below) are taken from ENISA Publication "Gaps in NIS Standardisation"[6] and the third column in Table 2 (below) provides an indication of what we perceive as a gap following the ENISA analysis of NIS:

Article of NIS	Comment/Observation from ENISA publication "Gaps in NIS Standardisation"[7]	Perceived Gap (Cyberwatching.eu input)
4	The term "high level of security" is undefinable. The affected systems are assumed to be those identified that support essential services.	• Level of security has not been defined clearly enough.
7	Procedures for CERTs to interoperate are defined in general terms. Many EU MS have already identified their CERTs. ENISA has prepared reports on the general topic of data exchange but as noted they cite large numbers of standards and practices with no single harmonised specification. The number of cited standards is of itself a problem and pending a more detailed analysis it is highly likely that the overall picture leads to confusion and overlap. It is suggested that an initial response is a best practice guide that identifies specific standards for specific actions and that overall the number of citations is cut to the single best practice document to be agreed by all MS.	• Single harmonised specification is lacking • Too many standards becomes problematic because it leads to confusion and overlap • Single best practice guide/document is required which will identify specific standards and required actions
8	This article stipulates: "*The Commission shall establish, by means of implementing acts, the necessary modalities to facilitate the cooperation between competent authorities and the Commission referred to in paragraphs 2 and 3. Those implementing acts shall be adopted in accordance with the consultation procedure referred to in Article 19(2)*" which may imply standards need to be developed and cited	• Standards may need to be developed and cited
9	Implementing acts may be required	• Implementing regulations may be required
13	This may be more easily fostered if the programme of standards supporting the "cooperation network" are also in common use internationally	• Agreement and guidance for common use of international standards

[6] Ibid ENISA
[7] Ibid ENISA

Article of NIS	Comment/Observation from ENISA publication "Gaps in NIS Standardisation"[7]	Perceived Gap (Cyberwatching.eu input)
		is necessary
14	ISO 27001 in particular is not very precise and has a cost burden to implement for SMEs who although excluded for now from the NISD may be in the overall supply chain and this requires that the entities they supply to take responsibility for all entities in the supply chain	• ISO 27001 is insufficiently precise • ISO 27000 entails a cost burden for SMEs. If a minimum baseline could be stipulated then this would encourage rather than deter SMEs to providing secure products and/or services • An implementing act would ensure that entities in the supply chain would take responsibility
15	Target of what is to be complied to needs to be stated. This should be a stated NIS Protection Profile or close equivalent.	• More specific information is necessary for compliance
16	The notes from Article 14 apply	
17	Not a technical standards issue but requires harmonisation of sanctions. It is noted that attacks may arise from outside the EU and other international laws may need to be invoked	• Harmonisation of sanctions • Harmonised use of international standards
22	Not a technical standards issue. However compliance without a sound standards basis may be difficult to enforce	Specific standards recommendation required

Table 2: Identification of standards gaps following analysis by ENISA in Table 1[8]

The following summary of existing ETSI and ISO standards in support of the NIS Directive were identified by ENISA in its publication "Improving recognition of ICT security standards"[9] (December 2017), and, as indicated above, the number of standards and overlap is confusing to the end user:

[8] Ibid ENISA

[9] Op cit ENISA "Improving recognition of ICT standards"

ETSI Specifications in support of NIS Directive

STANDARD	AREA
Doc. Nb. TR 103 331 Ver. 1.1.1 Ref. DTR/CYBER-0009 Technical Body: CYBER	CYBER; Structured threat information sharing
Doc. Nb. TR 103 306 Ver. 1.2.1 Ref. RTR/CYBER-0026 Technical Body: CYBER	CYBER; Global Cyber Security Ecosystem
Doc. Nb. TR 103 305-4 Ver. 1.1.1 Ref. DTR/CYBER-0012-4 Technical Body: CYBER	CYBER; Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms CSC Facilitation Mechanisms
Doc. Nb. TR 103 305-3 Ver. 1.1.1 Ref. DTR/CYBER-0012-3 Technical Body: CYBER	CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations CSC Service Sector Implementations
Doc. Nb. TR 103 305-2 Ver. 1.1.1 Ref. DTR/CYBER-0012-2 Technical Body: CYBER	CYBER; Critical Security Controls for Effective Cyber Defence; Part 2: Measurement and auditing CSC Measurement and auditing
Doc. Nb. TR 103 305-1 Ver. 2.1.1 Ref. RTR/CYBER-0012-1 Technical Body: CYBER	CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls Critical Security Controls for Effective Cyber Defence
Doc. Nb. TR 103 303 Ver. 1.1.1 Ref. DTR/CYBER-0001 Technical Body: CYBER	CYBER; Protection measures for ICT in the context of Critical Infrastructure Security of ICT in CI

Table 3: Taken from ENISA Publication "Improving recognition of ICT security standards"[10]

ISO Specifications in support of NIS Directive

STANDARD	AREA
ISO/IEC 27000	Information security management systems - Overview and Vocabulary
ISO/IEC 27001	Information security management systems – Requirements
ISO/IEC 27002	Code of practice for information security controls.
ISO/IEC 27005	Information security risk management
ISO/IEC 27007	Information security management systems - auditor guidelines
ISO/IEC 27008	Guidelines for auditors on ISMS controls
ISO/IEC 27009	Sector-specific application of ISO/IEC 27001 – Requirements
ISO/IEC 27033	Network security

[10] Ibid ENISA

STANDARD	AREA
ISO/IEC 27034	Application security
ISO/IEC 27035	Information security incident management
ISO/IEC 27044	Guidelines for Security Information and Event Management SIEM

Table 4: Taken from ENISA Publication "Improving recognition of ICT security standards"[11]

Recommendations set forth in ENISA Publication "Improving recognition of ICT security standards":

> "*In light of the above, the following solutions are recommended to mitigate the lack of overall awareness and trainings on the role of standards in NIS Directive compliance and to encourage wide deployment of common security platforms in the OES and PDS entities:*
>
> - *Training initiatives by the European Commission and ENISA through workshops for Member States' relevant agencies*
> - *Promotion of new work items in the European SDOs for some areas (e.g. criteria for defining OES / DSP) or the adoption of appropriate standards in Europe where existing (for example information exchange, where several mature efforts already are in place, like STIX12)*"
>
> Additional considerations:
>
> "*A set of standardisation requests identifying those standards which may be used to state NIS Directive compliance (when conformed with) should be drafted. To this aim, the expertise pool of the European Standardisation Organizations could be used, when needed.*"

2.1.2 Key Findings/Recommendations in ENISA Cybersecurity certification

Cybersecurity certification is complex in an innovative and changing ICT landscape where the supply chain is not confined to borders and where products, services, critical infrastructure are linked. Trust and security of information in the EU is an essential component of the Digital Single Market. The level of trust and security of ICT products and services can be raised through certification. Whilst efforts move forward at the national level to set high-level cybersecurity requirements, this could lead to market fragmentation and challenges to interoperability. Therefore, a common certification framework recognized by Member States would pave the path to achieving this goal of securing a trustworthy and secure ICT environment.

[11] Ibid ENISA"

ENISA has engaged in a number of activities to support the European Commission and Member States in finding a way forward to pursue certification of ICT products and services. Some of these activities have covered research, stakeholder interviews (experts from Member States, industry representatives) and surveys, resulting in a series of publications, including the following publications:

- Challenges of ICT Certification in Emerging ICT Environments (December 2016)
- Considerations in ICT Security Certification in EU (August 2017)
- Recommendations on GDPR Certification (November 2017)
- Mapping of OES Security Requirements to Specific Sectors (December 2017)
- Overview of ICT certification laboratories (January 2018)

In April 2017, a survey on "ICT Security Certification" was carried out by ENISA, with the aim to find the best approach to address certification across the EU within the available or envisaged policy options.

Some of the key challenges which were highlighted in the afore-mentioned publications are described below:

- **Harmonisation across EU** is a need. A common approach to standards and frameworks for certification at the EU MS level is required
- **Mutual recognition of certification standards and/or practices across the EU** at MS level is necessary otherwise market fragmentation emerges and presents the challenge of interoperability
- Standalone certified devices are usually considered trustworthy. However, this may not be the case after integration in a real computing environment which requires that **planning and testing of systems is crucial**. In addition, connection to complex and critical systems can open the door to potential attacks via devices such as phones, tablets and laptops
- Building cyber resilience requires that processes and procedures across systems is put in place, including **security by design**
- Outsourcing to third parties increases the risk of being vulnerable to cyber-attacks and again here procedures and processes are necessary

Key recommendations from ENISA Publication "Challenges of security certification in emerging ICT environments"[12]:

[12] ENISA Publication "Challenges of security certification in emerging ICT environments" (December 2016) (https://www.enisa.europa.eu/publications/challenges-of-security-certification-in-emerging-ict-environments)

> *"Organisations should strive for certifying their management system because it is a powerful tool that helps companies to achieve their business goals.* ***Process certification and compliance is vital*** *to support product quality, and it is often a ticket to the market. For markets large enough, product manufacturers can test and certify their products only once as they can have them accepted in many other markets or countries thereafter.*
>
> - *Both vendors and asset owners should take a holistic view when it comes to security certification and not merely focus on the functional element of the devices they use. Only after* ***verification*** *of a system in its entirety, including procedures for operation and maintenance, it can be considered* ***cyber secure****.*
> - *Organisations should invest more on improving the cyber security education of their engineers. This is because they usually do not have cyber security culture as they are often confronted with new technologies, or other domains unknown to them, until it is too late to adopt mitigation measures. Therefore, they need to be educated, to become aware of cyber risks and to realize that the system is as strong as each individual component, and that actions and decisions taken for a sub-part of the system can have a major impact on the overall performance of the system itself.*
> - *Cyber security service providers are recommended to implement an IT service management framework in their organizations as a proof that their services meet customers' needs.*
> - *Whenever this is financially justified, customers should look for the use of security service providers who provide a* ***follow-the-sun support4*** *team in order to ensure maximum availability of their services. Furthermore, they should seek for security service providers with an IT service management system which is based on international and widely known standards e.g. ITIL, ISO/IEC 20000 etc.*

In September 2017, the Commission adopted a cybersecurity package in which ENISA was given a more central and specific role in the EU's cybersecurity landscape. The reform proposal issued in September 2018 includes a permanent mandate for ENISA so that it not only provides advice but also can perform operational tasks. ENISA will also play an important role in the creation of the first voluntary EU cybersecurity certification framework.

2.2 ECSO Working Group 1 - Industry plus Public Sector community

Website: https://ecs-org.eu/

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 organisation 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. In particular, ECSO's Working Group 1 (WG1) covers standardisation, certification, labelling and supply chain management. ECSO has worked intensely since its creation in 2016 and has published the following documents.

1. The **State-of-the-Art Syllabus (SOTA)**[13] which is a comprehensive collection of existing cybersecurity standards and certification schemes across Europe which aims to address the challenges compiled in the Challenges of the Industry (COTI).
2. The **Meta-Scheme Approach** which is a broad set of security certification schemes for products, systems, solutions, services and organisations.
3. The **Challenges of the Industry (COTI)** compiled by SWG1.1, SWG1.2 and SWG1.3 (not publicly available).

2.2.1 State-of-the-Art Syllabus (SOTA)

SOTA : https://ecs-org.eu/documents/publications/5a3112ec2c891.pdf (Dec.2017)

As explained in SOTA, the goal of WG1 is to propose one or more harmonised, common certification framework(s), as much as possible based on existing standards, to address Cybersecurity within the European Digital Single Market. Through extensive work undertaken between SWG1.1, SWG1.2, SWG1.3 and SWG1.4, in June 2017, ECSO Working Group 1 (WG1) issued a State-of-the-Art Syllabus (SOTA) (updated in December 2017), in which it identified, across Europe, 294 standards and certification schemes deemed relevant in the area of assessing information security of a product and component, service or organisation. In this comprehensive document, the standards and schemes fall into the following categories, with each certification scheme presented according to focus, associated scheme and governance, process, practice, formal status and relationship with other standards/schemes:

- Products and Components:
  - Standards and schemes for generic IT products (8 standards/schemes)
  - Standards and schemes for products used in Industry 4.0 and ICS (2)
  - Standards and schemes for products used in energy and smart grids (3)
  - Standards and schemes for products used in telecom (1)
  - Standards and schemes for products used in the payment industry (4)
  - Standards and schemes for cryptographic modules (4)
  - Standards and schemes for web applications (2)
  - Standards and schemes for IoT products (1)
  - Standards and schemes for other IT products (2)

[13] ECSO publication "SOTA" (December 2017) https://ecs-org.eu/documents/publications/5a3112ec2c891.pdf

- ICT Services
    - Standards and schemes for cloud service providers (8)
- Service providers and organizations
    - Standards and schemes for generic organisations (20)
    - Standards and schemes for Industry 4.0 and ICS (7)
    - Standards and schemes for energy and smart grids (4)
    - Standards and schemes for transportation (road, rail, air, sea) (3)
    - Standards and schemes for financial services and insurance (3)
    - Standards and schemes for public services / eGovernment / digital citizenship (4)
    - Standards and schemes for healthcare (3)
    - Standards and schemes for smart cities and smart buildings (3)
    - Standards and schemes for telecom, media and content (3)
    - Standards and schemes for critical infrastructures (4)
    - Standards and schemes for general secure software development (5)
    - Standards and schemes for Cybersecurity service providers (2)
    - Standards and schemes for the payment industry (1)
    - Standards and schemes for IoT device vendors (7)
- Security professionals (9)
    - CompTIA certifications
    - CREST certifications
    - EC-Council certifications
    - GIAC certifications
    - ISACA certifications
    - ISA/IEC 62443 Cybersecurity Certificate Programs
    - (ISC). certifications
    - ISO/IEC 27021 (Competence requirements for ISMS professionals)
    - NCSC Certified Professional (CCP) certifications

The SOTA study is available online at https://www.ecs-org.eu/working-groups/news/wg1-state-of-the-art-syllabus-updated. It is a living document which will be extended regularly to include new identified gaps, new standards or schemes published.

2.2.2 Challenges of the Industry (COTI) – ECSO Working Group 1 working paper

Within Working Group ESCO WG1, the Challenges Of The Industry (COTI) is an internal document which lists some 290 inputs or issues highlighted by individual members of the ECSO WG as challenges encountered in addressing cybersecurity standards and certification. Given that the COTI is not public, the specifics contained therein cannot be shared within this deliverable, however in writing the deliverable the authors have a detailed knowledge of the COTI and as such the concerns of the industry, the research community, the public sector and the user community are inherently addressed in our work, albeit, the text of the COTI and the details cannot be shared directly.

2.2.3 Meta-Scheme Approach

Meta-scheme: https://www.ecs-org.eu/working-groups/news/wg1-european-cyber-security-certification

The Meta-Scheme Approach[14] prepared by ECSO WG1 has examined the COTI document and notes that many of the challenges found are recurrent topics, such as "*harmonisation, privacy, patching & updating, connected devices, time to market & innovation speed, base line, trusted products and brand protection.*" More specifically,

- Lack of harmonisation in **governance**
- **Scalability** of existing schemes is an issue, including the cost for upgrades which can be very expensive hindered by the heavy formal process and the time taken for certificate issuance
- There is a **lack of harmonised requirements** for baseline security
- **Risk assessment** is sometimes included in certification schemes but not always
- Certification can be **slow** and the process cumbersome
- There is an **assumed trust in a product** but if updates are duly certified a false impression is given to the end user

[14] ECSO Meta Scheme Approach (https://www.ecs-org.eu/working-groups/news/wg1-european-cyber-security-certification)

The meta-scheme approach proposes some key objectives[15] which could be considered in a future-proof certification model, as follows:

"***Obj 1. Threat analysis*** *and* ***risk assessment*** *shall be the* ***source to determine security requirements*** *that are used as the basis for security evaluation & certification of items.*

Obj 2. *The evaluation of the risk should involve the* ***risk owner*** *(e.g. user of a product) and consider the supply chain for* ***liability****.*

Obj 3. *A* ***minimum required baseline*** *shall be defined against which items are assessed to significantly reduce the deployment of unsecure items (product, services, infrastructure, ...) into the European market.*

Obj 4. *The* ***burden for manufacturers w.r.t. to certification****, such as bureaucracy, costs, time to market, shall be* ***minimized*** *in the context of its usage while ensuring adequate trust in security claims.*

Obj 5. *Security evaluation & certification shall confirm the* ***security strength of items*** *under evaluation against state-of-the art attacks.*

Obj 6. Regular lean re-assessments *shall be part of the governance procedure to reduce the risk of undiscovered vulnerabilities w.r.t. to new attacks that are found in the field; the frequency and methodology should depend on the application field and type (product, service, ...).*

Obj 7. Patching *shall be considered as a* ***standard process*** *in the certification flow (devices are mostly online in future) rather than as an exception (in the past devices where mostly offline) and shall incorporate delta-assessments.*

Obj 8. Fragmentation *of the market shall be reduced by means of harmonization while not reinventing the wheel (maximum re-use of existing schemes).*

Obj 9. Security by Design and Privacy by Design *shall be explicitly taken into account.*

[15] Ibid ECSO

2.2.4 What are the grand challenge areas in Cybersecurity within the academic research community?

With the majority of funding for academic research in any area being dependent on the availability of appropriate funding streams then the ability for the academic community to contribute within this area is limited to the funding plans and schedules of mostly national agencies that support them. As such we will consider the current funding landscape including priorities in a number of leading EU countries in this area as well as the EC funding programs themselves. Using the number of collected projects within the Cyberwatching.eu project catalogue and observatory as a benchmark of where the leading contribution is being made by national governments, we will be looking at the following countries individually and then attempting to synthesis their individual contributions with those by EC projects to create the description of grand challenge areas. The Countries are: Germany, France, United Kingdom, Czech republic, all of which have funded over twenty directly related cybersecurity projects.

Germany

The Federal Ministry of Education and Research (BMBF), which is responsible for this area, has established a number of research programs in this area to support development within sectors or areas that have critical importance for the German society and economy. Since 2009 it has funded programs to a value of €66M and has established research into innovative approaches of IT security as a priority task in a number of specific domains, namely:

- **Industry 4.0**: as a globally recognised leader in high quality engineering and technology it is unsurprising that leading players in this area are considering moving to the next generation manufacturing methodologies. As such, these involve substantial increases in networking, digitisation etc. all of which increase the attack surface for the application in question. This part of the program is concerned in protecting businesses both from 'normal' hacking as well as nation state scale industrial espionage.
- **Privacy**: Germany is seen as a leader in the development of policies, processes and technology that supports the privacy of the individual. The many different services that are available to users on the internet often meet with justified reservations on the part of the public as they frequently entail involuntary insights into people's private lives with loose or difficult to understand privacy capabilities. Personal data is not only of great interest to industry but can also often be used by state institutions. One of the key challenges facing IT security therefore is to develop processes and tools which enable members of the public to enforce their right to informational self-determination.
- **Critical Infrastructure**: Modern life depends on the reliability and assurance that we are able to give to digital systems that are operating the underpinning infrastructure that we mostly take for granted, be that energy, water, transport or, communications. These are all high value targets and as such with recent examples of how vulnerable if not properly protected these type of systems are a high priority

is given to projects to research and develop new solutions for IT security at critical infrastructures.

- **Safe Cloud Computing**: the cloud is a hugely important IT paradigm that correctly implemented and used can bring enormous benefits to both the provider and consumer. It is also a domain where established security and privacy actions can be difficult to apply, where there is a corresponding increase in vulnerability due to the attractiveness of the large datacentres that make up the clouds physical infrastructure. Developing new, verifiable security concepts must therefore be developed and implemented in order to make full use of the potential of cloud computing. Only then will users have confidence in cloud computing as a business model.

France

Academic research in the area of cybersecurity is funded within France by the L'Agence nationale de la recherché (ANR) though a number of key themes which have been supported through a number of annual program announcements. They are all broad in their remit and the projects which they support.

In the program published in 2013 the following themes were supported

- Security of the Digital Society,
- Software Science and Technology,

Within the 2016 launched France Europe 2020 program the two following societal challenges were covered which both have significant cybersecurity components of support within them.

- Information and Communication Society
- Freedom and security of Europe, its citizens and residents

Within a larger overall theme of activities around both cybersecurity and cyber defense the following theme was hosted in a wider partnership between ANR and other agencies.

- Cybersecurity of society and fight against cybercrime

United Kingdom

Within the UK, the Engineering and Physical Sciences Research Council is responsible for the funding of academic research into cybersecurity. Within this organisation cybersecurity sits within one of twelve key themes, Global Uncertainty. Cybersecurity sits within this though it is contributed to by a large number of fundamental research areas that are within the remit of the organisation. There have also been a number of specifically targeted funding activities that have included for example work to research the link between and the detection of criminal activity within cloud computing environments. Alongside these small project focused funding sources are a number of larger programs that include the establishment of a set of Doctoral Training centres, hosted by leading institutions which are intended to grow the number of practitioners in cybersecurity over the coming years. To showcase the work that is both funded by the EPSRC and that from other agencies the EPSRC has also supported the establishment of a number of institutions as Academic Centres of Excellence in Cybersecurity. This is co-badged with the UK GCHQ and National Cyber Security Centre. There are 14 of these centres currently. Alongside this directly academic only funding there is also applied R&D support which though industrially led normally has partnership within the consortia by academic institutions. InnovateUK the agency responsible for this support has in the past held specific funding calls for cybersecurity within their main R&I competition as well as targeted Knowledge transfer Partnerships which connect a business with an academic organisation which is intending to transfer its knowledge to the business. InnovateUK operates within a set of challenges as set out by the UK government, some of which are security related or have cybersecurity as components of them and alongside other countries already discussed may be defined as Advanced manufacturing, personalised healthcare, cybersecurity and advanced creative industries.

