A public-private partnership providing a holistic approach to cybersecurity in Europe

Eda Aygen

ECSO Head of Communications and Advisor to the Secretary General

Digital Era 2018

25 May 2018 – Riga

www.ecs-org.eu

About the European Cybersecurity PPP

A EUROPEAN PPP ON CYBERSECURITY

The European Commission has signed on July 2016 a PPP with the private sector for the development of a common approach and market on cybersecurity.

AIM

1. Foster cooperation between public and private actors at early stages of the research and innovation process in order to allow people in Europe to access innovative and trustworthy European solutions (ICT products, services and software). These solutions take into consideration fundamental rights, such as the right for privacy.

2. Stimulate cybersecurity industry, by helping align the demand and supply sectors to allow industry to elicit future requirements from end-users, as well as sectors that are important customers of cybersecurity solutions (e.g. energy, health, transport, finance).

3. Coordinate digital security industrial resources in Europe.

BUDGET

The EC will invest up to €450 million in this partnership, under its research and innovation programme Horizon 2020 for the 2017-2020 calls (4 years). Cybersecurity market players are expected to invest three times more (€ 1350 mln: leverage factor = 3) to a total up to €1800 mln.

SUPPORT

European Cyber Security Organisation – ECSO Association has been created to engage with the EC in this PPP.
ECSO is open to any stakeholder (public / private; user / supplier) allowed to participated in H2020 projects.

About ECSO

The ECSO approach is going beyond the work of a typical Association supporting a cPPP, as it tackles, on top of Research & Innovation issues, all those topics that are linked to the market development and the protection of the development of the Digital Single Market, in the frame of the European Cybersecurity Strategy.

A peculiarity of ECSO is to include among its members (also at Board of Directors level and within the working groups*) **high representatives and experts from national and regional public administrations**. This approach is fundamental

- in a sector dealing with "security" as application of cybersecurity is and will remain a sovereign issue.
- **to increase the quality of the ECSO recommendations** to the European and national institutions → allowing a faster decision making by public bodies and a viable implementation by the private sector of the decisions taken (regulations, standards etc.).

For this reason **ECSO itself is a public – private body**, creating a **new and dynamic multi-stakeholder dialogue**, preparing for the future evolutions and needs in this sector, as envisaged in the EU cybersecurity strategy.

***ECSO working groups are dealing with the different aspects of what we call "cybersecurity industrial policy"**

Where we started (2016): cybersecurity challenges for the EU Industry

Industrial cybersecurity challenges in Europe

- Global cybersecurity and ICT market dominated by global suppliers from outside Europe.
- Innovation led by imported ICT products.
- Strategic supply chain dependency.
- Mature commodity market; professional applications under development / evolution ➔ full Digitalisation of the society and of the EU Industry
- Market fragmentation
- Innovation: strong in Europe but not always properly funded due to a lack of a consistent transnational approach and global EU strategy. Results of Research and Innovation are hardly reaching the market.
- Weak entrepreneurial culture, lack of venture capital.
- European industrial policies not yet addressing specific cybersecurity issues.
- Human factor
- Sovereignty

Industrial operational and strategic objectives

1. Protecting infrastructures from cyber threats.
2. Increased European digital autonomy.
3. Security and trust of the whole supply chain.
4. Increase competitiveness.
5. Investments in areas where Europe has a clear leadership.
6. Develop market enablers / incentives in public – private cooperation (e.g. legislation, standards, certification – when / where needed)
7. Leveraging upon the potential of SMEs.
8. Support local / regional / national competence and development.
9. Develop education (/skills) / training and awareness (citizens and decision makers)

Where we are (2018): cybersecurity has become a major global issue

EUROPEAN CYBER SECURITY ORGANISATION

- **Cybersecurity is a growing issue** at political (elections), societal (social media / privacy) and economic (industry 4.0; digitalisation) level
- **Cybersecurity is a global issue:** cyber threats hit at local / regional / local / international level. We are all (almost) on the same footing
- **Digitalisation** (including the massive introduction of IoT and IIoT) **is still a phenomenon not well understood**, in particular by the industrial sector (and in particular by SMEs)
- **IT** (Information Technology – i.e. data management) **and OT** (Operational Technology – i.e. control of operations) once disconnected **are increasingly closer and interacting**: optimisation needed, both to avoid vulnerabilities (lack of security of data for control of manufacturing operation can have disruptive impacts) and for reducing costs
- **Risk management is still a challenge** to be correctly implemented in an industrial cycle, while considering potential disruptions
- We introduce (when we can) solutions / patches validated / certified wrt the present understanding of threats, **but threats are continuously evolving: we need flexibility and scalability of systems**
- **Awareness is still limited** in all kind of stakeholders
- **CISO** (Chief Information Security Officers) are increasing in companies, but they are still difficulty to get sufficient attention from the Board of Directors and get adequate risk management measures implemented

Europe and cybersecurity: now evolving faster
Overview of the context

- 2011: Initial discussions with the EC for a European PPP on cybersecurity
- 2013: EU Cybersecurity Strategy
- 2014: Digital Single Market / Digitalisation
- 2016: cPPP on Cybersecurity
- 2017: Joint Communication on EU strategy Review and Cybersecurity Act ("New" EU Cyber Security Agency: ENISA + EU Certification Framework)
- New technologies and process: Artificial Intelligence / Big