Czech Republic

Within the Czech Republic, the support available for research comes through four main channels, the Ministry of Education, Youth and Sport, Ministry of the Industry and Trade, Czech Science Foundation and Technology Agency of the Czech Republic. Alongside these a significant number of projects in cybersecurity research in academia are through a program from the Ministry of the Interior called “Security Research Programme of the Czech Republic in the years 2015 – 2020”. The program has a remit that is actually broader than just Cybersecurity, considering a main objective of the Programme to increase the security of the state and citizens using new technologies, knowledge and other results of applied research, experimental development and innovation in the field of identification, prevention and protection against acts of unlawful interference, natural or industrial disasters, to the detriment of Czech citizens, organisations or structures goods and infrastructure.

The Ministry of Industry and trade is actively promoting an Industry 4.0 strategy which includes within in it work on the security required for such as program to be successful. Alongside this is the recognition of possible vulnerabilities in critical national infrastructure and therefore programs have been launched that include support for R&I in this area.

The TACR hosts within one of its programs (Epsilon), work on cybersecurity as part of the overarching knowledge-based economy theme.

Summary

Overall national funding in many areas can be divided in two, either for the fundamental research that may then be utilised for more applied activities either by the research team themselves or through partnership funding models working with relevant businesses or other organisations able to produce user relevant services or content. As is to be expected, the domains and core challenges that are supported nationally are replicated within EC cybersecurity support programs though these some benefit in being multi-national activities.

2.2.5 How are the academic results being transferred either to public or private sector?

It is clear that within the majority of the programs amongst these leading nations that have been discussed, a number of which have funding available not just for academic organisations but anyone who can successfully defend the work they are doing as Research and Innovation, though they must be nationally resident. Other programs, for example those specifically within the UK from the Research Councils though only support the activities of universities or Research organisations.

More generally than just cybersecurity, nearly all funding agencies discussed for leading countries, now support publication through open access supporting publications. These allow research outputs and other material to be more easily accessible to industry and other relevant groups that previously have had to directly engage an academic in partnership to gain access to required knowledge for their business.

2.2.6 What participation in cybersecurity standards development is there by the academic community?

Contributing to standards development is performed under a variety of business models – that is to say, under a participation model that adds value and benefits to the participating organisation.

This is closely tied to many other aspects of academic involvement: Knowledge transfers into the public and private sector (e.g. the very successful UK Knowledge Transfers Partnerships, KTP), direct commercialisation through spin-off companies, licensing patents and IPR, are all but a few examples of how universities participate in cybersecurity development.

Hence, involvement of the academic sector in standards development is only one of the necessary activities in this area. Therefore, the decision to join an SDO is also influenced by the membership structure as well as fee structure offered by the SDO under scrutiny – in short the question of “value for money” plays a significant role here as well.

In collaboration with the StandICT.eu project, Table 5 the following Standards Development Organisations (SDO) have been identified as active and significant contributors to cybersecurity standards development.

Body	Academic tier?	Academic fee (thousands)	Standard rate (thousands)	Discount	# Academic partners
ETSI	yes	2	6 - 155	66 - 98%	36
ECSO	yes	2	2 - 12	0 - 83%	67

EOS	yes	n/a	n/a	n/a	2
OASIS	yes	1.5	1.5 - 10	0 - 85%	24
W3C	yes	7.8	21 - 68	62 - 99%	37

Table 5: International Standards Development Organisations with academic involvement

This list is complemented by the following SSOs: CEN, CENELEC, ISO/IEC JTC1, and ITU-T SG17. Interestingly, this differentiation did not appear due to their difference in developing vs. setting standards (technical development only, and elevation and approval into regulatory power, respectively), but their fundamental differences in membership programmes:

SSOs do not offer direct membership – only the national bodies coordinate and propose members and experts for their technical committees.

Conversely, any SDO we examined offered *direct* membership, and all offered membership discounts as illustrated in

Body	Academic tier?	Academic fee (thousands)	Standard rate (thousands)	Discount	# Academic partners
ETSI	yes	2	6 - 155	66 - 98%	36
ECSO	yes	2	2 - 12	0 - 83%	67
EOS	yes	n/a	n/a	n/a	2
OASIS	yes	1.5	1.5 - 10	0 - 85%	24
W3C	yes	7.8	21 - 68	62 - 99%	37

Table 5.

The participation figures provided in Table 5 are not accurate in the sense that, with the exception of ETSI and ECSO, all SDOs concern many areas of ITC other than cybersecurity. The level of university participation in those organisations for cybersecurity purposes is therefore likely much lower than the figures provided.

2.3 The AEI Experience

The AEI Ciberseguridad is the Spanish Cybersecurity Cluster that brings together companies, research centers and other organizations interested in the promotion of the Cybersecurity sector and other advanced technologies such as Big Data, Blockchain, IoT, Smart Cities, etc.

Our cluster has around 80 members, over 60 are companies and we are also one of the founding members of the European Cyber Security Organization (ECSO) since 2016.

The AEI Seal of Cybersecurity for Organizations is a certification scheme developed by the 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 Seal of Cybersecurity for Organizations has been created from the collaborative work of a group of member companies of the AEI. Currently there are three certified companies as consultants of the Seal, which has generated them a new line of business in the field of consulting. Also, there are currently thirteen entities in the certification phase as consultants. The company SGS is the one who acts as a qualified auditor to carry out the evaluation processes.

The members of this group are:

- Grupo CFI
- Grupo SGS
- University of León
- CSA
- S21SEC
- Proconsi
- Xeridia
- Panda Security

More information regarding the Seal of Cybersecurity is public available on the AEI website and also in another deliverable of this project, *"D3.2: European cybersecurity and privacy Research & Innovation Ecosystem"*.

The general assessment of the AEI of Cybersecurity as a representative organisation of SMEs is that there is still a lot of work to accomplish in this area, although the good news is that the deficiencies are clearly identified.

Normally, European SMEs usually work only in their place of origin and compliance with national regulations is usually sufficient. However, our analysis of deficiencies in cybersecurity standards is that there are defined high-level regulations where technical issues are not addressed or defined. We believe that regulations should include the definition of specific technical protection measures to be applied and regulated according to high, medium or low levels.

This is defined in Spain according to the National Cybersecurity Scheme, which specifies the firewalls to be used, the backup copies or how to manage the permissions. By proposing specific technical measures, greater harmonisation by countries would be achieved and there would be no different interpretations and different security requirements according to each country. A field where European harmonisation is well regulated and also functions well is at the level of critical infrastructure protection.

From the point of view of cost implications for European SMEs, we can analyse the following considerations. If the regulation would include an accurate technical description of the requirements to be covered at European level:

- Investment costs for companies would be high, but they would already be compliant to work at a European level
- A company could objectively estimate the costs of operating in another European country, eliminating subjectivities.
- In the long term it could mean an economic saving and a simplification of internal processes of the company, which would make it more competitive

Therefore, the way forward is to simplify cybersecurity standards at a technical level, defining specific technical solutions so that all countries are subject to the same requirements.

On the other hand, a greater implementation of cybersecurity regulations will come when Public Administrations or large companies enforce compliance from their suppliers as a prerequisite to working with them. In that way, a top-down drag effect will be generated. In order to favor greater homogenization, the regulations must include the obligation (even if progressive) of compliance with levels of cybersecurity to work with these large organizations.

Only with demanding legislation will SMEs be forced to incorporate the corresponding technical requirements. As long as it is not mandatory, they will not comply with it, in such a way that although progress is made in legal harmonisation, there will be deficiencies in everyday situations.

Regarding future challenges, we think it is interesting that the EU could establish minimum standards required for all electronic and computer equipment imported into the EU, especially in the future thinking of devices with IoT components that can connect to the Internet. Regulate the connection protocols of these devices, avoid that they can connect automatically or the protection of the generated data are aspects to take into account.

Another clear future trend for SMEs will be the use of managed security. From the point of view of legal compliance, it is necessary to satisfy the requirements demanded by all type of regulations, as well as to establish corporate security processes (risk analysis, backup copies, contingency plan, etc.). A Security Operations Center (SOC) is an infrastructure that monitors the activity of a company's computer systems in real time in order to prevent security incidents or, in the event that they occur, offer a rapid and adequate response. This type of facility sends information in real time, detects anomalous behavior and reacts in advance before the client / provider calls you with the problem already generated.

2.4 EU best practices

EC-funded projects are contributing to shaping and influencing the standards and certification landscape. The Cyberwatching.eu webinar in M17 saw the participation of 4 of these projects which are outlined below[16].

StandICT.eu Supporting European Experts Presence in International Standardisation Activities in ICT

Jan 2018 – Dec 2019

www.standict.eu

StandICT.eu addresses the need for ICT Standardisation and defines a pragmatic approach and streamlined process to reinforce EU expert presence in the international ICT standardisation scene. Through a Standards Watch, StandICT.eu analyses and monitor the international ICT standards landscape and liaise with Standards Development Organisations (SDOs) and Standard Setting Organisations (SSOs), key organisations such as the EU Multistakeholder Platform for ICT Standardisation as well as industry-led groups, to pinpoint gaps and priorities matching EU DSM objectives. These are the topics for a series of 10 Open calls focused on priority domains and a continuous cascading grants process, launched by StandICT.eu from March 2018, providing support for European specialists to contribute to ongoing standards development activities, and attend SDO & SSO meetings.

End-users

- European Standards experts
- SDOs
- Standards-related organisations

Open calls are based on the five pillars of the Digital Single Market. Cybersecurity is therefore one of the core call topics. To date 2 open calls have been completed and a total of four activities have been funded.

Successful applications

1. Participation in and contribution to the European Cyber Security Organisation (ECSO) Working Group 1 (Cybersecurity Standards / Certification / Supply Chain)
2. Expert member of ISO/IEC SC27 WG2 – IT Security Techniques
3. European consumer representation in ISO/PC 317 “Consumer protection: privacy by design for consumer goods and services” to develop ISO/NP 23485 standard

[16] https://www.cyberwatching.eu/cybersecurity-standards-and-certification-challenges

4. Support as rapporteur in ETSI Intelligent Transport Systems WG5 Security

Sample of unsuccessful applications

a) Pushing Privacy-Preserving Cryptography into Global ICT Standards
b) Secure and efficient Internet communication in the IoT and Internet backbone (IETF)
c) General end-to-end security and quantum-safe algorithms for Smart Grid (IEC TC 57 WG 15)
d) Trustworthy Key Provisioning for Software Defined Network Elements
e) Bringing human factors into the cybersecurity standards process (ETSI Cyber #14)
f) Collaboration with W3C on revising generic sensor API specifications

The applications reflect the changing European landscape in terms of new regulations and the importance of cybersecurity in other technologies. The presence of applications related to privacy, included Privacy by design, is of interest given the introduction of the GDPR earlier this year and the NIS Directive. Linked to the NIS Directive, the smart Grid application is related to critical infrastructure, although the application was unsuccessful. European legislation places an emphasis on protecting citizens and the importance of training to avoid human errors and this is reflected in application 3 which focusses on consumer protection versus application e on bringing human factors into the cybersecurity standards process.

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 develops a security certification methodology for cyber-physical systems (CPS). CPS are characterized by safety-critical nature, complexity, connectivity and open technology. Risk scenarios may lead to complex failures and irreparable physical damage to European critical infrastructure and cost human lives.

certMILS aims to build a Multiple Independent Levels of Security (MILS) Platform which assures compositional security of cyber-physical systems that use COTS products and demonstrate the effectiveness of safety & security certification for this platform. In this way, certMILS will increase the economic efficiency and European competitiveness of CPS development.

End-users

- Public and private organizations that operate critical European infrastructure including three pilot projects where MILS will be tested
- European security certification and evaluation bodies
- Developers and researchers of COTS for critical infrastructure.

End-user benefits

certMILS will create a highly secured operating system for CPS (MILS Platform) that will offer increased security of critical infrastructure pilots and become a standard in European and global industries. Drawing from the pilot projects, certMils will produce a standardised and validated methodology for evaluating and certifying high-assurance composed systems thereby easing standard compliance of such systems for the industry and third-party developers while lowering related costs.

cyberwatching.eu Service Offer

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

Presentation at Cyberwatching.eu webinar:

https://www.cyberwatching.eu/sites/default/files/04%20-%20Architecture%20and%20composition%20in%20security%20standards_0.pdf

TRUESSEC.EU: TRUst-Enhancing certified Solutions for Security and protection of Citizens' rights in digital Europe

Jan 2017 - Dec 2019

www.truessec.eu

There is a crowded market for labelling in ICT which many businesses and citizens do not understand. The majority of labels do not go beyond what is required legally and therefore do not take an ethical approach.

TRUESSEC.EU creates online and offline discussions and synergies in the European social and academic landscape. It produces high-level research in order to identify the different criteria that could be used to assess trustworthiness of ICT products and services by citizens from multi-disciplinary perspectives: sociological, cultural, legal, ethical, technological and business.

The final goal is to make a proposal for ETEL - European Trust-Enhancing Label: a machine-readable transparency statement. This includes a self-certification process which is completed by companies involving a standard set of questions which goes beyond legal requirements and is flexible to be sector, device and platform specific.

TRUESSEC Deliverable 7.1 – Evaluation of existing trustworthiness seals and labels"[17] had as an objective "*to summarize existing certification schemes, labels, seals and trustmark related to trust in Information and Communication Technology (ICT) products and services. It covers a total of 24 schemes, analyzed individually against a set of 23 criteria designed to represent the scheme's general identity, functioning, positive and negative aspects*." From the results of this study, it appears that the data collection

[17] TRUESSEC Deliverable D7.1 (https://truessec.eu/content/work-package-7-recommendations-trustworthiness-enhancement-labels)

process in this exercise proved to be difficult due to the **general lack of transparency and publicly available information**.

It was difficult for a European consumer to find information on a seal awarded to an ICT product or service, and evaluate the trustworthiness. Certification initiatives struggled to generate engagement and acknowledgment by the public. Thus, again, **there needs to be specific guidance and easily retrievable information to make the certification process easy and understandable by the end user.**

End-users

- Citizens and increasing their trust in DSM services
- ICT Businesses and digital companies looking to increase the trust of their customers.
- Governmental bodies and businesses that want to make ICT security certification accessible to European citizens
- Governmental bodies and businesses that aim to enhance the Digital Single Market for which citizen trust is essential
- European scientists and interest groups that want to participate in the discussion towards building ICT social trust as well as citizens in general who want to feel safe online.

End-user benefits

Businesses will be able to learn from trust-enhancing best practices thereby being better able to benefit from the Digital Single Market, governments will be able to progress in increasing the trust of their citizens in ICT products thereby allowing them to expand their purchasing options throughout the Digital Single Market, scientists and interest groups will be able to contribute in the European digital transformation by promoting their views towards policy recommendations and best practices for the certification of trust in ICT products and services.

cyberwatching.eu Service Offer

https://cyberwatching.eu/truesseceu-trust-enhancing-certified-solutions-security-and-protection-citizens%E2%80%99-rights-digital

Presentation at Cyberwatching.eu webinar: https://www.cyberwatching.eu/sites/default/files/09%20-%20TRUESSEC.EU_.pdf

EU-SEC: The European Security Certification Framework

Jan 2017 – Dec 2019

www.sec-cert.eu

EU-SEC is working to create a European framework for the certification and concept evaluation of cloud infrastructure security where existing national and international certifications are harmonized and can co-exist.

In this way, EU-SEC contributes to the business value, efficiency and effectiveness of existing cloud security certification schemes and strengthens the European strategy towards a Digital Single Market. The final goal is to contribute to the trustworthiness, security and compliance of cloud infrastructures.

End-users

- EU governments
- Certification bodies
- Public and private institutions and businesses relying on cloud infrastructures, cloud service providers.

End-user benefits

The framework will allow EU governments to streamline processes, mechanisms and tools for continuous auditing and certification of cloud infrastructures which reduces human interaction and therefore costs.

European certification schemes will become more established in light of GDPR enforcement as the framework will ensure mutual recognition of certification and reusability of already certified cloud computing components.

Consumers of cloud services will be able to demonstrate compliance to security and privacy regulations and increase client trust.

European cloud service provides will be able to ensure trustworthiness and compliance of their products across the European Digital Single Market.

cyberwatching.eu Service Offer

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

Presentation at cyberwatching.eu webinar: https://www.cyberwatching.eu/sites/default/files/03%20-%20The%20European%20Security%20Certification%20Framework%20Initial%20Results%20From%20the%20EU-SEC%20Project_0.pdf

Security Working Group – 5G Infrastructure Association within the 5G PPP (Unit E1)

5G IA SEC WG

Chairs: Pascal Bisson (Thales); Jean-Pierre Wary (Orange)

5G PPP Phase 2 projects

End-users

- Telecommunications industry: large enterprises and SMEs
- Vertical industries: 8 vertical clusters covered in the 5G PPP Verticals Cartography[18] (automotive, energy, health, industry (factories; farming), media and entertainment, public safety, smart cities[19], transport and logistics)
- Smart cities deploying 5G applications and services, including network densification (e.g. security and privacy risks related to fake small cells)
- Critical infrastructures, e.g. energy (ASM Terni, IT and ENGI, FR)
- Standards organisations with security groups working on 5G (e.g. ETSI CYBER; 3GPP – SA3; ITU Study Group 17).
- Telecommunications regulators and industry associations.

End-user benefits

Security risk management, protection and response; security monitoring and management (horizontal and across verticals), e.g.

- Security levels and related SLAs.
- Regulation compliance.
- Network slicing and isolation.
- Liability and law enforcement.
- Privacy and anti-fraud protection.
- Trust Model**.**

Security-as-a-Service, new products and services for security and privacy.

Security imperatives for telecom operators:

- Embedding security in company's DNA.
- Improving data protection.
- Increased attention to integrity.
- Monetising security.
- **Interactions with enterprise CISOs.**
- **Open and transparent testing standards.**

New 5G security architecture.

Security enhancements through 5G standards for implementation, including trust model (e.g. 3GPP – SA3).

Outputs and related work

5G PPP Phase 1 Security Landscape, June 2017

5G PPP Phase 2 Security Landscape (forthcoming)

5G PPP Phase 2 – Verticals Security Landscape (forthcoming)

ENISA, Security Considerations in 5G network slicing, October 2018 (draft)

[18] https://www.global5g.org/cartography.

[19] http://www.bbc.co.uk/news/business-45952693.

3GPP Technical Specifications Release 15 (ratified); Release 16 (forthcoming)

3GPP 5G Security, A. Prasad et al, June 2018, River Publishers

A synergy could be established with the 5G IA SEC WG to share new knowledge emerging on cyber/network risks, on-going research and standardisation work in a landscape where cyber-attacks could increase in number and severity. The synergy could help identify standardisation gaps and future R&I priorities, which would also benefit EC policy makers and the DSM strategy.

2.5 European Standardisation Bodies

Standards are mainly initiated according to market needs and, therefore, industry plays an important role in order to ensure that goods and services meet the requirements of European policies and regulations. Within Europe, the key players in the development of European standards are the following organizations (as identified in European Regulation 1025/2012, articles 2 and 4):

- The **European Committee for Standardisation (CEN),** a private international non-profit organization, brings together the National Standarization Bodies (NSB) of 33 European countries, providing a platform for the development of European Standards and other technical documents in various fields (products, materials, services and processes). Industry can only access CEN through the NSBs.
- The **European Committee for Electrotechnical Standardisation (CENELEC),** also a private international non-profit organization, is responsible for standardisation in the electro-technical engineering field. At an international level, CENELEC also creates market access through its close collaboration with the International Electrotechnical Commission (IEC). Industry can only access CENELEC through NSBs.
- The **European Telecommunications Standards Institute (ETSI)** produces globally-applicable standards for information and communications technology (ICT) (including fixed, mobile, radio, converged, broadcast and internet technologies). ETSI's objective is to produce and maintain the technical standards required by its members. Access is not restricted and industry can get directly involved in the process of standards development.

CEN and CENELEC have outlined their objective for 2020 in their "Ambitions 2020".

A joint group, the "Cyber Security Coordination Group (CSCG)", of the three officially recognized European Standardisation Organizations (CEN, CENELEC and ETSI) was formed in 2011 with a mandate to provide strategic advice on standardisation in the field of IT security, network and information security and cyber security. ENISA also participates in CSCG.

In ETSI document TR 103 456 [20], the following recommendations were published:

- *“There is basically no cyber security standards gap*
- *There are several standards available, perhaps one could note, even too many, and many are not actionable or particularly useful*
- *The real need is to converge toward useful, practical, actionable, interoperable sets of standards*
- *Standards that are not freely available on-line, constantly evolving, and well-versioned have diminished value and represent cyber security impediments*
- *TC CYBER sought to discover the ecosystem and focus on identifying the most effective platforms and specifications and that have the broadest industry support”*

ENISA Publication “Gaps in NIS Standardisation”[21], page 4:

“A significant concern consists in the fact that EU Regulation No 1025/2012 referenced by the NIS Directive only defines a small handful of organisations as constituting standardisation bodies. This is not an accurate reflection of the current state of the market, nor those used within the highly specialized sectors to which the Directive applies.”

The recommendations of this report include extending the technical basis for information sharing in the following ways:

- Adoption of threat exchange open standards based on the globally accepted STIX/TAXII/CyBOX platform to be prepared as an EN defining the syntax and semantics of the data and the necessary transfer protocol, and an accompanying guide to the implementation of the standard.
- Extension of the risk analysis and defensive measures capabilities defined in current standards to allow Member States to address the provisions necessary to mitigate risk both at national and regional level. This should be prepared as an EN extending the capabilities already described in ETSI TS 102 165-1 [i.7], ETSI TR 103 305 [i.3], ISO/IEC 15408 [i.25] and in relevant ISO/IEC JTC1 27000 series standards [i.16]. It is noted that it is not possible to separate provisions for NIS from general provisions for cyber security which have been developed by a broad array of ICT standards bodies. It is also noted that NII, NIS and cyber security cannot be geographically isolated in its provisioning, in the origin of attack, or in defense measures, and that this distributed complexity should be considered in implementation of the necessary information sharing required for effective NIS. Thus many of the capabilities of the NII will of commercial necessity be implemented using software and hardware from a global market.

[20] https://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf

[21] Op cit ENISA “Gaps in NIS Standardisation”, page 4:

3 International Perspectives

3.1 International Standardisation Bodies

The International Organisation for Standardisation (ISO) is an independent, non-governmental international organisation with membership of 162 national standards bodies and 786 technical committees and subcommittees. It is the dominant developer and publisher of international standards in terms of scope with 22,359 international standards and related documents. One of the best-known standards for information security management systems is the ISO/IEC 27001 family.

The International Telecommunications Union (ITU) is an "intergovernmental public-private partnership organization" which develops international standards in telecommunications known as ITU-T Recommendations. Launched in 2012, 'IMT for 2020 and beyond' is ITU's program for 5G, setting the stage for 5G research activities around the world. The process is planned for completion in 2020, when a draft new ITU-R Recommendation with detailed specifications for the new radio interfaces.

https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx

The 3rd Generation Partnership Project (3GPP) is the international telecommunications standardisation body developing standards for 5G, the next generation of mobile communication systems. 3GPP releases are submitted to ITU after ratification. SA3 (services and system aspects) is a working group within 3GPP responsible for standardizing security enhancements for 5G as an evolution of 4G mobile communication system, i.e., system architecture evolution/long term evolution (SAE/LTE). Key enhancements over 4G include: access agnostic primary authentication with home control, security key establishment and management, security for mobility, service-based architecture security, inter-network security, privacy and security for services provided over 5G with secondary authentication.

http://www.3gpp.org/ - http://www.3gpp.org/specifications-groups/sa-plenary/sa3-security

3.2 H2020 Projects with international scope

The following H2020 projects with an international scope have been listed hereafter to learn from their findings as produced in certain deliverables.

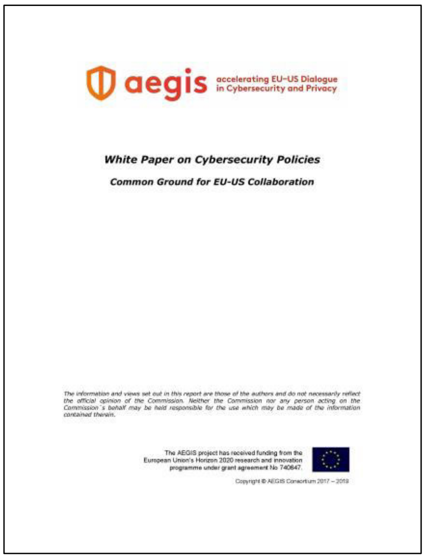
3.2.1 AEGIS Project

The AEGIS Project, a Coordination and Support Action (CSA) funded by Horizon 2020 (the EU framework program for research and innovation) that aims to facilitate EU-US dialogue and cooperation in cybersecurity and privacy research and innovation (R&I), has developed this White Paper to capture the current landscape of cybersecurity policies on both sides of the Atlantic.

AEGIS published the following deliverables which provide some insight into the international cybersecurity landscape:

- **White Paper on Cybersecurity Policies** – Common Ground for EU-US Collaboration[22] (May 2018)

> *"This Paper focuses on three policy areas which impact bilateral cyber dialogues and research and innovation collaboration between the EU and the US. The three policy areas are: Standards and certification; privacy and data Protection; and public-private information sharing."*



aegis accelerating EU-US Dialogue in Cybersecurity and Privacy

White Paper on Cybersecurity Policies

Common Ground for EU-US Collaboration

The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the Commission. Neither the Commission nor any person acting on the Commission´s behalf may be held responsible for the use which may be made of the information contained therein.

The AEGIS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740647.

Copyright © AEGIS Consortium 2017 – 2019

- **Report on Cybersecurity and Privacy** R&I Priorities for EU-US Cooperation[23] (2018)

> *"The report on Cybersecurity and Privacy Research and Innovation (R&I) priorities presents the results of a survey conducted by the AEGIS project in the EU and the US to identify R&I priorities for future collaboration in cybersecurity and privacy between both regions."*

aegis accelerating EU-US Dialogue in Cybersecurity and Privacy

Report on Cybersecurity and Privacy R&I Priorities for EU-US cooperation

The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the Commission. Neither the Commission nor any person acting on the Commission´s behalf may be held responsible for the use which may be made of the information contained therein.

The AEGIS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740647.

Copyright © AEGIS Consortium 2017 – 2019

[22] AEGIS Project White Paper on Cybersecurity Policies (https://drive.google.com/open?id=1qkvmaxFzPQwjB0T_BxjvdxUtRfPBot34)

[23] AEGIS Report on Cybersecurity and Privacy (https://drive.google.com/open?id=1nieB-rb1fs0y1_MhFVOtsvB1VOi0f1XJ)

3.2.1.1 Key findings taken from the AEGIS publications

The following findings with respect to standards have been extracted from the above-mentioned AEGIS publications[24].

Cybersecurity Key points	EU	US	Similarities	Differences
Standards	NIS Directive: Law creates a common set of security standards that Member States must adhere to in order to be adequately prepared in case of a cyber attack. Also creates standards for operators of essential services in the EU. **Cybersecurity Act**: Legislative proposal would create a cybersecurity standards and certification scheme for ICT products in the EU. Certificates would be recognized by all Member States. **Liability standards in the EU**: No legislation that comprehensively address liability when it comes to new technologies or liability in the case of a cyber attack. **eID Regulation**: eID would allow citizens of one European country to access services they have a right to in other EU countries by showing an ID.	**NIST Framework**: Voluntary cybersecurity standards for the public and private sector. The framework aims to help companies safeguard their systems with flexible standards that help them "identify, prioritize, manage and/or communicate cyber risks." **Standard setting in the US**: Coordinated through the Department of Homeland Security. Adopts private sector consensus based standards if possible. **Liability standards in the US**: Liability laws are piecemeal and there is no comprehensive legislation in this area. There are federal, state and municipal laws.	**Improve cyber preparedness**. The NIS Directive and the NIST Framework aim to improve cyber preparedness of public and private sector entities. **Best measures available**. The NIS Directive and the NIST Framework call on entities to use the best cybersecurity measures available. **Not one-size-fits-all**. Neither NIS or NIST are a one-size-fits-all solution. They recognize that organizations must employ measures that make sense for them and their specific risks. Voluntary standards are important. The certification framework for ICT products under the Cybersecurity Act would not be mandatory in the EU.	**Law vs. voluntary standards**. The NIS Directive is a law that must be followed by all EU Member States and operators of essential services. NIST is a voluntary framework that organizations can choose to adopt if they so wish. **EU appears to be actively working on harmonizing and clarifying liability standards.** It has called for the formation of a working group on this matter. There is no similar effort on a federal level in the US, although states and municipalities are active.

[24] Ibid AEGIS Project - Report on Cybersecurity and Privacy R&I Priorities for EU-US cooperation.

Cybersecurity Key points	**EU**	**US**	**Similarities**	**Differences**
			Meanwhile, DHS always works to adopt voluntary standards adopted by the private sector. **Liability is not clearly defined**. Liability is mentioned in both regions at various levels but not defined at a comprehensive level or EU level.	

Table 6: Taken from AEGIS Project "White Paper on Cybersecurity Policies"[25]

Relevant recommendation from AEGIS Project "White Paper on Cybersecurity Policies - Common Ground for EU-US Collaboration" [26]

> *"Near term attainable milestones:*
>
> *2. Increase synergy and collaboration between the agencies responsible for the NIST Framework and those tasked with implementation of the NIS Directive and the GDPR. The desired outcomes are a common framework, standards and practices that facilitate compliance by companies in the EU and the US. …*
>
> *3. Adopt a common and **harmonised language for stakeholder communication, which will accelerate EU-US collaboration in cybersecurity.** This goal can be achieved through requests for feedback in consultation with relevant industry representatives to advise and inform government officials who are charged with developing agreed-upon terms and taxonomy."*
>
> *"Longer term benchmarks*
>
> *3. Promote the adoption of a unified approach based on international standards to foster collaboration in cybersecurity R&I across the Atlantic. A unified approach will allow EU researchers to develop products and services that have the capabilities to compete in the highly-competitive US market and other international markets. Collaborating on the development of common standards in ICT and ensuring those standards remain voluntary, consensus-based and market-led are critical to this unified approach. "*

[25] Ibid AEGIS P

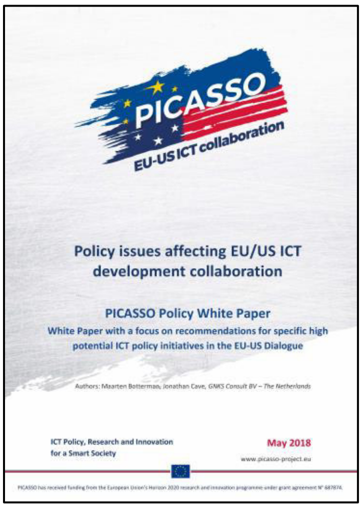
[26] Op cit AEGIS

3.2.2 PICASSO Project

The project PICASSO "ICT Policy, Research and Innovation for a Smart Society: towards new avenues in EU-US ICT collaboration", brings together EU and US prominent specialists with the aim of reinforcing EU-US ICT collaboration in pre-competitive research in key enabling technologies related to societal challenges of common interest – 5G Networks, Big Data, Internet of Things and Cyber Physical Systems – and to support the EU-US ICT policy dialogue

- **Policy issues affecting EU/US ICT development Collaboration**[27] – PICASSO Policy White Paper (May 2018)

> *"This paper brings together insights relating to the reciprocal relation between policy and the further development, and thus R&I collaboration on development, of 5G networks; Big Data; and IoT/CPS."*


PICASSO
EU-US ICT collaboration

Policy issues affecting EU/US ICT development collaboration

PICASSO Policy White Paper

White Paper with a focus on recommendations for specific high potential ICT policy initiatives in the EU-US Dialogue

Authors: Maarten Botterman, Jonathan Cave, GNKS Consult BV – The Netherlands

ICT Policy, Research and Innovation
for a Smart Society

May 2018

www.picasso-project.eu

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

Proposals taken from PICASSO project "PICASSO Policy White Paper"[28]

> *"**Strategic Proposals for the Way Forward:***
>
> *Considering all we learned during the course of the study, we conclude with the following strategic proposals for possible ways forward, that we believe will be supportive to effective, further enhanced ICT R&I collaboration between the European Union and the United States of America.*
>
> 1. *Privacy: Solutions need to be found to allow services to develop that respect (European and US) privacy and data protection frameworks and – _where appropriate – _challenge their provisions. This will require policy collaboration that is looking forward to joint and sustainable solutions aimed at ensuring an even higher level goal than preserving privacy: that of preserving "human dignity*" in a digital age, ensuring that we can still live as humans in our digital environment*
>
>   *a. These approaches should not treat current laws as fixed constraints, but as natural experiments that can shed light on how to improve the ethical character of law and practice, and at a deeper level on the ethics of privacy itself;*
>
>   *b. As part of this, the adequacy of principles such as user empowerment, consent and restricting privacy policy attention to data protection should be examined theoretically, practically and empirically.*

[27] PICASSO Project, Policy issues affecting EU/US ICT development Collaboration (May 2018) (http://www.picasso-project.eu/wp-content/uploads/2018/06/PICASSO-Policy-White-Paper-Final-v1.pdf)

[28] Ibid PICASSO

Proposals taken from PICASSO project “PICASSO Policy White Paper[29]

> 2. *Security: Recognising basic security is key to whatever we want to ensure: set up joint EU/US research collaboration to develop biologically inspired security. With IoT and underlying interconnections, there’s a significant risk with IoT devices providing a back door to enterprise systems and data. Using biological constructs (in particular those relating to immune responses and contagion), we may be able identify attacks before they become widespread and respond in a proportionate and dynamic fashion by directing resources to the appropriate area. As part of this*
>
>   a. *Security roles and responsibilities should be explored as negotiable, flexible and layered, especially as regards technological, operational, commercial and regulatory domains; and*
>   b. *The common aspects of security and privacy (both of which concern access to information and the functions and systems it enables) should be recognised and a common technical, operational, business and legal basis explored.*

3.2.3 EUNITY Project

The EUNITY project aims to encourage, facilitate and develop the dialogue between Europe and Japan on cybersecurity and privacy research and innovation trends and challenges, in order to foster and promote cybersecurity activities in both regions.

- Deliverable 3.1 - Preliminary version of the Cybersecurity Research Analysis Report for the two regions[30]

> *“This document contains a description of legal and policy aspects, research and innovation aspects as well as industrial and standardisation aspects. It contains a review of the mechanisms used to finance research and innovation in Europe and Japan, a review of the main research directions in the field, and identification of the strong and weak points in the European and Japanese research landscape.”*

H2020 FRAMEWORK PROGRAMME

H2020-DS-SC7-2016
DS-05-2016

EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation

Cybersecurity and privacy dialogue between Europe and Japan[1]

Deliverable D3.1: Preliminary version of the Cybersecurity Research Analysis Report for the two regions

Abstract: This document contains a description of legal and policy aspects, research and innovation aspects as well as industrial and standardization aspects. It contains a review of the mechanisms used to finance research and innovation in Europe and Japan, a review of the main research directions in the field, and identification of the strong and weak points in the European and Japanese research landscape.

[1] The research leading to these results has received funding from the European Union H2020 Programme under grant agreement n° 740507.

[29] Ibid PICASSO

[30] EUNITY project D3.1 - Preliminary version of the Cybersecurity Research Analysis Report for the two regions (https://www.eunity-project.eu/m/filer_public/53/4a/534abeb6-6532-4c59-a4ae-22ac91b3d885/eunity-d31.pdf)

In this report, the common areas of interest in industry in both regions are described. A few are mentioned hereafter, namely, 5G, Next Generation Network (NGN), big data, IoT, Artificial Intelligence (AI), VR/AR, High Performance Computing (HPC), distributed OS.

Some of the areas which need the most collaboration between Europe and Japan, as listed in EUNITY Deliverable 3.1[31] are given below:

> *"*
>
> - *education and awareness*
>   - *education on various levels,*
>   - *enhancing security awareness,*
>   - *development of human resources,*
>   - *promoting the exchange of personnel,*
> - *standards and regulations*
>   - *harmonization on standards and regulations among government and industrial*
>   - *association ,*
>   - *guidelines by industry sector,*
>   - *sharing best practices regarding cybersecurity, procedures,*
> - *information sharing*
>   - *sharing environments to monitor attacks,*
>   - *sharing security intelligence among security vendors/organizations,*
>   - *continuous information feeds on web sites ex. blog, whitepaper,*
>   - *continuous exposure in conferences/exhibitions,*
>   - *continuous workforce activities ex. industry ISAC.*
>
> *Other activities which could be performed together are the following:*
>
> - *Interpol-like cooperation and non-aggression treaties,*
> - *improve communication, information/data sharing, legal framework,*
> - *harmonize legal and penal frameworks to ensure effective prosecution of cybercriminals,*
> - *reduce administrative,*
> - *intensify collaboration between CERT/CSIRT teams,*
> - *promote joint initiatives (including meetings and workshops).*
>
> *Certainly boosting the responsiveness of Europe as a whole and fostering cooperation and coordination in cybersecurity between Member States and Japan is a very important issue. There is a need of industry-government cooperation and global collaboration to exchange sensitive data and to enlarge the cooperation to as many countries and industry sectors as possible. Global collaboration shall not only be horizontal, i.e., limited to state entities, nations and international organizations. Rather, global cooperation should be horizontal and vertical, i.e. also involving private entities and other stakeholders (academia for instance).*

In summary, for the H2020 projects mentioned above, the common challenge is to stimulate dialogue, collaboration and cooperation on a global level to ensure that the European market access and vice versa is open to encourage economic growth. Education, awareness training in regulatory requirements of block regions would assist in furthering the opening of such markets. Furthermore, in such an international dialogue, a common language taxonomy in cybersecurity would accelerate collaboration in cybersecurity.

4 Survey to identify Gaps in the Cybersecurity Standards and Certification Environment

In order to obtain current feedback from the EU cybersecurity projects, cybersecurity users (public and private sectors), and cybersecurity products and services providers, a survey was launched to identify the gaps in cybersecurity standards and the certification environment. The results and the analysis of those results of this survey are included as part of this deliverable.

4.1 Focus of the survey

The focus of the survey was to learn from the user community where they could identify gaps in the current and existing cybersecurity standards and certification environment.

4.2 Identification of stakeholders

The stakeholder group was identified as public sector, private sector (large and small and medium-sized enterprises), EU projects, academic, research. 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 (± 43 contacts)
- TRUST-IT to the contacts from H2020 projects database, some ± 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
- AON through their 25/30 contacts
- CONCEPTIVITY to ECSO partners to ± 230 companies via their newsletter
- CONCEPTIVITY through LinkedIN, 7000 contacts, three repeat posts
- CONCEPTIVITY to EOS - published in the EOS newsletter
- CONCEPTIVITY through personalized messages
- European Commission through their newsletter of September 2018
- Cyberwatching.eu web site's portal contained the survey for four months
- Cyberwatching.eu Webinar – 50 participants
- Cyberwatching.eu Annual Event – 30 participants

4.3 Dissemination of the survey

The online survey (ANNEX C) was widely disseminated by e-mail, social media (twitter, LinkedIn), and published on the cyberwatching.eu website at the end of June 2018. The objective was to solicit feedback from stakeholder communities on the gaps in the current and existing cybersecurity standards and certification environment.

The survey was launched at the end of June 2018 and kept open until mid-October. Due to the summer holiday season and an initially limited response, 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 August and September. The survey was also distributed to the participants of the Webinar in September 2018 and to participants at the Annual Cyberwatching event in Krakow in October 2018.

With the wide distribution as described above and several reminders to the large number of recipients of the survey communication, 31 replies were received from the following countries: Cyprus (1), Finland (2), France (1), Greece (4), Ireland (1), Italy (2), Netherlands (1), Romania (2), Spain (9), Switzerland (2), United Kingdom (4), United States of America (2). The replies covered 10 EU countries. The breakdown category of the responses was:

- 29% were from the industry,
- 23% non-for-profit,
- 19% universities
- 16% SMEs,
- 7% governmental
- 6% were not specified.

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

4.4 Analysis of Response to the Online Survey

Although the survey was completed by only 31 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.

4.4.1 Survey Question 1 – Usage of cybersecurity standards

Question 1:

Are you using cybersecurity standards (and/or certification) in your work efforts?

Figure 1 below provides an indication of the type of stakeholder group which responded to the survey.

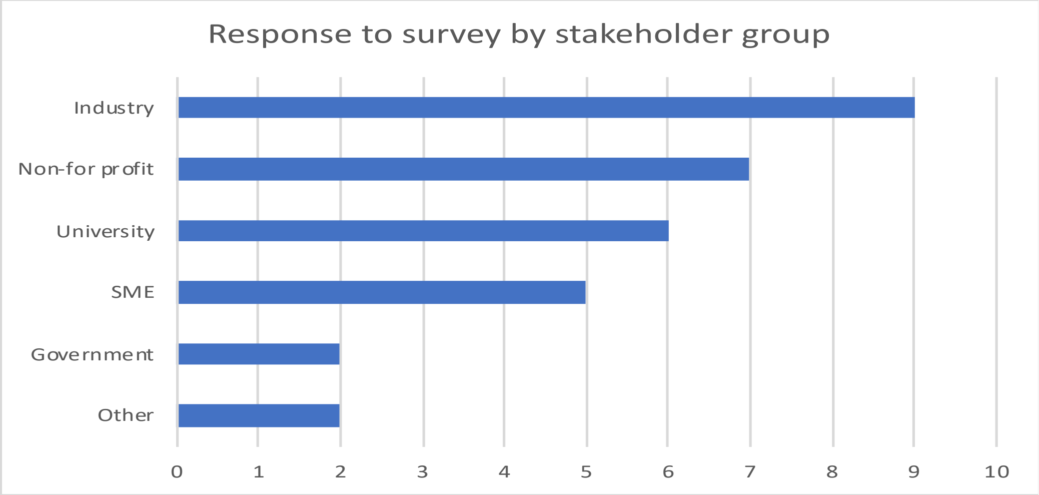


Figure 1: Response to survey by stakeholder group

72% responded affirmatively that cybersecurity standards and/or certification were used at work. Of this positive response, 14 replies were from people involved in EU projects, two responses were from USA.

4.4.1.1 Survey Question No. 1A

Question 1A:

In which areas are these standards (certification)?

The survey prompted the responder to identify in which categories standards and/or certification were used. The majority identified "software", followed by "organization" (e.g. ISO 27000 family), followed by devices (as given in Figure 2 below).

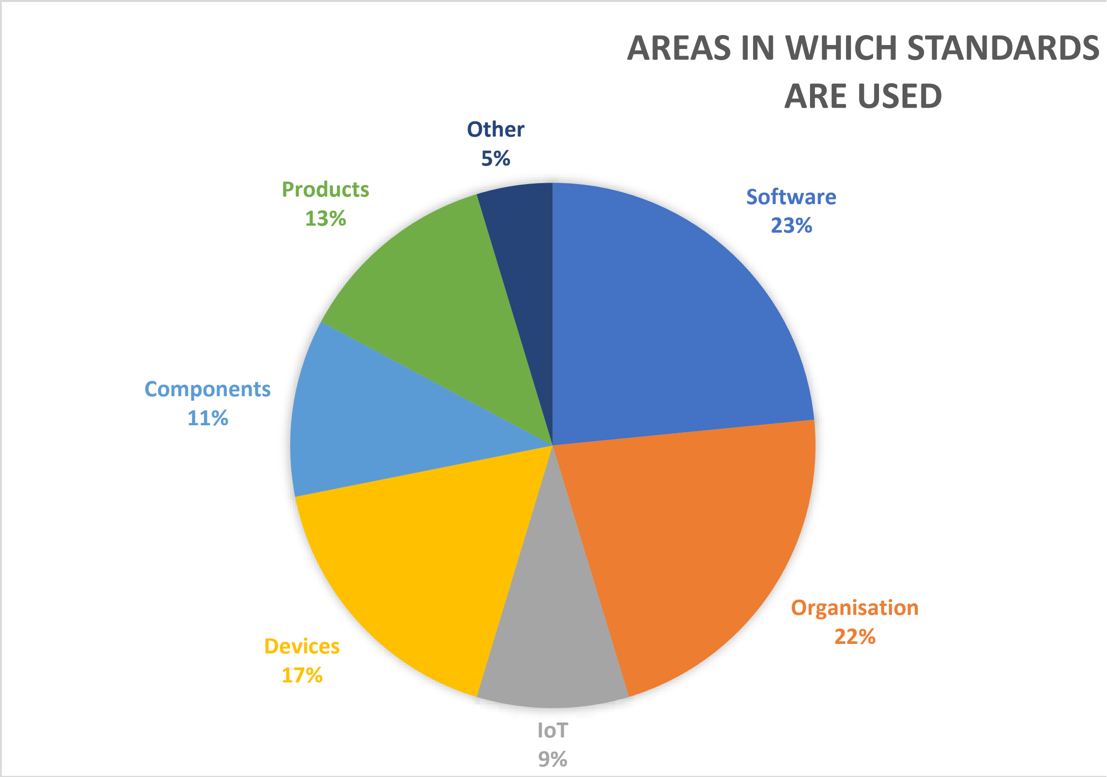


Figure 2: Areas in which standards are used

4.4.1.2 Survey Question No. 1B

Question 1B:

If you know the standards/certification used, can you list them here?

A variety of standards/certifications were listed as being used, the most common ones being the ISO 27000 family, ETSI and others covering several areas (information security management, risk management, software testing, conformance testing, payment card industry etc.), as given below in Table 7:

Type of standard	Standard	Area
ISO:	ISO/IEC 27001	Information security management
	ISO/IEC 27000	Information security standards

Type of standard	Standard	Area
	ISO 31000	Risk management
	ISO 29119	Software testing
	ISO 17065	Standard for certification bodies
	IS0 17024	Conformity assessment requirements for certification
	ISO 19086	
	ISO/IEC 15408	Security techniques – Evaluation criteria for IT security
CEN-CENELEC	ENS (not specified)	
ETSI	ETSI TS 102 871-1 V1.4.1 (2017-05)	Conformance test specifications for GeoNetworking
	ETSI EN 302 636-4-1 V1.3.0 (2017-05)	Vehicular Communications; GeoNetworking;
	ETSI TR 102 893 V1.2.1 (2017-03)	Threat, Vulnerability and Risk Analysis
	ETSI TR 103 099 V1.4.1 (2017-03)	Architecture of conformance validation framework
	ETSI TS 102 869-1 V1.5.1 (2017-03)	Conformance test specifications for Decentralized Environmental Notification Basic Service
National Institute of Standards and Technology (USA)	NIST framework	Cybersecurity
IEC	IEC 62351	Security in automation systems in the power system domain
IEE	IEEE 1686	Standard for intelligent electronic devices

Type of standard	Standard	Area
	XSG	eXtendable Scene Graph format
PCI	PCI-DSS	Payment Card Industry Data Security Standard
National certifications	Not specified	Not specified
Creative Commons	Common Criteria (2)	
ANSSI	CSPN	Certification de Sécurité de Premier Niveau
	UL CAP	UL Cybersecurity Assurance Program
Commercial Product Assurance scheme	CPA	Not specified
	CSA CCM	
	WSAGreement GFP.192	

Table 7: Standards used by respondents

4.4.2 Survey Question 2 – List of standards/certification used

Question 2:

Do you see any gaps in the current cybersecurity standards (or certification)?

- 84% responded affirmatively
- 16% responded negatively

4.4.2.1 Survey Question 2A

Question 2A:

In which areas are these (gaps) in standards (certification)?

The areas in which these perceived gaps in standards and/or certification are given in Figure 3, i.e., IoT, devices, software, and information security management were of the most concern.

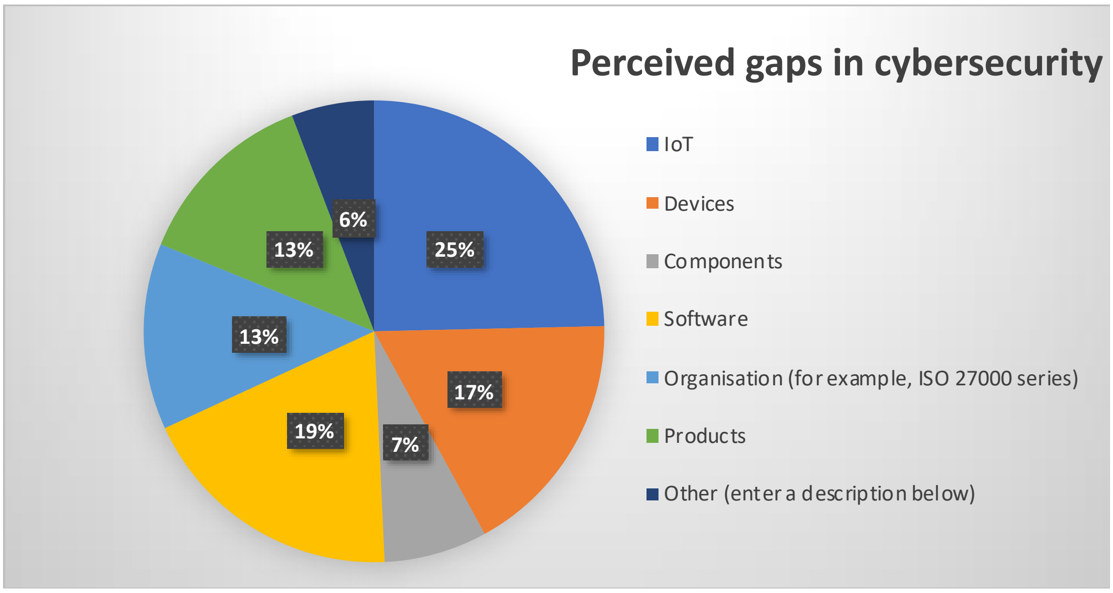


Figure 3: Perceived gaps in cybersecurity

4.4.2.2 Survey Question 2B: What are those gaps?

Question 2B:

And specifically, what are those gaps?

In describing the gaps in further detail, it is no surprise to find very similar responses as already expressed within the state of play described in Chapter 2. Some main concerns are:

- Standards in some industry sectors are very well defined but for other areas, there is a **pronounced lack of standards** (including technical interoperable standards) and certification. In particular, a lack of protocol and standards for **IoT and devices** was mentioned in several instances. A given example was that standards and protocol for IoT products related to ocean activities was not available. Furthermore, there is a big gap in **certification of IoT products and devices** and little knowledge of where the cybersecurity risks lie with respect to IoT. A minimum cybersecurity level for market access requirement would seem necessary and a pragmatic approach. IoT products and devices present further challenges related to scalability, automation, specific threats for IoT.
- **Lack of common terminology – this makes it difficult**

- **Lack of definition of cybersecurity risks –** a complete view of security is missing
- **New technologies are emerging very fast.** Several problems occur: for example, whilst the initial platform for new technologies may be limited, as the technologies expand to government platforms, a corresponding secure framework is necessary and there is a concern in keeping up the pace with emerging technologies.
- **Standards and certification will constantly need to evolve.** In order to adapt to the evolving business landscape, standards and certification schemes will also need to keep up with the fast pace of innovation. On the other hand, concern was expressed that the development of standards does take time and interim measures would need to be taken. To add to the complexity, in today's business ecosystem, standards are still immature and do not fully address the platforms of extended enterprise and multiparty trust. Concerning components and devices, common criteria is considered good but how it is applied still remains outdated and changes to meet current and future market requirements. Agility, flexibility and cost-efficiency were attributes which need to be taken into consideration.
- **Lack of knowledge about the importance of standardisation and a lack of understanding of requirements.** Equally important, there is a lack of guidance as to what standards should be used
- **Best practices in secure coding** are lacking. This leads to the **need for security by design.**
- **Certification scheme**. One scheme would be better than multiple schemes which becomes costly and cumbersome. Overlaps in certification should be overcome. With the GDPR, a standards and certification scheme on privacy and security is required.
- **Trust, Ease of use and product safety** remain important factors

4.4.3 Survey Question 3 – Is risk assessment comprehensively addressed

Question 3:

In your opinion are risk assessment, risk management and risk mitigation comprehensively addressed and is this fit for purpose within the current and existing cybersecurity standards?

As given in Figure 4 below:

- 45% felt that risk assessment, risk management and risk mitigation were not comprehensively addressed and were not fit for purpose within the current and existing cybersecurity standards
- 36% affirmed that the risk assessment, management and mitigation were comprehensively addressed and were fit for purpose
- 19% were not sure

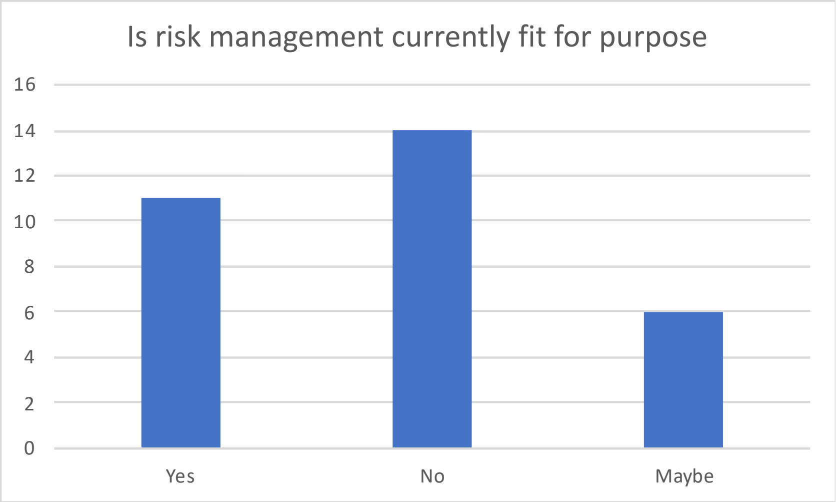


Figure 4: Current risk management is not fit for purpose

4.4.3.1 Survey Question 3A and 3B

Question 3A:

If your answer is “No” or “Maybe” - how can this be improved?

The following response was received to indicate the direction of improvement:

- 46% of the responders felt it important to **create a new "fit for purpose" cybersecurity risk assessment, risk management and risk mitigation standard**
- 36% of the responders felt it important to **improve risk assessment, risk management and risk mitigation elements** within the **current existing standards**
- 18% of the responders felt it important to **improve specific standards** such as ISO 27000 with respect to the risk assessment, risk management and risk mitigation aspects

Question 3B:

Further explain your answers in the text box below

From the additional explanations received through the survey, the following needs or issues emerged:

- **Ease of use in standards and a clear common-language guide** will lead to faster adoption
- **Risk management** needs to be **part of the culture** and not seen as an additional task

- As cybersecurity technology and risks evolve, it was felt that new standards and tools would be required to address **new risks**
- **Cost is an issue** which needs to be overcome: For SMEs, this is particularly important as the processes are time consuming, often requiring specialised personnel
- **Risk assessment** could be improved by providing for an automated approach which would result in a more objective assessment
- **Raise awareness in society** about real risks: case studies close to real life situations could make society more conscious
- **Feed the risk assessment framework**: provide information about data of cyberattacks and intentions in order to understand the risks out there
- Tools such as **cyber insurance** could be a potential risk-mitigation solution

4.4.4 Survey Question 4 – Greatest concerns in cybersecurity standards/certification

Question 4:

What are your 3 greatest concerns about the cybersecurity standards/certification? (Select the three most relevant ones)

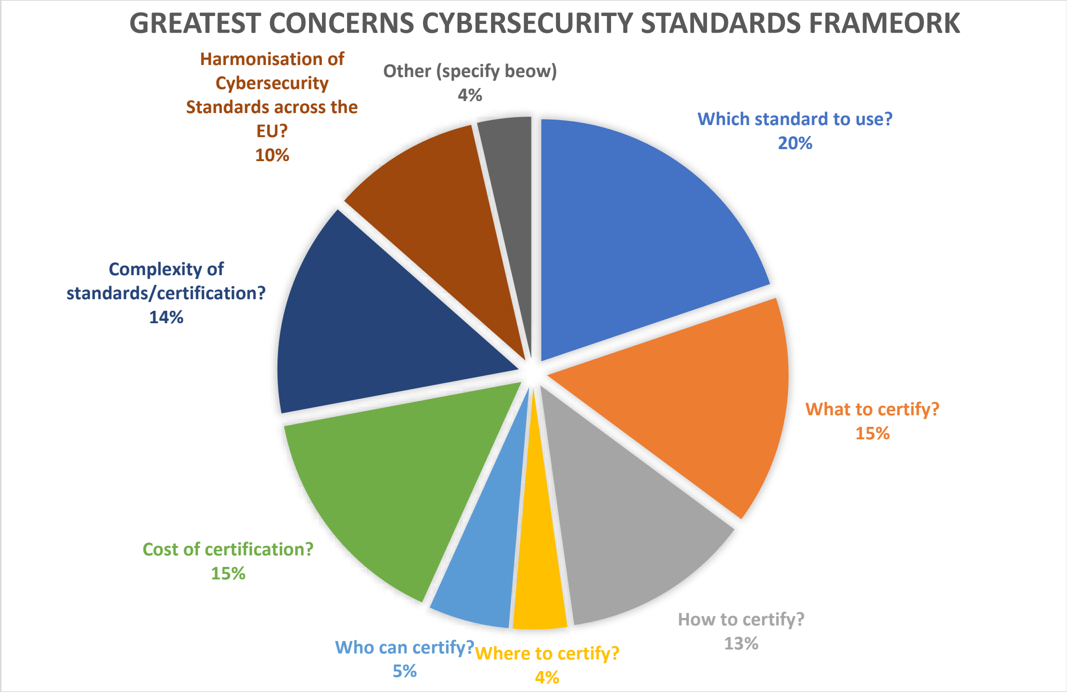


Figure 5: Greatest concerns in the cybersecurity standards framework

The greatest concerns in a cybersecurity standards framework are:

- **Which standards to use?**

From the multitude of national and international standards in a complex and confusing landscape, there is difficulty expressed in identifying **which standards to use**. For example, technology developers found that there were **too many standards** and which to select for the certification of their products.

- **What to certify?**
  What actually needs to be certified is also not clear – would it be the software, processes, cybersecurity measures. The scope should be clear. With emerging technologies, the task of **what to certify becomes even more difficult.**

- **Cost of certification**
  Certification becomes costly across a varied landscape with different certification approaches. There is a direct cost plus the time dedicated to certification. Furthermore, the process is slow and becomes costly. The certification process also does not keep up with the speed of innovation. Unfortunately, cost can be a hindrance to cybersecurity.

- **Complexity of standards/certification**
  There is a multitude of standards together with a very wide range of certification schemes in a complex European and international market. The different approaches at the national level adds to the complexity: for example, comparison of certified devices becomes more difficult when different certification approaches are used, different processes, lengthy and time-consuming approaches, too much formal documentation, added costs. Insufficient guidelines are available. The importance of standards and certification should be conveyed through education. Another angle is that products and systems themselves are so complex – it is difficult to clarify which parts need to be certified and how to compile a composition of certificates.

- **Harmonisation of cybersecurity standards across Europe**:
  There is a clear conflict which occurs at the European level (Cybersecurity Act) and at the national level. Mutual recognition of standards in the EU would need to be further examined.

4.4.5 Survey Question 5 – Known harmonized cybersecurity standards/certification

Question 5:

Are you aware of any cybersecurity standard(s)/certification that has/have been harmonised across the EU member states?

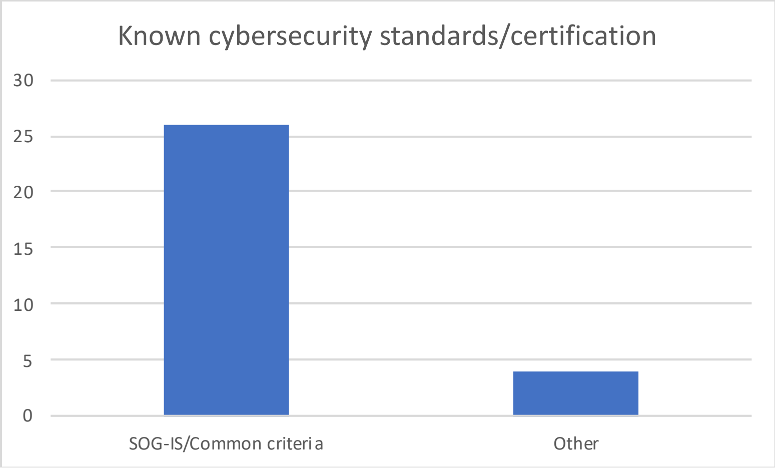


Figure 6: Known cybersecurity standards/certification

The most known cybersecurity standards/certification is SOG-IS/Common Criteria.

4.4.5.1 Survey Question 5B

Question 5B:

Please provide any additional feedback concerning harmonization of cybersecurity standards/certification harmonized across the EU member states

- Europe is recognized globally for its market access regulations which should improve through a harmonization and usage of international standards developed by recognized standard-setting bodies.
- A common body is essential with the main authority. A common research agenda needs to be outlined.
- There should be at least one certification scheme in common for all EU MS with mandatory cybersecurity that guarantees a minimum of security standards.
- Not all EU Member States have recognized the Common Criteria Recognition Arrangement (CCRA) although a large number of EU MS are part of the arrangement.
- After software has been developed, it is difficult to compile information in the way required by Common criteria certification entities.
- The most recognized and standardized security certification approaches are NIST-NIST FIPS 140-X and CC. CC is the oldest ICT evaluation scheme. Whilst SOG-IS/CC is

a good start, there is still a need for adapting to future needs and also to cover the whole EU

- Re-certification should be considered and the dynamism of security. Flexibility is important
- Labs should be able to get accredited in any country and not just in the country where it is located. In this manner, a manufacturer can freely choose the country for certification and the workload is better distributed across certification bodies.
- GDPR and NIS may need specific a standard or certification scheme
- Focus is needed on enabling joint cyber defense and response through harmonized accountability and interplay
- From both an international and European perspective, guidance is lacking on the requirements in the European market. It would be useful to have a single-entry portal which provides the recognized approaches and schemes across the EU

4.4.6 Survey Question 6 – Certification costs

Question 6:

Are certification costs and the time and resources involved of concern to you?

- 86% responded affirmatively
- 14% responded negatively

Question 6A:

If yes, please select which aspects?

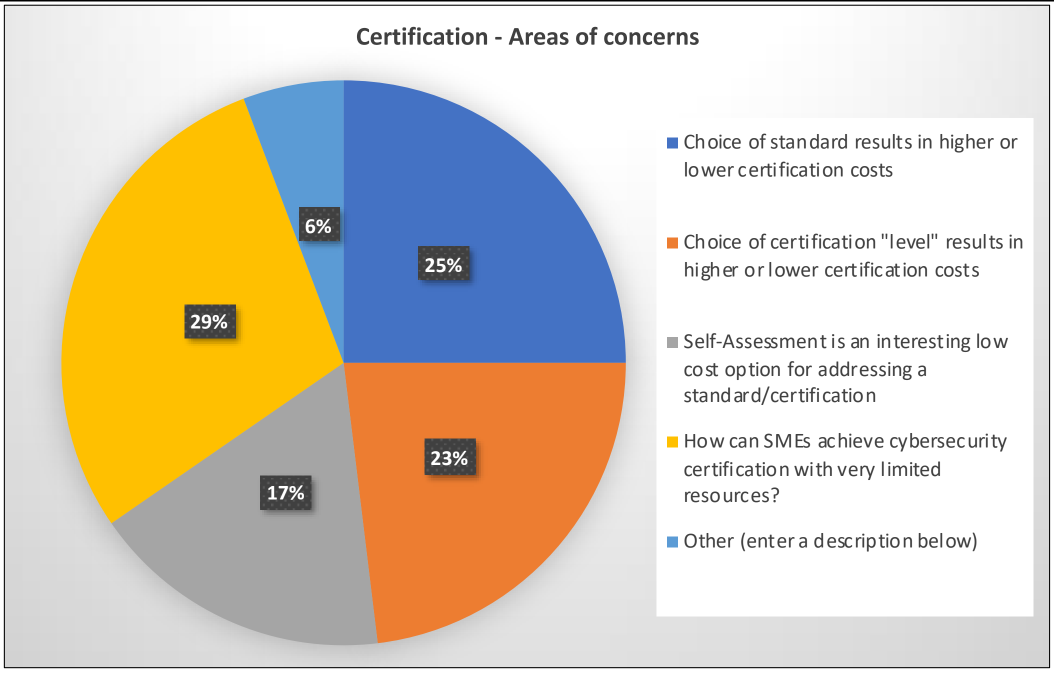


Figure 7: Certification cost concerns

Concerning concerns in the cost of certification, there was a wide range of comments, as summarised below:

- For SMEs, the cost of certification is definitely an issue. This has been repeatedly conveyed in the survey and, in particular here. First, it is not clear what to certify and once this has been determined by the choice of standard and type of certification, the costs can be very high. If compliance to a minimum standard of cybersecurity is enforced, SMEs would need support, and a suggestion is that a subsidy be provided Another suggestion is self-assessment / self-conformance. In some cases, the cost may not be the cost of certification but rather the impact of time-to-market when third party need to study the product to be able to certify it. New start-ups may have even more difficulty

- In order to plan for certification, costs need to be predictable and manageable so that budgets can be set aside. Again for SMEs, the additional overhead is an additional burden

- Once software has already been developed, the process of adapting documentation to the CC certification is time consuming and can be costly

- The level of certification of the product or system determines the cost. In a lab, it becomes unmanageable and expensive for manufacturers and more so for SMEs

- Certification requires independent third-party auditing and authorisation. Furthermore, public sector procurement may limit the choice of certifiers resulting in a possible higher cost of certification and in worst case, multiple certifiers for one certification

- From a university perspective, training in certification and acquisition of such competences is frequently requested.

- Standardized ways of (cyber)security assurance in ITS need to address the great number of 3rd party modules integrated into the vehicles. Certification costs are increased due to the complexity (large attack space) of the 'connected vehicle' paradigm.

- Risk analysis plays an important role. The level of certification should be defined upon completion of risk analysis that takes into account assets, threats, probability of occurrence, impact. The

5 Cyberwatching.eu Webinar – Cybersecurity Standards & Certification

A free Cyberwatching.eu webinar took place on September 5, 2018, on the challenges in cybersecurity standards and certification. Some of the key areas touched up were trust, harmonization, GDPR, governance, risk management, among other topics of interest within the cybersecurity community. With a slate of interesting speakers and thought-provoking topics, the webinar attracted the largest number of participants thus far, in total 50 participants, from around the globe from different fields, as can be seen in Figure 8: below:

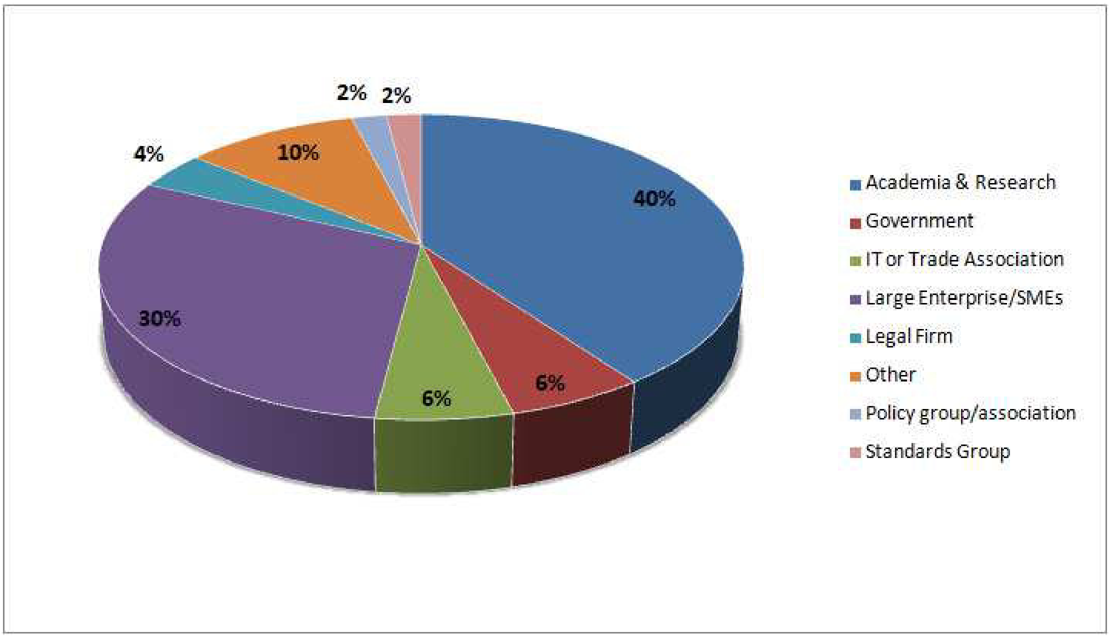


Figure 8: Webinar participation according to interest group

The webinar is published online at: https://www.cyberwatching.eu/free-webinar-cybersecurity-standards-and-certification-challenges and the agenda and list of speakers is available in ANNEX D.

6 Cyberwatching.eu Annual Workshop – Krakow, October 8, 2018

The 2018 Annual Cyberwatching.eu event took place in Krakow on October 8, 2018, alongside CYBERSEC FORUM 2018. The Annual Workshop was organized into three sessions, as follows:

- International cooperation and alignment on cybersecurity and privacy issues
- The European watch on cybersecurity and privacy
- Assessing research outputs within the cybersecurity and privacy landscape

The detailed Agenda is available in ANNEX E.

The side event "**International cooperation and alignment on cybersecurity and privacy issues**“ was specifically related to research on the topic of this paper. About 30+ participants attended and displayed much interest through the many questions put forth to the speakers.

7 Cyber Risk Management

Cyber Risk is defined as “the potential of loss or harm related to technical infrastructure or the use of technology within an organization”. In fact, cyber risk is one of the most impactful sources of risk in the modern enterprise as the consequences of cyber security failures can be damaging to business revenues and brand reputation. C-level management have even lost their positions as a result of data breaches due to inept preparation and planning. It is therefore important to understand the culture of the company and how the key stakeholders answer the following questions:

- What losses would be catastrophic?
- What can we live without and for how long?
- What information absolutely cannot fall into the wrong hands or be made public?
- What could cause personal harm to employees, customers, partners, visitors?

Implementing a process of **Cyber Risk Management** is crucial because it will often be the difference between success and failure for modern enterprises. The cost of some cyber security failures can be measured in monetary units and other costs are more difficult to quantify:

A. ***Hard currency costs***: include fines, legal fees, lost productivity and mitigation, remediation, and incident response, fines from lack of compliance.
B. ***Qualitative and long-lasting***: include diminished brand equity, reduced goodwill, loss of intellectual property all leading to a weaker market position or, in some cases, complete elimination of competitive advantage.

There are third party impacts in both directions. It is possible that a third party experiences a loss event could have an impact on deadlines or worse reveal proprietary information. These costs that are more difficult to quantify but still have large, negative impact on the business and must be accounted for.

Risk Management is necessary for establishing and promoting internal control systems and the possible continuous improvement suggested by risk management generally presents solutions and actions in different cyber security domains. Risk Management enables organisations to identify a comprehensive inventory of potential cyber risks, quantify their potential impact, and prioritise them effectively. This process must involve stakeholders across the organisation to gain perspective and consensus: it must be an ongoing process involving constant evaluation and re-evaluation.

7.1 Gaps and Challenges in Cyber Risk Management

Cyber Security, data protection, data sharing is becoming more relevant and interconnected together in different markets and sectors. The number of threats, attacks, and vulnerabilities have raised awareness in critical sectors of the need to adapt and improve cyber security and privacy in their systems and business services/offers to clients. The lack of a common understanding of cyber risks, threats, incidents, vulnerabilities and exposures linked to latest cybercrime trends, creates uncertainty in assessing the extent of risk and quantifying potential losses and damage in particular in scenarios of propagation with cyber risk exposure / losses accumulation.

There are many recommended approaches to risk management and several different guides, risk management frameworks and standards have been published. However, there are still some gaps and these are very representative of today’s challenges in Cyber Risk Management. Therefore, it is necessary to develop new standards and an innovative Cyber Risk Management process to overcome the following gaps.

7.1.1 Lack of common language in cyber risk management processes

Creating a common risk management taxonomy and language is essential for an organisation to understand cyber risk in the context of its overall objectives. Market fragmentation and lack of standardised terminology are all highly detrimental for cyber risk management adoption, in particular by SMEs who have limited capacity and expertise to invest in cyber security solutions. Recommendation in this case are integrating different regulations and directives such as NIS, ENISA, GDPR, JRC.

7.1.2 Lack of integration between Business-Critical Processes and Cyber Security Processes

Today there is a lack of commitment between IT teams and top management. It is necessary to:

- Improve relationships between all cyber security stakeholders
- Align business objectives and security issues

In particular, it is easier for large organisations which have the in-house capability to devise risk mitigation solutions and deploy them to address cybersecurity risks to small and medium sized organizations which do not have such capabilities.

7.1.3 Lack of integration between Cyber Security and Privacy Compliance

The General Data Protection Regulation (GDPR) applicable since May 25th 2018 is now the legal framework for the protection of personal data in Europe. Compared to its predecessor

Directive 95/46/EC, it contains some important novelties such as direct applicability of its provisions in all EU Member States; inclusion of a more robust accountability principle[32]; extended scope of territorial application[33]; risk based approach in defining the appropriate technical and organizational measures to implement in order to ensure the security of processing of personal data[34]; elimination of inefficient and superfluous administrative burdens; more guarantees for effective enforcement by means of application of stricter and higher administrative sanctions[35]; better protection of the data subjects; and a European wide requirement to notify personal data breaches[36] to the competent supervisory authority. So, Cyber Security processes must be well integrated with data protection processes in order to:

- Ensure and to be able to demonstrate that processing is performed in accordance with the GDPR;
- Satisfy data subject's privacy needs and rights;
- Improve transparency between data controllers and data subject services;

[32] According to Article 24 of the GDPR: " The controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this regulation".

[33] According to Article 3 of the GDPR:
"1.The regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

[34] According to Article 32 of the GDPR: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (…)".

[35] According to Article 83, the infringements of the core provisions of the GDPR can be subject to a maximum of administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year.

[36] According to Article 33 of the GDPR: "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons".

- Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing;
- Find a trusted basis for risk calculation services in cyber sector.

Even though the GDPR provided an updated legal framework to protect personal data, a challenge comes up when one considers what the practical implementation of this framework is. The legislation allows for approved certification mechanisms as a way to demonstrate the compliance with the data protection rules[37], however, until such certification mechanisms get approved according to the GDPR[38], the data protection matters still cannot be easily integrated with the cyber security solutions available in the market. This means that currently there seems to be a gap between the legislation and its application when it comes to techniques of ensuring and demonstrating a compliance through certifications.

Additionally, certification mechanisms can be established by certification bodies that have been accredited either by a national data protection authority or a national accreditation body (legally named under European Union law)[39]. Hence, as certification mechanisms get approved by different national bodies, there may reasonably be a lack of harmonization with which cyber security processes must somehow adhere to.

7.1.4 Lack of solid data on Cyber Incidents and Threats

Cyber Risk Management remains notably under-developed especially due to lack of sufficient and solid data on cyber incidents and threats that can be used for actuarial purposes. For these reasons, cyber threat intelligence and information sharing will allow cyber security firms to implement more precise and dynamic risk and impact assessment. Sharing of most recent cyber threat intelligence is critical, in particular in critical sectors such as finance, health or energy as they depend on large-scale critical infrastructures which typically connect stakeholders in complex value and delivery chains. Data sharing must be secure, well-organised and regulated, and based on a common language or taxonomy.

7.1.5 Lack of ability to demonstrate Return On Security Investment

It is difficult to show return on investment for cyber risk programs. Organisations need to develop the ability to demonstrate that the investments they are making are aligned with the actual risks they face. They have to ask if they are making the appropriate investments in

[37] According to Article 24(3) of the GDPR: "Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller".

[38] The mechanism of approval of certifications is described in Articles 42 and 43 of the GDPR.

[39] The Certification Bodies are described in Article 43 of the GDPR.

security, vigilance, and resilience, and whether those decisions are based on a realistic understanding of the specific risks their organisation faces – and the magnitude of impact that a cyber-attack could have. It would be crucial to develop a formal and approved model of ROSI (Return On Security Investment) to obtain investment for Cyber Security Investment.

7.1.6 Lack of addressing current vulnerabilities considering the cyber security about new technologies

The implementation of new technologies should consider the evolution of cyber risk based on the business factors, regulations and threat intelligence development.

7.1.7 Lack of sustainable employee turnover

One of the most important problems in a company is the high level of employee turnover . Currently, with a dearth of cybersecurity experts in the European workforce, finding the right expert is challenging. Therefore the company should remember that is easier to explain the core business knowledge than technical skills.

The technical knowledge that an employee has is one of the main and most important aspects to be assessed in cyber risk management. Better training for staff and education at both university level and before is a key aspect of this.

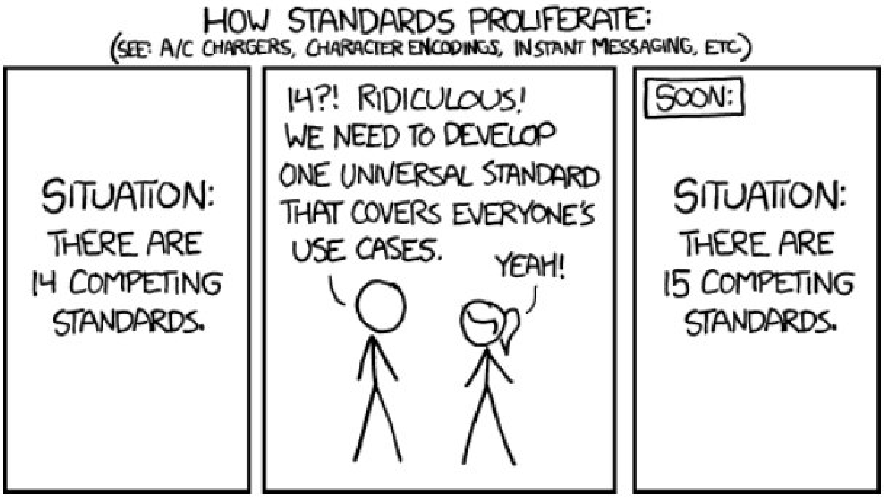
7.1.8 Lack of impactful measurements and standards hinders comparisons

Lack of standards defining the risk parameters for each sector and company size requires companies to consider benchmarks in cyber risk management "balance sheet" taking a holistic view of vulnerabilities.

Finally, while cyber risk management policies are necessary for every organisation, reducing a category of risk to zero is impossible. **Cyber Insurance** *can help cover the gaps between a robust cyber risk management program and any remaining risks*. Nevertheless, it is necessary to adopt a risk-based insurance strategy to implement a valuable insurance process so Cyber Risk Management remains the first step towards information security.

8 Conclusions and recommendations

The CONCLUSION of what we have found can be summarized quite well in the cartoon below:


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Drawing courtesy of XKCD[10]

https://xkcd.com/

In this respect, ETSI document TR 103 456, summarises very well "*The real need is to converge toward useful, practical, actionable, interoperable sets of standards*".

However, we take this one level further, which also matches with the conclusions of previous deliverables from Cyberwatching.eu – While many cybersecurity standards and certification solutions already exist, it is the general consensus that the biggest gap occurs with respect to **fragmentation** and the often **national nature of the systems** (without mutual recognition) raising issues such as challenges in **interoperability**, **market fragmentation** and increased **cyber risk**.

Thus, as a FIRST RECOMMENDATION, the issue of **Mutual Recognition** must be addressed along with **Harmonisation**. The ECSO Working Group 1 has already embarked upon this process, but it is clear that this will take time to accomplish, with the aspect of "Political Will" coming from the European Union Member States being one of the most important elements to accomplish the mission.

Our survey also identified that there is no clarity on which standards and guidelines to use, especially when a product or solution could be used in multiple Member States and as such there is a lack of confidence and/or knowledge in selecting the "right" standard (and certification). Overall lack of awareness of what standards and certification systems are available poses a significant problem as well and was identified in our survey as a key issue. An important point (identified both in our survey and the ENISA publication "Improving recognition of ICT security standards"[2]) is that there is also need to identify and present clearly which standards should be used to state NIS Directive compliance since this will build on a high common level of security of network and information systems across the Union and it cannot be limited geographically or nationally. The expertise found in recognised ESOs could be used to fill this gap.

Thus, a general SECOND RECOMMENDATION is that we need to **raise awareness concerning the available accepted standards and certification and a certification process in case of multi-party composition of products** – ECSO is already making certain efforts in that respect, but further work is needed.

A THIRD RECOMMENDATION is EC funding for **Raising Awareness and Education in Cybersecurity Standards and Certification** for both the Public and Private sectors. This recommendation stems from the repeated request in our survey, and at events, to provide information, education and guidance so that both public and private sectors in order to move forward with the essential knowledge to address this gap of expertise in standards and certification. It is already recognised that Europe does not have enough of skilled experts which the industry needs and stakeholders lack the cybersecurity knowledge.

A FOURTH RECOMMENDATION - **International Cooperation** was identified as an area to be looked upon for opportunities to benchmark best practices and standards that may already exist as a way to not "reinvent the wheel", however, caution is urged in taking care not to immediately co-opt existing standards that may put European industry at a disadvantage. From the results of ongoing projects in US and JP, several common areas of interest for collaboration emerged.

A FIFTH RECOMMENDATION is to address the **cost issue for SMEs** looking toward using cybersecurity standards and certification. As SMEs are the innovation engine especially in the cybersecurity realm, it is important that they can access standards and the related certification – with cost being a huge issue for them, self-assessment and other low-cost solutions must be explored since relying on specialised experts is very costly, including the cost of specific standards. The current lengthy and complicated process only adds to costs and finally acts as a hindrance to innovation. Again, ECSO Working Group 1 has efforts to address this issue.

A SIXTH RECOMMENDATION is to address the Internet of Things (IoT) which was as well identified in our survey as an area where there is **evidence of a lack of cybersecurity standards and certification** and this does require some concerted effort on the part of the research and industrial community to address this fast-evolving gap. This is also a well-known area that will be on the agenda of organisations such as the IoT Forum and ECSO.

A SEVENTH RECOMMENDATION is to elaborate a common research agenda across EU Member States (MS). Through the vehicle of the ERC which is available to all MS scientists, it would be sensible to open out specific calls for projects in the area of cybersecurity with clear aims and requirements on developing in areas of relevance to standards in cybersecurity. This call should be proceeded by a large publicity campaign. It would not be possible to get MS themselves to operate internal funding in a coherent manner so using academic research focused central money such as ERC would be a more cost-effective mechanism. There should also be the continued push for EC sponsored research to be fully open access not only in the final publication but also in the protocols, software and data used within the projects supported.

The overall goal of cybersecurity standards and certification is to increase the trust and confidence in European products and services, so that buyers can discern which products, services and solutions can be trusted. This is also a direct effect in supporting the competitiveness of European industry and clearly addressing the protection and security of the European citizen.

The **CONCLUSION** of this deliverable is that after studying and analyzing the existing publications and feedback (through surveys, webinars, events) on the gaps in cybersecurity standards and certification and at the same time surveying the supply side, the demand side and the stakeholders, it is evident that we have a long way to go in order to address the gaps identified. The majority of the recommendations center around the efforts of the European Cyber Security Organisation (ECSO) to address the outstanding issues and gaps and the overall recommendation is that the continued support of and cooperation with ECSO is an absolute necessity. We also look forward to our continuing work and collaboration with ECSO in our further efforts within the Cyberwatching.eu project.

ANNEX A. Glossary

Term	Explanation
AI	Artificial Intelligence
ANSI	American National Standards Institute
CEN	Comité Européen de Normalisation
CENELEC	European Committee for Electrotechnical Standardisation
CCRA	Common Criteria Recognition Arrangement
CSIRT	Computer Security Incident Response Team
DSP	Digital Service Provider
ECSO	European Cyber Security Organisation
ENISA	European Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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”)
HPC	High Performance Computing
ITSEF	IT Security Evaluation Facility
KTP	Knowledge Transfer Partnerships
MS	Member States
NGN	Next Generation Network
NIS Directive	Network and Information Systems Directive
NIST	National Institute of Standards and Technology
NSB	National Standardisation Bodies
OES	Operator of Essential Services
R&I	Research and Innovation
SOC	Security Operations Center

ANNEX B. Collection of relevant publications

ENISA Publication:

Improving recognition of ICT security standards

(December 2017)

ISBN: 978-92-9204-249-3

> *“This report is a continuation and an extension of previously carried out ENISA work on approaches to the NIS Directive by Member States, which have provided recommendations on standardisation and have outlined the use and management of CSIRTs."*

enisa

Improving recognition of ICT security standards

Recommendations for the Member States for the conformance to NIS Directive

VERSION: 1.0
DECEMBER 2017

www.enisa.europa.eu European Union Agency For Network and Information Security

ENISA Publication:

Gaps in NIS standardisation –

Recommendations for improving NIS in EU standardisation policy

(November 2016)

ISBN: 978-92-9204-186-1

> *“This report recommends that the European Commission, with the support of the Member States, pursuant to the NIS Directive, adopt a standards based framework for the exchange of threat and defensive measure information that impacts the functioning of Network Information Infrastructure (NII). The capabilities from this framework underscore NII as Critical Infrastructure of the EU and its Member States.”*

enisa

Gaps in NIS standardisation

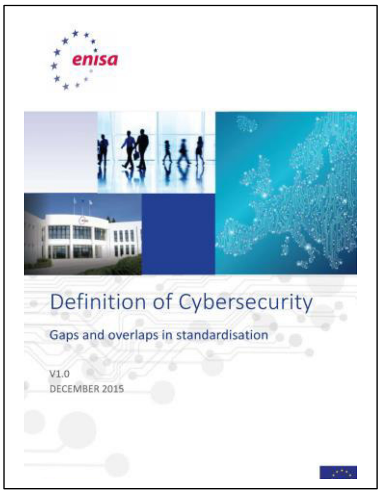
Recommendations for improving NIS in EU standardisation policy

V. 1.0
NOVEMBER 2016

ENISA Publication:

Definition of Cybersecurity – Gaps and overlaps in standardisation

(December 2015)



enisa

Definition of Cybersecurity

Gaps and overlaps in standardisation

V1.0
DECEMBER 2015

> *“This document analyses the usage of this term by various stakeholders and reviews standardisation activities in the area of Cybersecurity, providing an overview of overlaps and gaps in available standards. It has been written by CSCG and ENISA experts as a response to the Recommendation #2 and forms a logical entity together with the response to the CSCG Recommendation #1, Governance framework of the European standardisation – Aligning Policy, Industry and Research, published by ENISA at the same time.”*

ENISA Publication:

Governance framework for European standardisation –

Aligning Policy, Industry and Research

(December 2015)

ISBN: 978-92-9204-154-0

enisa

Governance framework for European standardisation

Aligning Policy, Industry and Research

V1.0
DECEMBER 2015

www.enisa.europa.eu European Union Agency For Network And Information Security

> *“In response to the European Union’s Cybersecurity Strategy, the CSCG has published a White Paper with recommendations on digital security. The CSCG’s recommendations underline the importance of Cybersecurity standardisation to complete the European internal market and to raise the level of Cybersecurity in Europe in general. CSCG Recommendation #1 proposes a review of the current governance framework. This document analyses the good practices within the governance framework of the European Union and proposes recommendations for stakeholders. It has been written by CSCG and ENISA experts as a response to the Recommendation #1 and forms a logical entity together with the response to the CSCG Recommendation #2, Definition of Cybersecurity – Gaps and overlaps in standardisation, published by ENISA at the same time.”*

ENISA Publication:

Analysis of standards related to Trust Service Providers -

Mapping of requirements of eIDAs to existing standards

(June 2016)

> "*This report on one hand analyses the eIDAS requirements with regard to the standards, on the other analyses currently available standards and compares the results of both analyses. Such a mapping is oriented at the requirements specified in the various eIDAS articles. Pursuant to this mapping it can be concluded that usually the analysed standards usually cover some requirements in part or whole.*"

ENISA Publication:

Information security and privacy standards for SMEs –

Recommendations to improve the adoption of

information security and privacy standards

in small and medium enterprises

(December 2015)

ENISA Publication:

Overview of the practices of ICT Certification Laboratories in Europe

(January 2018)

ISBN: 978-92-9204-248-6

> *"This study seeks to identify and analyse the current landscape of ICT security certification laboratories in EU Member States, comparing them also with third countries practices. The findings of this study constitute the basis for the Agency's proposal towards an EU wide ICT products and services certification framework."*

ENISA Publication:

Recommendations on European Data Protection Certification

(November 2017)

> *"The objective of this report is to identify and analyse challenges and opportunities of data protection certification mechanisms, including seals and marks, as introduced by the GDPR, focusing also on existing initiatives and voluntary schemes."*

ENISA Publication:

Challenges of security certification in emerging ICT environments

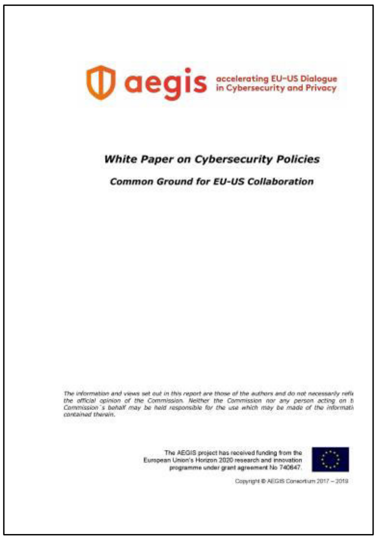
(February 2017)

> *"This report aims to provide decision makers with a thorough description of the security certification status concerning the most impactful equipment in five different critical business sectors. Results of this study should help to improve and harmonize the certification standards and frameworks in place, and pave the way towards a common approach to security certification in these sectors in the EU."*

AEGIS Project:

- **White Paper on Cybersecurity Policies** –
  Common Ground for EU-US Collaboration[40]
  (May 2018)

> *"This Paper focuses on three policy areas which impact bilateral cyber dialogues and research and innovation collaboration between the EU and the US. The three policy areas are: Standards and certification; privacy and data Protection; and public-private information sharing."*



aegis accelerating EU-US Dialogue in Cybersecurity and Privacy

White Paper on Cybersecurity Policies

Common Ground for EU-US Collaboration

The information and views set out in this report are those of the authors and do not necessarily refle the official opinion of the Commission. Neither the Commission nor any person acting on t Commission´s behalf may be held responsible for the use which may be made of the informati contained therein.

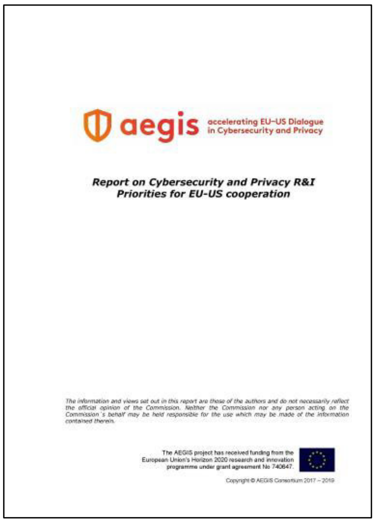
The AEGIS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740647.

Copyright © AEGIS Consortium 2017 – 2019

AEGIS Project:

- **Report on Cybersecurity and Privacy**
  R&I Priorities for EU-US Cooperation[41]
  (2018)

> *"The report on Cybersecurity and Privacy Research and Innovation (R&I) priorities presents the results of a survey conducted by the AEGIS project in the EU and the US to identify R&I priorities for future collaboration in cybersecurity and privacy between both regions."*



aegis accelerating EU-US Dialogue in Cybersecurity and Privacy

Report on Cybersecurity and Privacy R&I Priorities for EU-US cooperation

The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the Commission. Neither the Commission nor any person acting on the Commission´s behalf may be held responsible for the use which may be made of the information contained therein.

The AEGIS project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740647.

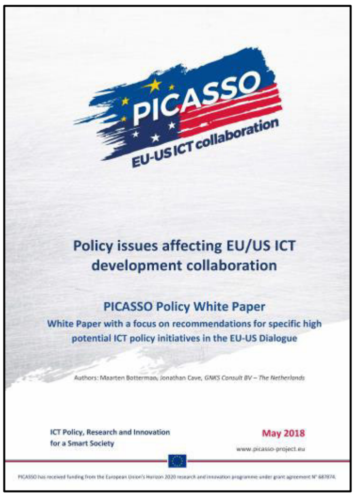
Copyright © AEGIS Consortium 2017 – 2019

[40] https://drive.google.com/open?id=1qkvmaxFzPQwjB0T_BxjvdxUtRfPBot34

[41] https://drive.google.com/open?id=1nieB-rb1fs0y1_MhFVOtsvB1VOi0f1XJ

PICASSO Project:

- **Policy issues affecting EU/US ICT development Collaboration** – PICASSO Policy White Paper (May 2018)



Policy issues affecting EU/US ICT development collaboration

PICASSO Policy White Paper

White Paper with a focus on recommendations for specific high potential ICT policy initiatives in the EU-US Dialogue

Authors: Maarten Botterman, Jonathan Cave, *GNKS Consult BV – The Netherlands*

ICT Policy, Research and Innovation
for a Smart Society

May 2018

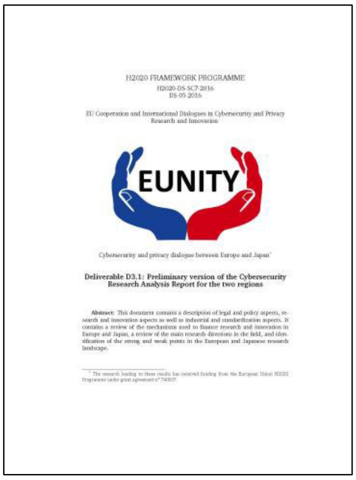
www.picasso-project.eu

PICASSO has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 687874.

EUNITY Project:

- **Preliminary version of the Cybersecurity Research Analysis Report for the two regions**[42]

> *"This document contains a description of legal and policy aspects, research and innovation aspects as well as industrial and standardisation aspects. It contains a review of the mechanisms used to finance research and innovation in Europe and Japan, a review of the main research directions in the field, and identification of the strong and weak points in the European and Japanese research landscape."*



H2020 FRAMEWORK PROGRAMME
H2020-DS-SC7-2016
DS-05-2016

EU Cooperation and International Dialogues in Cybersecurity and Privacy Research and Innovation

Cybersecurity and privacy dialogue between Europe and Japan[1]

Deliverable D3.1: Preliminary version of the Cybersecurity Research Analysis Report for the two regions

Abstract: This document contains a description of legal and policy aspects, research and innovation aspects as well as industrial and standardisation aspects. It contains a review of the mechanisms used to finance research and innovation in Europe and Japan, a review of the main research directions in the field, and identification of the strong and weak points in the European and Japanese research landscape.

[1] The research leading to these results has received funding from the European Union H2020 Programme under grant agreement n° 740507.

[42] https://www.eunity-project.eu/m/filer_public/53/4a/534abeb6-6532-4c59-a4ae-22ac91b3d885/eunity-d31.pdf

ANNEX C. Online survey on gaps in cybersecurity standards and certification

SURVEY TO GATHER INFORMATION FROM THE PERSPECTIVE OF SUPPLY & DEMAND
REGARDING GAPS IN THE CERTIFICATION AND STANDARDS FRAMEWORK
IN THE EUROPEAN UNION & ASSOCIATED COUNTRIES

www.cybersecurity.eu "The European watch on cybersecurity & privacy" aims to create a cybersecurity & privacy ecosystem offering prime and guided access to a catalogue of services & marketplace.
More information about the project at https://www.cyberwatching.eu/about/project

This Cyberwatching survey consists of six questions and is intended to get input and feedback concerning the gaps in the current and existing cybersecurity standards and certification environment. We thank you in advance for taking the time to respond.

Q1. Are you using cybersecurity standards (and/or certification) in your work efforts?

Yes □ No □

If "Yes": in which areas are these standards (certification)? –

- IoT
- Devices
- Components
- Software
- Organisation (for example, ISO 27000 series)
- Products
- Other (enter a description below)

If you know the standards/certification used, can you list them here?

2. Do see any gaps in the current cybersecurity standards (or certification)?

Yes □ No □

If "Yes": in which areas are these standards (certification)? –

- IoT
- Devices
- Components
- Software

Annex C, page 2

- Organisation (for example, ISO 27000 series)
- Products
- Other (enter a description below)

And specifically, what are those gaps?

3. In your opinion are risk assessment, risk management and risk mitigation comprehensively addressed and is this fit for purpose within the current and existing cybersecurity standards?

- Yes
- No
- Maybe

If your answer is “No” or “Maybe” - how can this be improved?:

- Improve risk assessment, risk management and risk mitigation elements within the current existing standards
- Improve specific standards such as ISO 27000 with respect to the risk assessment, risk management and risk mitigation aspects
- Create a new "fit for purpose" cybersecurity risk assessment, risk management and risk mitigation standard
- Other

Further explain your answers in the text box below:

4. What are your 3 greatest concerns about the cybersecurity standards/certification? (SELECT THE THREE MOST RELEVANT ONES)

- Which standard to use?
- What to certify?
- How to certify?
- Where to certify?
- Who can certify?
- Cost of certification?
- Complexity of standards/certification?
- Harmonisation of Cybersecurity Standards across the EU?
- Other (specify beow)

Annex C, page 3

Explain why you have selected the above three options:

4. Are you aware of any cybersecurity standard(s)/certification that has/have been harmonised across the EU member states?

- SOG-IS
- Common Criteria
- Other (list below):

Please provide any additional feedback concerning harmonization of cybersecurity standards/certification harmonized across the EU member states:

5. Are certification costs and the time and resources involved of concern to you?

Yes □ No □

If yes, please select which aspects:

- Choice of standard results in higher or lower certification costs
- Choice of certification "level" results in higher or lower certification costs

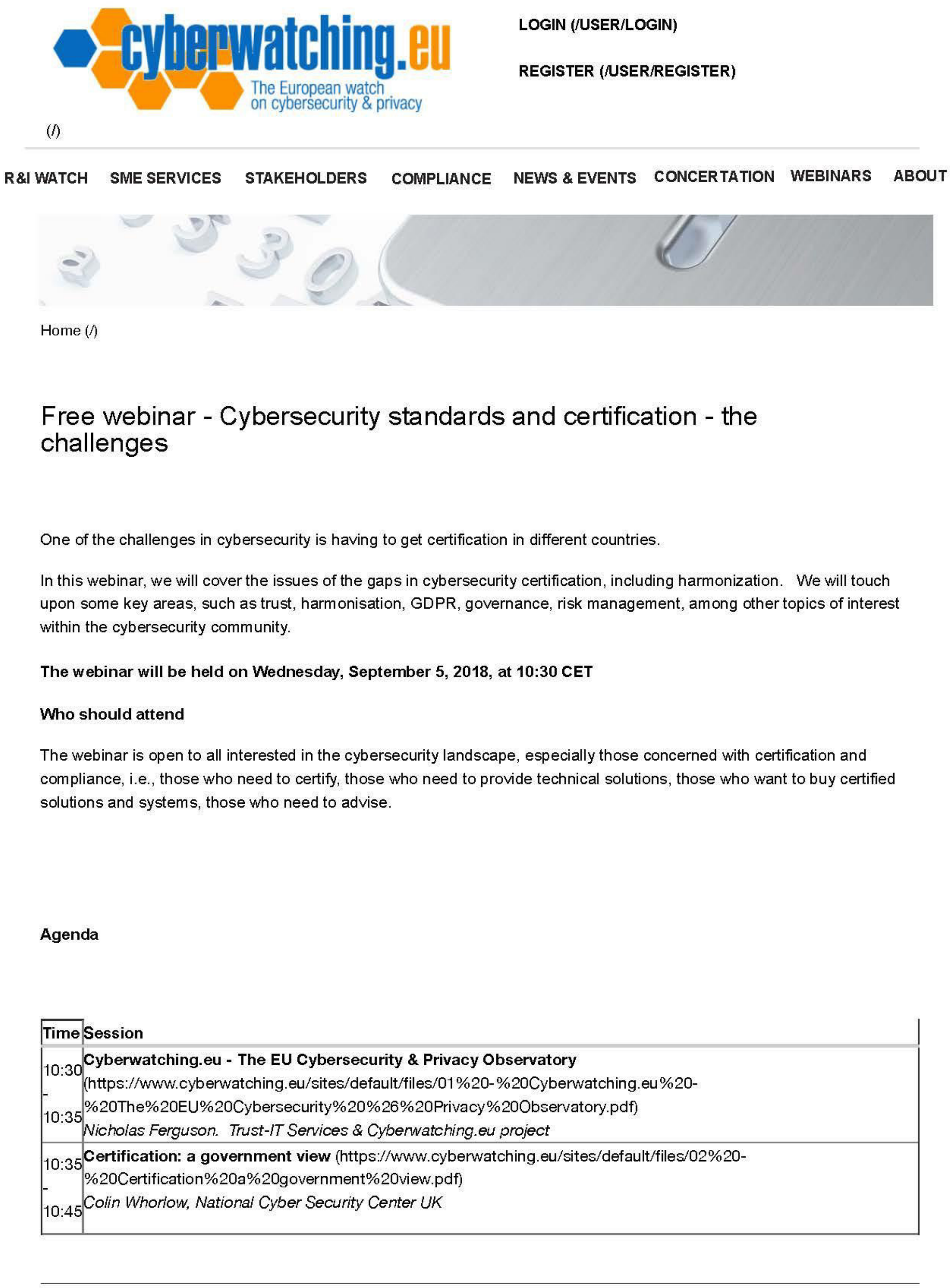
Annex C, page 3

- Self-Assessment is an interesting low cost option for addressing a standard/certification
- How can SMEs achieve cybersecurity certification with very limited resources?
- Other (enter a description below):

Please give your feedback concerning your selections:

Thank you!

ANNEX D. Agenda of Webinar "Cybersecurity Standards & Certification", September 5, 2018 "



Free webinar - Cybersecurity standards and certification - the challenges

One of the challenges in cybersecurity is having to get certification in different countries.

In this webinar, we will cover the issues of the gaps in cybersecurity certification, including harmonization. We will touch upon some key areas, such as trust, harmonisation, GDPR, governance, risk management, among other topics of interest within the cybersecurity community.

The webinar will be held on Wednesday, September 5, 2018, at 10:30 CET

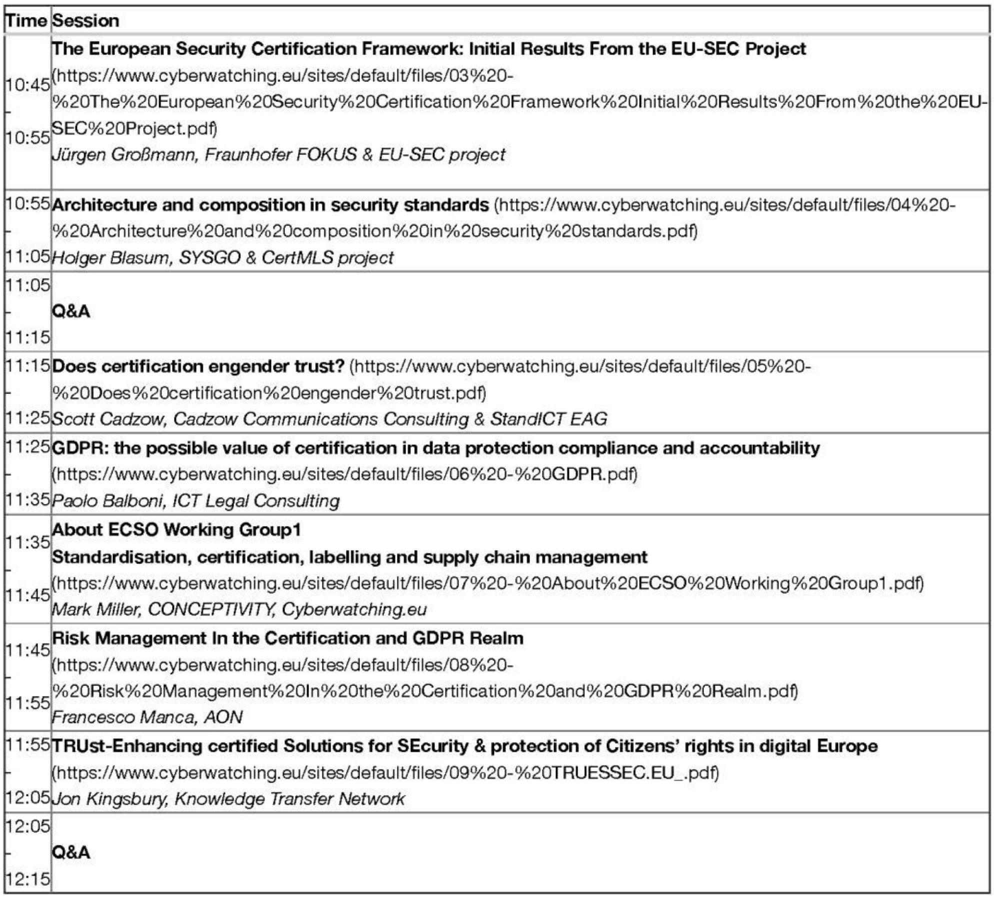
Who should attend

The webinar is open to all interested in the cybersecurity landscape, especially those concerned with certification and compliance, i.e., those who need to certify, those who need to provide technical solutions, those who want to buy certified solutions and systems, those who need to advise.

Agenda

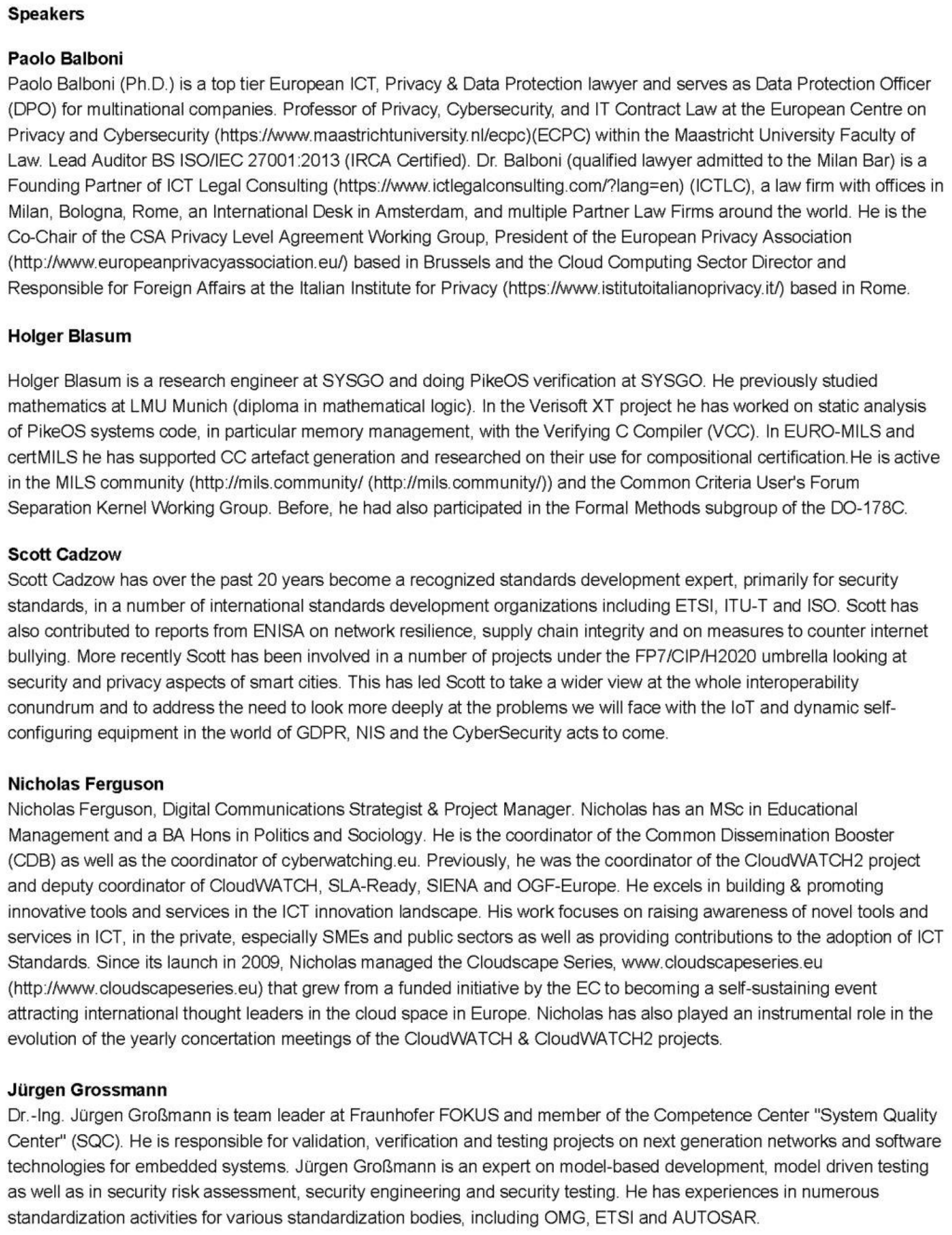
Time	Session
10:30 - 10:35	**Cyberwatching.eu - The EU Cybersecurity & Privacy Observatory** (https://www.cyberwatching.eu/sites/default/files/01%20-%20Cyberwatching.eu%20-%20The%20EU%20Cybersecurity%20%26%20Privacy%20Observatory.pdf) *Nicholas Ferguson. Trust-IT Services & Cyberwatching.eu project*
10:35 - 10:45	**Certification: a government view** (https://www.cyberwatching.eu/sites/default/files/02%20-%20Certification%20a%20government%20view.pdf) *Colin Whorlow, National Cyber Security Center UK*

Annex D, page 2



Time	Session
10:45 - 10:55	**The European Security Certification Framework: Initial Results From the EU-SEC Project** (https://www.cyberwatching.eu/sites/default/files/03%20-%20The%20European%20Security%20Certification%20Framework%20Initial%20Results%20From%20the%20EU-SEC%20Project.pdf) *Jürgen Großmann, Fraunhofer FOKUS & EU-SEC project*
10:55 - 11:05	**Architecture and composition in security standards** (https://www.cyberwatching.eu/sites/default/files/04%20-%20Architecture%20and%20composition%20in%20security%20standards.pdf) *Holger Blasum, SYSGO & CertMLS project*
11:05 - 11:15	**Q&A**
11:15 - 11:25	**Does certification engender trust?** (https://www.cyberwatching.eu/sites/default/files/05%20-%20Does%20certification%20engender%20trust.pdf) *Scott Cadzow, Cadzow Communications Consulting & StandICT EAG*
11:25 - 11:35	**GDPR: the possible value of certification in data protection compliance and accountability** (https://www.cyberwatching.eu/sites/default/files/06%20-%20GDPR.pdf) *Paolo Balboni, ICT Legal Consulting*
11:35 - 11:45	**About ECSO Working Group1** **Standardisation, certification, labelling and supply chain management** (https://www.cyberwatching.eu/sites/default/files/07%20-%20About%20ECSO%20Working%20Group1.pdf) *Mark Miller, CONCEPTIVITY, Cyberwatching.eu*
11:45 - 11:55	**Risk Management In the Certification and GDPR Realm** (https://www.cyberwatching.eu/sites/default/files/08%20-%20Risk%20Management%20In%20the%20Certification%20and%20GDPR%20Realm.pdf) *Francesco Manca, AON*
11:55 - 12:05	**TRUst-Enhancing certified Solutions for SEcurity & protection of Citizens' rights in digital Europe** (https://www.cyberwatching.eu/sites/default/files/09%20-%20TRUESSEC.EU_.pdf) *Jon Kingsbury, Knowledge Transfer Network*
12:05 - 12:15	**Q&A**

Annex D, page 3



Speakers

Paolo Balboni

Paolo Balboni (Ph.D.) is a top tier European ICT, Privacy & Data Protection lawyer and serves as Data Protection Officer (DPO) for multinational companies. Professor of Privacy, Cybersecurity, and IT Contract Law at the European Centre on Privacy and Cybersecurity (https://www.maastrichtuniversity.nl/ecpc)(ECPC) within the Maastricht University Faculty of Law. Lead Auditor BS ISO/IEC 27001:2013 (IRCA Certified). Dr. Balboni (qualified lawyer admitted to the Milan Bar) is a Founding Partner of ICT Legal Consulting (https://www.ictlegalconsulting.com/?lang=en) (ICTLC), a law firm with offices in Milan, Bologna, Rome, an International Desk in Amsterdam, and multiple Partner Law Firms around the world. He is the Co-Chair of the CSA Privacy Level Agreement Working Group, President of the European Privacy Association (http://www.europeanprivacyassociation.eu/) based in Brussels and the Cloud Computing Sector Director and Responsible for Foreign Affairs at the Italian Institute for Privacy (https://www.istitutoitalianoprivacy.it/) based in Rome.

Holger Blasum

Holger Blasum is a research engineer at SYSGO and doing PikeOS verification at SYSGO. He previously studied mathematics at LMU Munich (diploma in mathematical logic). In the Verisoft XT project he has worked on static analysis of PikeOS systems code, in particular memory management, with the Verifying C Compiler (VCC). In EURO-MILS and certMILS he has supported CC artefact generation and researched on their use for compositional certification.He is active in the MILS community (http://mils.community/ (http://mils.community/)) and the Common Criteria User's Forum Separation Kernel Working Group. Before, he had also participated in the Formal Methods subgroup of the DO-178C.

Scott Cadzow

Scott Cadzow has over the past 20 years become a recognized standards development expert, primarily for security standards, in a number of international standards development organizations including ETSI, ITU-T and ISO. Scott has also contributed to reports from ENISA on network resilience, supply chain integrity and on measures to counter internet bullying. More recently Scott has been involved in a number of projects under the FP7/CIP/H2020 umbrella looking at security and privacy aspects of smart cities. This has led Scott to take a wider view at the whole interoperability conundrum and to address the need to look more deeply at the problems we will face with the IoT and dynamic self-configuring equipment in the world of GDPR, NIS and the CyberSecurity acts to come.

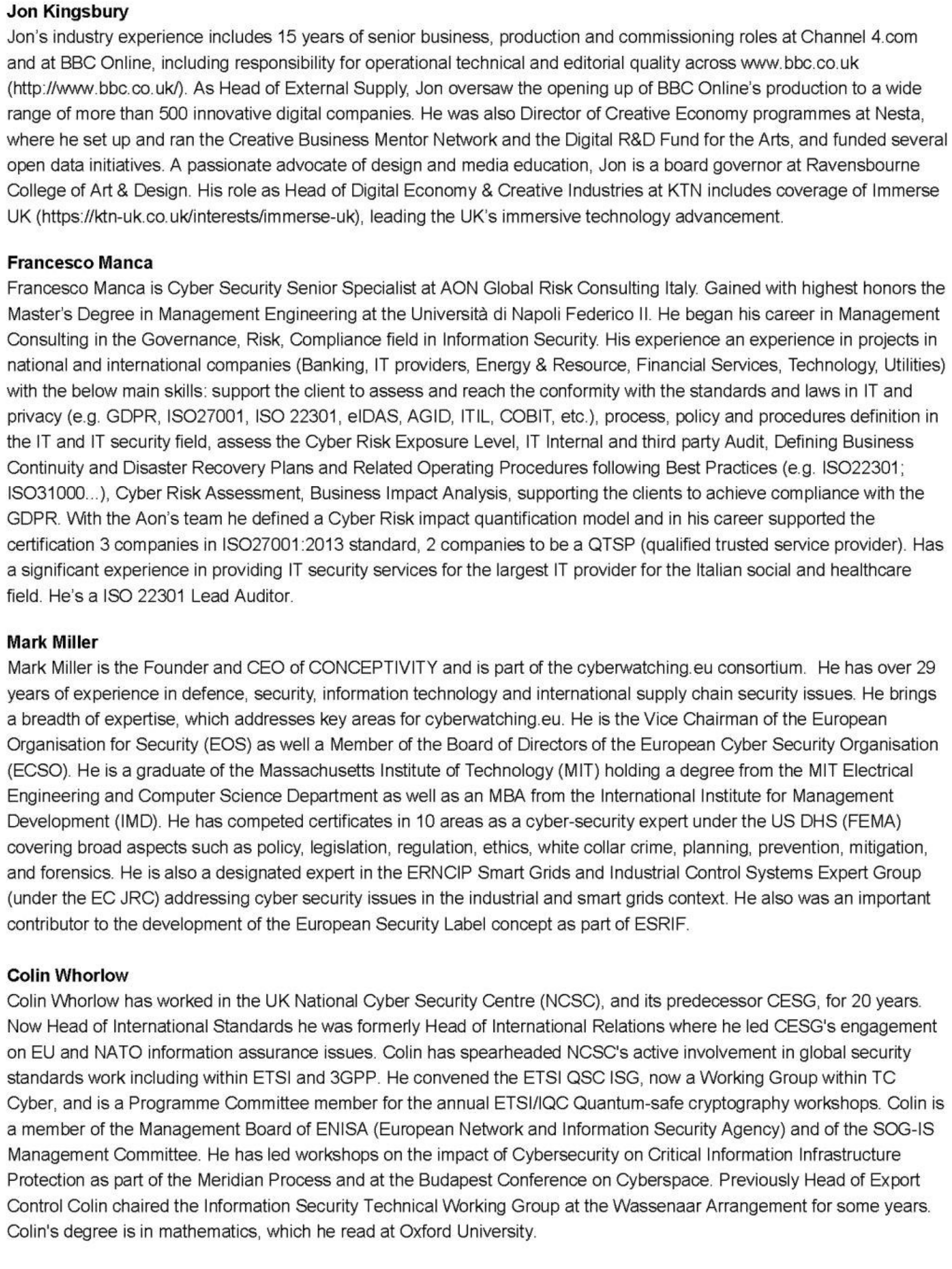
Nicholas Ferguson

Nicholas Ferguson, Digital Communications Strategist & Project Manager. Nicholas has an MSc in Educational Management and a BA Hons in Politics and Sociology. He is the coordinator of the Common Dissemination Booster (CDB) as well as the coordinator of cyberwatching.eu. Previously, he was the coordinator of the CloudWATCH2 project and deputy coordinator of CloudWATCH, SLA-Ready, SIENA and OGF-Europe. He excels in building & promoting innovative tools and services in the ICT innovation landscape. His work focuses on raising awareness of novel tools and services in ICT, in the private, especially SMEs and public sectors as well as providing contributions to the adoption of ICT Standards. Since its launch in 2009, Nicholas managed the Cloudscape Series, www.cloudscapeseries.eu (http://www.cloudscapeseries.eu) that grew from a funded initiative by the EC to becoming a self-sustaining event attracting international thought leaders in the cloud space in Europe. Nicholas has also played an instrumental role in the evolution of the yearly concertation meetings of the CloudWATCH & CloudWATCH2 projects.

Jürgen Grossmann

Dr.-Ing. Jürgen Großmann is team leader at Fraunhofer FOKUS and member of the Competence Center "System Quality Center" (SQC). He is responsible for validation, verification and testing projects on next generation networks and software technologies for embedded systems. Jürgen Großmann is an expert on model-based development, model driven testing as well as in security risk assessment, security engineering and security testing. He has experiences in numerous standardization activities for various standardization bodies, including OMG, ETSI and AUTOSAR.

Annex D, page 4



Jon Kingsbury

Jon's industry experience includes 15 years of senior business, production and commissioning roles at Channel 4.com and at BBC Online, including responsibility for operational technical and editorial quality across www.bbc.co.uk (http://www.bbc.co.uk/). As Head of External Supply, Jon oversaw the opening up of BBC Online's production to a wide range of more than 500 innovative digital companies. He was also Director of Creative Economy programmes at Nesta, where he set up and ran the Creative Business Mentor Network and the Digital R&D Fund for the Arts, and funded several open data initiatives. A passionate advocate of design and media education, Jon is a board governor at Ravensbourne College of Art & Design. His role as Head of Digital Economy & Creative Industries at KTN includes coverage of Immerse UK (https://ktn-uk.co.uk/interests/immerse-uk), leading the UK's immersive technology advancement.

Francesco Manca

Francesco Manca is Cyber Security Senior Specialist at AON Global Risk Consulting Italy. Gained with highest honors the Master's Degree in Management Engineering at the Università di Napoli Federico II. He began his career in Management Consulting in the Governance, Risk, Compliance field in Information Security. His experience an experience in projects in national and international companies (Banking, IT providers, Energy & Resource, Financial Services, Technology, Utilities) with the below main skills: support the client to assess and reach the conformity with the standards and laws in IT and privacy (e.g. GDPR, ISO27001, ISO 22301, eIDAS, AGID, ITIL, COBIT, etc.), process, policy and procedures definition in the IT and IT security field, assess the Cyber Risk Exposure Level, IT Internal and third party Audit, Defining Business Continuity and Disaster Recovery Plans and Related Operating Procedures following Best Practices (e.g. ISO22301; ISO31000...), Cyber Risk Assessment, Business Impact Analysis, supporting the clients to achieve compliance with the GDPR. With the Aon's team he defined a Cyber Risk impact quantification model and in his career supported the certification 3 companies in ISO27001:2013 standard, 2 companies to be a QTSP (qualified trusted service provider). Has a significant experience in providing IT security services for the largest IT provider for the Italian social and healthcare field. He's a ISO 22301 Lead Auditor.

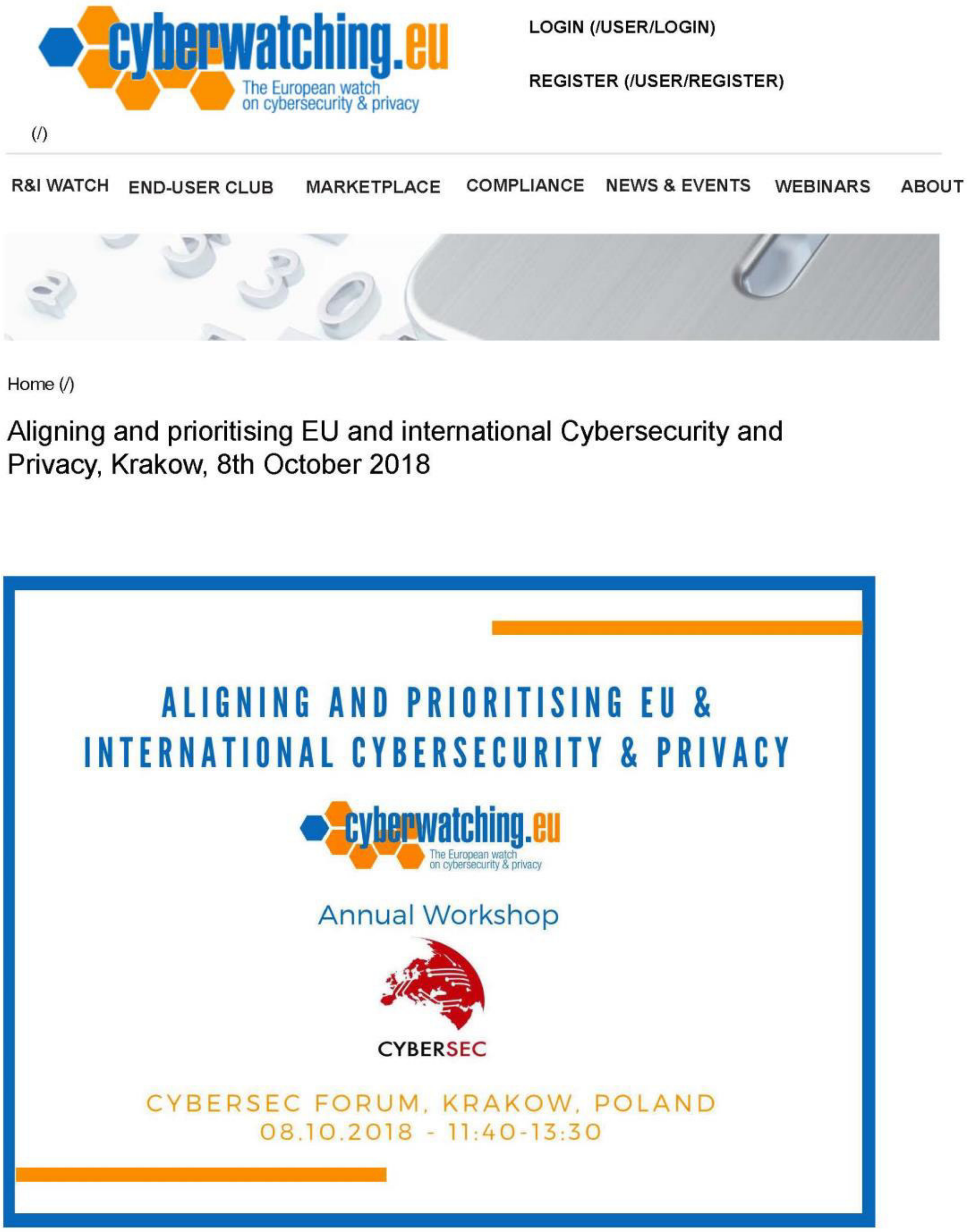
Mark Miller

Mark Miller is the Founder and CEO of CONCEPTIVITY and is part of the cyberwatching.eu consortium. He has over 29 years of experience in defence, security, information technology and international supply chain security issues. He brings a breadth of expertise, which addresses key areas for cyberwatching.eu. He is the Vice Chairman of the European Organisation for Security (EOS) as well a Member of the Board of Directors of the European Cyber Security Organisation (ECSO). He is a graduate of the Massachusetts Institute of Technology (MIT) holding a degree from the MIT Electrical Engineering and Computer Science Department as well as an MBA from the International Institute for Management Development (IMD). He has competed certificates in 10 areas as a cyber-security expert under the US DHS (FEMA) covering broad aspects such as policy, legislation, regulation, ethics, white collar crime, planning, prevention, mitigation, and forensics. He is also a designated expert in the ERNCIP Smart Grids and Industrial Control Systems Expert Group (under the EC JRC) addressing cyber security issues in the industrial and smart grids context. He also was an important contributor to the development of the European Security Label concept as part of ESRIF.

Colin Whorlow

Colin Whorlow has worked in the UK National Cyber Security Centre (NCSC), and its predecessor CESG, for 20 years. Now Head of International Standards he was formerly Head of International Relations where he led CESG's engagement on EU and NATO information assurance issues. Colin has spearheaded NCSC's active involvement in global security standards work including within ETSI and 3GPP. He convened the ETSI QSC ISG, now a Working Group within TC Cyber, and is a Programme Committee member for the annual ETSI/IQC Quantum-safe cryptography workshops. Colin is a member of the Management Board of ENISA (European Network and Information Security Agency) and of the SOG-IS Management Committee. He has led workshops on the impact of Cybersecurity on Critical Information Infrastructure Protection as part of the Meridian Process and at the Budapest Conference on Cyberspace. Previously Head of Export Control Colin chaired the Information Security Technical Working Group at the Wassenaar Arrangement for some years. Colin's degree is in mathematics, which he read at Oxford University.

ANNEX E. Agenda of Annual cyberwatching.eu event, Krakow, October 8, 2018



Aligning and prioritising EU and international Cybersecurity and Privacy, Krakow, 8th October 2018

ALIGNING AND PRIORITISING EU & INTERNATIONAL CYBERSECURITY & PRIVACY

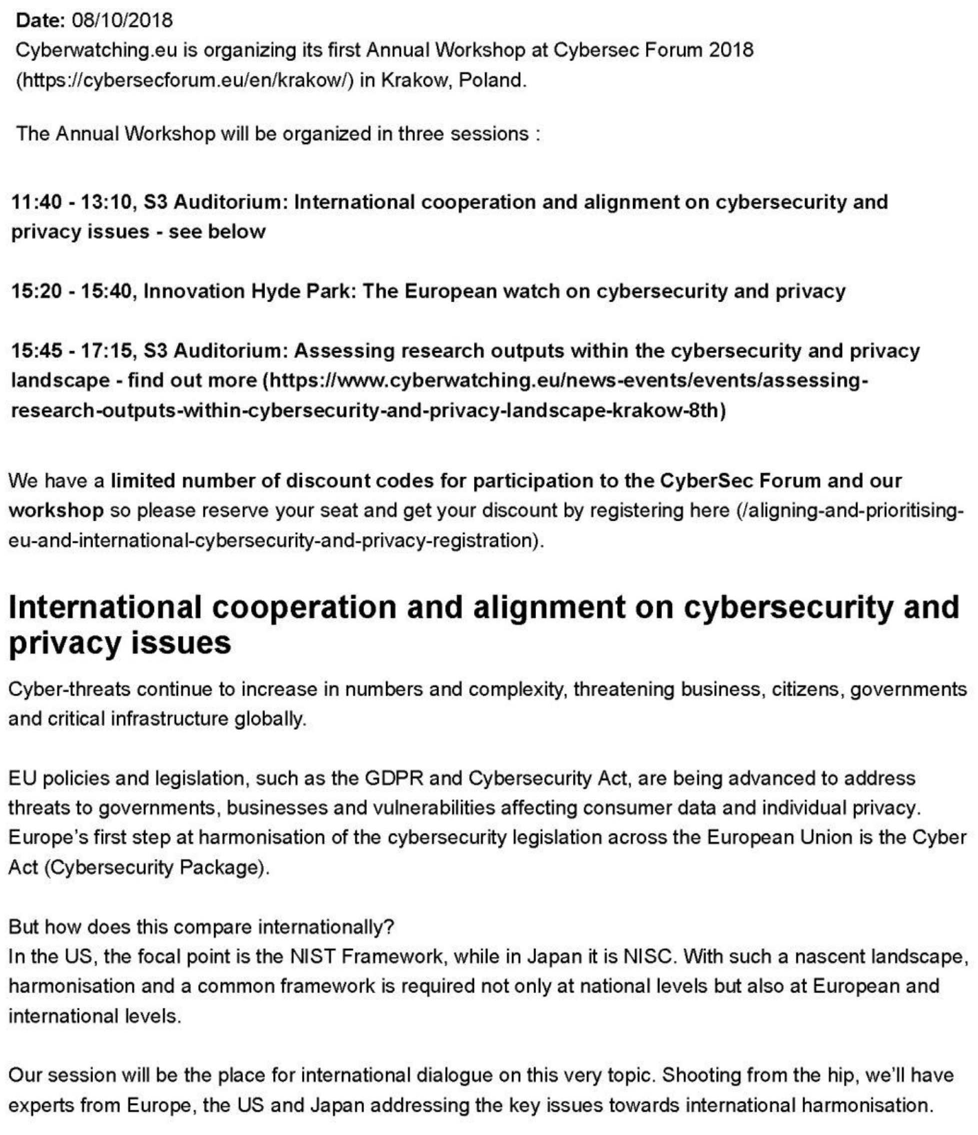
cyberwatching.eu
The European watch on cybersecurity & privacy

Annual Workshop

CYBERSEC

CYBERSEC FORUM, KRAKOW, POLAND
08.10.2018 - 11:40-13:30

Annex E, page 2



Date: 08/10/2018
Cyberwatching.eu is organizing its first Annual Workshop at Cybersec Forum 2018 (https://cybersecforum.eu/en/krakow/) in Krakow, Poland.

The Annual Workshop will be organized in three sessions :

11:40 - 13:10, S3 Auditorium: International cooperation and alignment on cybersecurity and privacy issues - see below

15:20 - 15:40, Innovation Hyde Park: The European watch on cybersecurity and privacy

15:45 - 17:15, S3 Auditorium: Assessing research outputs within the cybersecurity and privacy landscape - find out more (https://www.cyberwatching.eu/news-events/events/assessing-research-outputs-within-cybersecurity-and-privacy-landscape-krakow-8th)

We have a **limited number of discount codes for participation to the CyberSec Forum and our workshop** so please reserve your seat and get your discount by registering here (/aligning-and-prioritising-eu-and-international-cybersecurity-and-privacy-registration).

International cooperation and alignment on cybersecurity and privacy issues

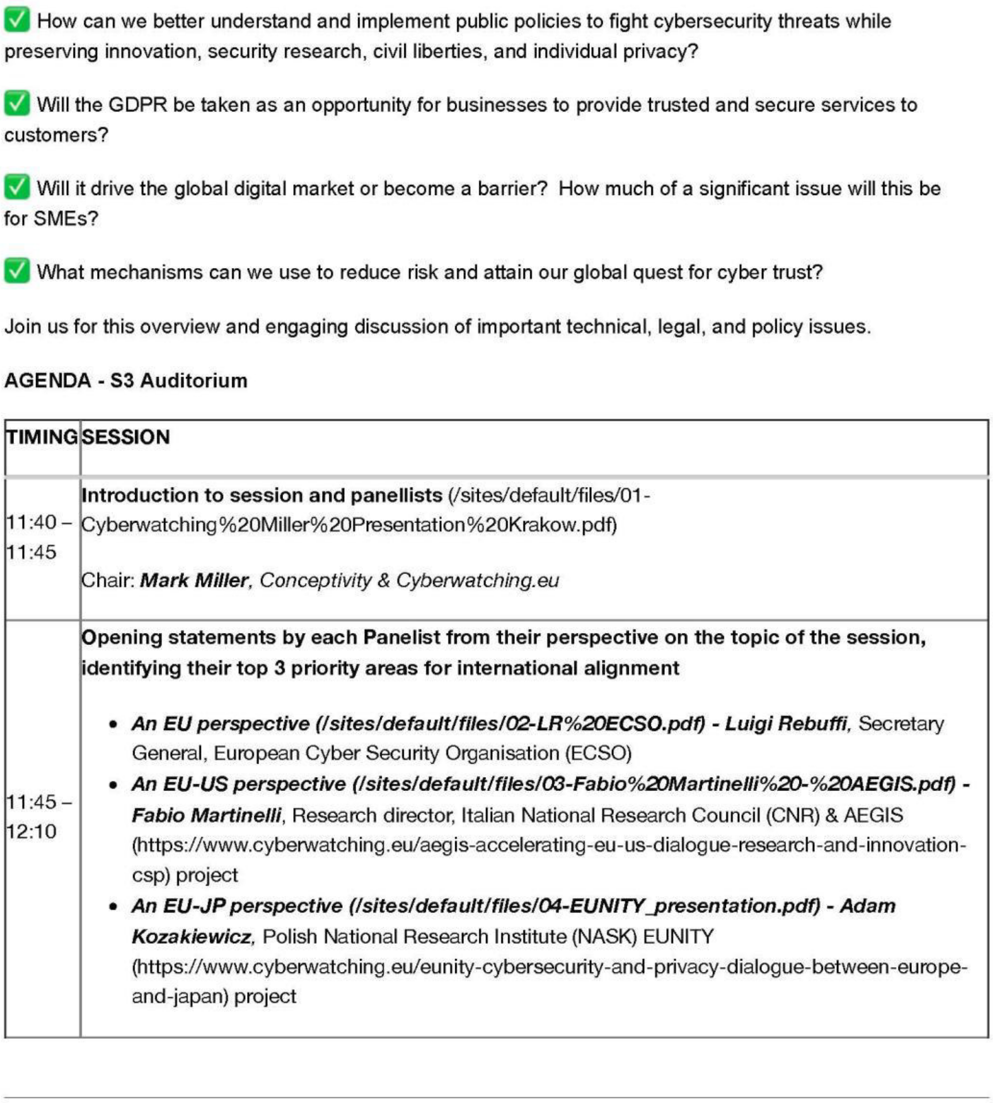
Cyber-threats continue to increase in numbers and complexity, threatening business, citizens, governments and critical infrastructure globally.

EU policies and legislation, such as the GDPR and Cybersecurity Act, are being advanced to address threats to governments, businesses and vulnerabilities affecting consumer data and individual privacy. Europe's first step at harmonisation of the cybersecurity legislation across the European Union is the Cyber Act (Cybersecurity Package).

But how does this compare internationally?
In the US, the focal point is the NIST Framework, while in Japan it is NISC. With such a nascent landscape, harmonisation and a common framework is required not only at national levels but also at European and international levels.

Our session will be the place for international dialogue on this very topic. Shooting from the hip, we'll have experts from Europe, the US and Japan addressing the key issues towards international harmonisation.

Annex E, page 3



✅ How can we better understand and implement public policies to fight cybersecurity threats while preserving innovation, security research, civil liberties, and individual privacy?

✅ Will the GDPR be taken as an opportunity for businesses to provide trusted and secure services to customers?

✅ Will it drive the global digital market or become a barrier? How much of a significant issue will this be for SMEs?

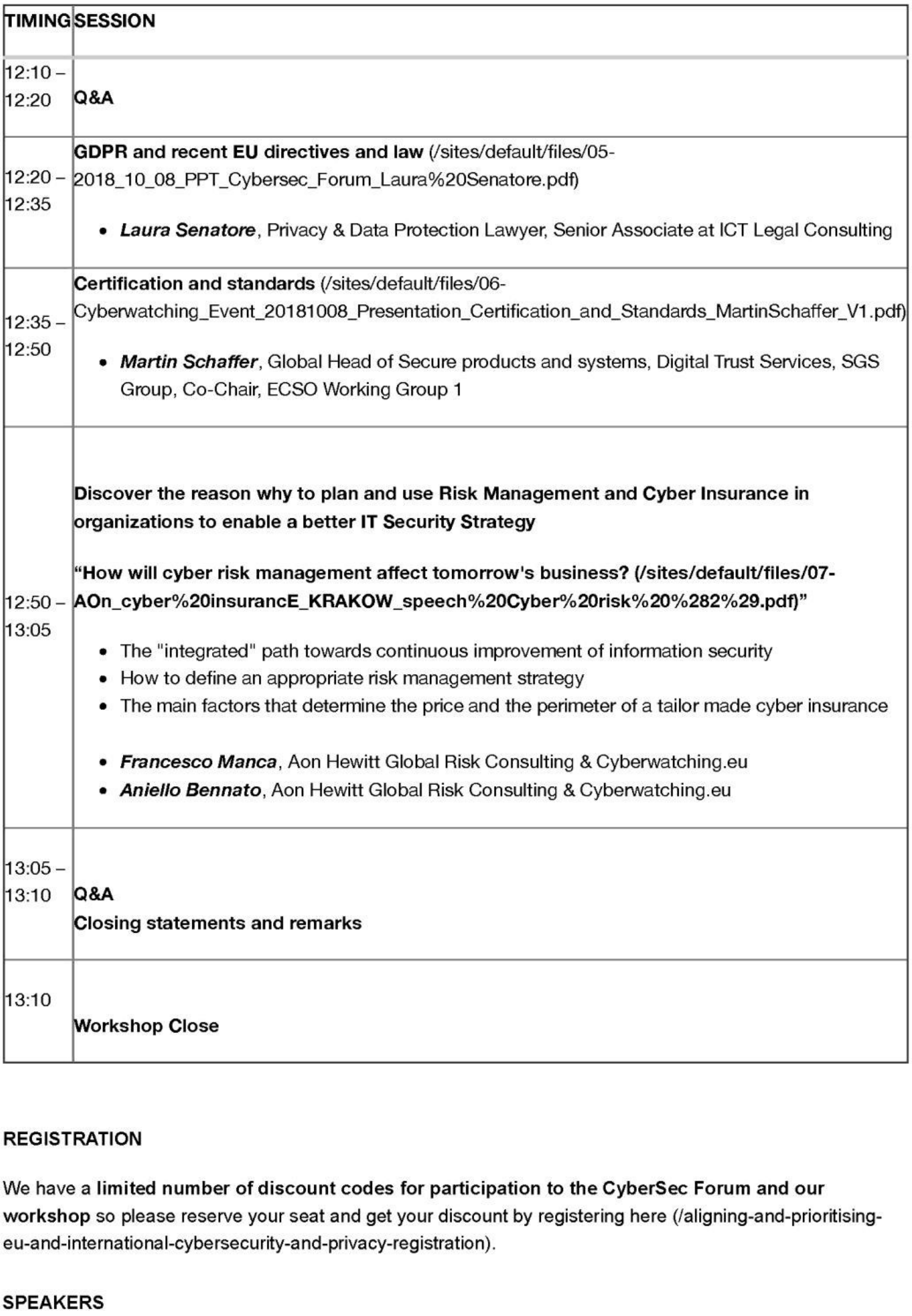
✅ What mechanisms can we use to reduce risk and attain our global quest for cyber trust?

Join us for this overview and engaging discussion of important technical, legal, and policy issues.

AGENDA - S3 Auditorium

TIMING	**SESSION**
11:40 – 11:45	**Introduction to session and panellists** (/sites/default/files/01-Cyberwatching%20Miller%20Presentation%20Krakow.pdf) Chair: ***Mark Miller***, *Conceptivity & Cyberwatching.eu*
11:45 – 12:10	**Opening statements by each Panelist from their perspective on the topic of the session, identifying their top 3 priority areas for international alignment** • ***An EU perspective (/sites/default/files/02-LR%20ECSO.pdf) - Luigi Rebuffi***, Secretary General, European Cyber Security Organisation (ECSO) • ***An EU-US perspective (/sites/default/files/03-Fabio%20Martinelli%20-%20AEGIS.pdf) - Fabio Martinelli***, Research director, Italian National Research Council (CNR) & AEGIS (https://www.cyberwatching.eu/aegis-accelerating-eu-us-dialogue-research-and-innovation-csp) project • ***An EU-JP perspective (/sites/default/files/04-EUNITY_presentation.pdf) - Adam Kozakiewicz***, Polish National Research Institute (NASK) EUNITY (https://www.cyberwatching.eu/eunity-cybersecurity-and-privacy-dialogue-between-europe-and-japan) project

Annex E, page 4



TIMING	SESSION
12:10 – 12:20	**Q&A**
12:20 – 12:35	**GDPR and recent EU directives and law** (/sites/default/files/05-2018_10_08_PPT_Cybersec_Forum_Laura%20Senatore.pdf) • ***Laura Senatore***, Privacy & Data Protection Lawyer, Senior Associate at ICT Legal Consulting
12:35 – 12:50	**Certification and standards** (/sites/default/files/06-Cyberwatching_Event_20181008_Presentation_Certification_and_Standards_MartinSchaffer_V1.pdf) • ***Martin Schaffer***, Global Head of Secure products and systems, Digital Trust Services, SGS Group, Co-Chair, ECSO Working Group 1
12:50 – 13:05	**Discover the reason why to plan and use Risk Management and Cyber Insurance in organizations to enable a better IT Security Strategy** **"How will cyber risk management affect tomorrow's business? (/sites/default/files/07-AOn_cyber%20insurancE_KRAKOW_speech%20Cyber%20risk%20%282%29.pdf)"** • The "integrated" path towards continuous improvement of information security • How to define an appropriate risk management strategy • The main factors that determine the price and the perimeter of a tailor made cyber insurance • ***Francesco Manca***, Aon Hewitt Global Risk Consulting & Cyberwatching.eu • ***Aniello Bennato***, Aon Hewitt Global Risk Consulting & Cyberwatching.eu
13:05 – 13:10	**Q&A** **Closing statements and remarks**
13:10	**Workshop Close**

REGISTRATION

We have a **limited number of discount codes for participation to the CyberSec Forum and our workshop** so please reserve your seat and get your discount by registering here (/aligning-and-prioritising-eu-and-international-cybersecurity-and-privacy-registration).

SPEAKERS

Annex E, page 5

Mark Miller

Mark Miller

Mark Miller is the Founder and CEO of CONCEPTIVITY and is part of the cyberwatching.eu consortium. He has over 29 years of experience in defense, security, information technology and international supply chain security issues. He brings a breadth of expertise, which addresses key areas for cyberwatching.eu. He is the Vice Chairman of the European Organisation for Security (EOS) as well a Member of the Board of Directors of the European Cyber Security Organisation (ECSO) and the Cybersecurity Public Private Partnership (cPPP). He is a graduate of the Massachusetts Institute of Technology (MIT) holding a degree from the MIT Electrical Engineering and Computer Science Department as well as an MBA from the International Institute for Management Development (IMD). Mr. Miller is the Chairman of ECSO Working Group 1.4 (Cybersecurity Standards / Certification / Supply Chain), Chairman of ECSO Working Group 2.3 (Cybersecurity International Cooperation) as well as Chairing ECSO Working Group 3.4 (Financial Sector Vertical).

Lugi Rebuffi

Luigi Rebuffi

Luigi Rebuffi is the CEO and founder of EOS (European Organisation for Security) and the Secretary General and founder of ECSO (European Cyber Security Organisation).

After having graduated in Nuclear Engineering at the Politecnico di Milano (Italy), he has worked in Germany on the development of high power microwave systems for the next thermonuclear fusion reactor (ITER). He continued his carrier at Thomson CSF / Thales in France where he took on increasing responsibilities for European Affairs (R&D) in different sectors: telecom, industrial, medical, scientific, and becoming in 2003 Director for European Affairs for the civilian activities of the Group. He suggested the creation of EOS and coordinated its establishment in 2007. In 2016 he contributed at the creation of ECSO and signed with the E. Commission the cPPP on cybersecurity. Until 2016 and for 6 years, he has been an advisor to the European Commission for the EU Security Research Programme and President of the Steering Board of the French ANR for security research.

Fabio Martinelli

Fabio Martinelli

Fabio Martinelli is a research director of the Italian National Research Council (CNR) where he is referent for cyber security activities. His main research interests involve security and privacy in distributed and mobile systems and foundations of security and trust. He usually manages R&D projects on information and communication security and, in particular, he is currently the Project Coordinator of the EU Network on Cyber Security (NeCS) and of the Collaborative information sharing and analytics for cyber protection (C3ISP) project. He also serves as expert in the H2020 Protection and Security Advisory Group (PASAG) and acts as First director in the Board of the European Cyber Security Organization (ECSO). He is also member of the Italian Committee for Cyber Security Research (as CNR security expert).

Annex E, page 6

Adam Kozakiewicz

Adam Kozakiewicz

Adam Kozakiewicz has worked for NASK-PIB (Research and Academic Computer Network - National Research Institute) since 2006. Assistant Professor and head of the Network and Information Security Methods Team in the NASK Research Division. Interests include intrusion detection, honeynets, critical systems protection and virtualisation security.

NASK's representative in the Information Technology – Security Techniques Technical Committee of the Polish Committee for Standardization. Has taken part in several national and EU-funded research projects (EU: WOMBAT, FISHA, NECOMA, SISSDEN, EUNITY), currently the coordinator of the SISSDEN project. The author of over forty publications, he has spoken at many conferences. Adam Kozakiewicz holds a PhD degree in Telecommunications and MSc degree in Computer Science, both from the Warsaw University of Technology, where he also works part-time as Assistant Professor in the Institute of Control and Computation Engineering.

Laura Senatore

Laura Senatore

I am a legal consultant in the fields of Data Protection Law as well as Information, Communication and Technology Law.

I received my master's degree, magna cum laude, in Law from the University of Salerno in 2015, with a thesis about the evolution of privacy in Digital Age, with special reference to the role of personal data in social networks.

After a traineeship at the Italian Data Protection Authority, I am currently associate of ICT Legal Consulting, a law firm specialised in the fields of Information and Communication Technology Law and Privacy, and research fellow at the Italian Institute for Privacy.

Martin Schaffer

Martin Schaffer

Martin Schaffer is Global Head of Secure Products & Systems, Digital Trust Services of the SGS Group with deep expertise in cryptography and applied security for embedded devices as well as in security evaluation & certification. He is a regular speaker at international conferences, actively participates in industry associations such as ECSO and Eurosmart, where he is chairing dedicated working groups on certification. Since November 2017, he is "ad personam" a member of ENISA's Permanent Stakeholders Group. Martin holds a degree PhD-degree in computer science from Klagenfurt University, focusing on security, privacy and cryptography.

Francesco Manca

Francesco Manca is Cyber Security Senior Specialist at AON Global Risk Consulting Italy. Gained with highest honors the Master's Degree in Management Engineering at the Università di Napoli Federico II. He began his career in Management Consulting in the Governance, Risk, Compliance field in Information Security. His experience an experience in projects in national and international companies (Banking, IT providers, Energy & Resource, Financial Services, Technology, Utilities) with the below main skills: support

Francesco Manca

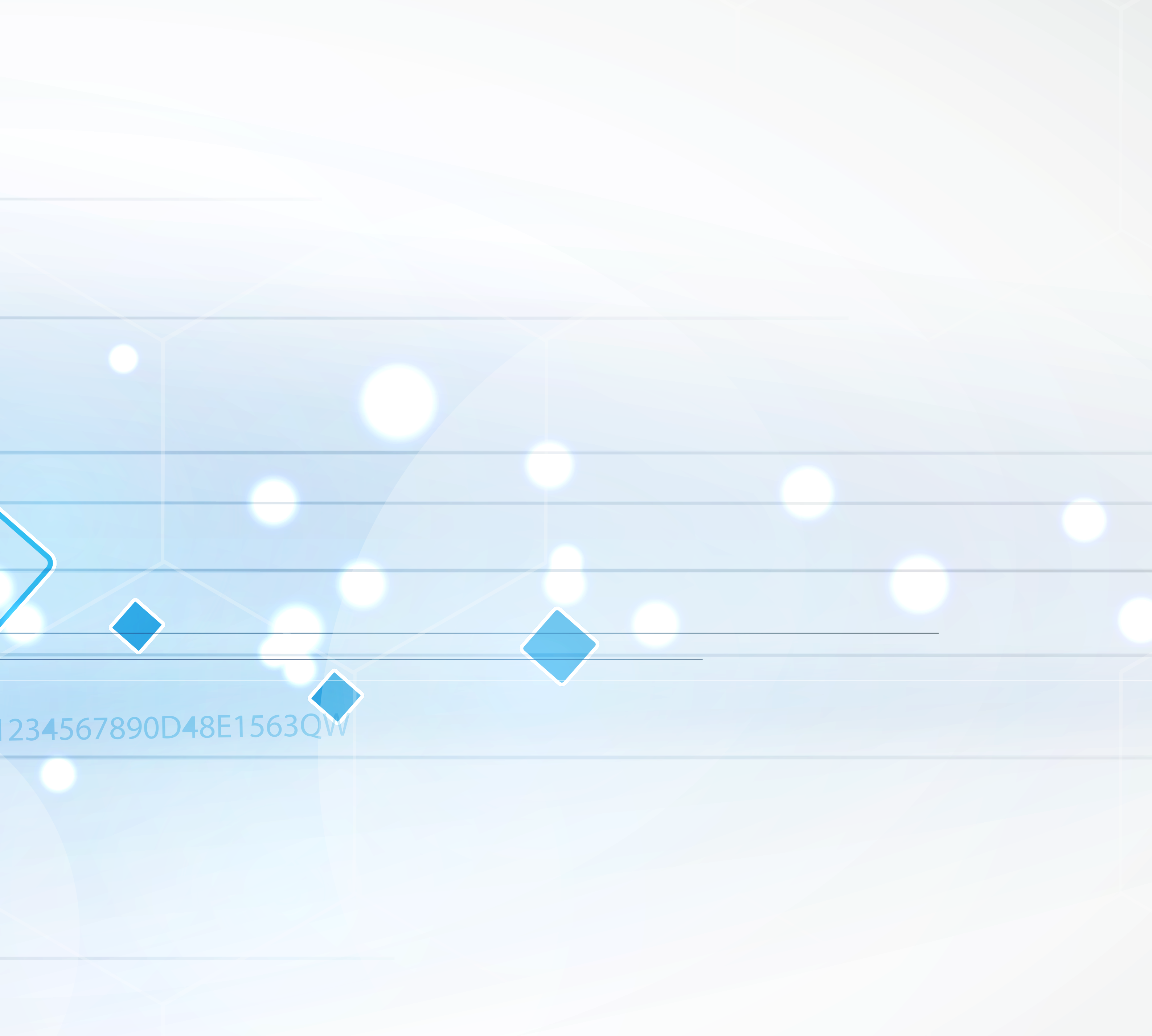
the client to assess and reach the conformity with the standards and laws in IT and privacy (e.g. GDPR, ISO27001, ISO 22301, eIDAS, AGID, ITIL, COBIT, etc.), process, policy and procedures definition in the IT and IT security field, assess the Cyber Risk Exposure Level, IT Internal and third party Audit, Defining Business Continuity and Disaster Recovery Plans and Related Operating Procedures following Best Practices (e.g. ISO22301; ISO31000...), Cyber Risk Assessment, Business Impact Analysis, supporting the clients to achieve compliance with the GDPR. With the Aon's team he defined a Cyber Risk impact quantification model and in his career supported the certification 3 companies in ISO27001:2013 standard, 2 companies to be a QTSP (qualified trusted service provider). Has a significant experience in providing IT security services for the largest IT provider for the Italian social and healthcare field. He's a ISO 22301 Lead Auditor.

Aniello Bennato

Aniello Bennato

Aniello is a Cyber Risk Project manager within Aon's department of AGRC Aon Global Risk Consulting - Governance, Risk Resilience (IT, CS & Privacy Risk Management) services.

Involved in Governance, risk and resilience projects with the aim to improve the conformity of the financial clients to European / Italian laws, evaluating the non-conformity risks, reviewing the client's policies and procedures to ensure their compliance, being part of a team involved in IT, CS & Privacy Risk Management / risk management / data governance and GDPR Compliance and implementation projects.



www.cyberwatching.eu

@cyberwatchingeu

/in/cyber-watching/

cyberwatching.eu has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 740129.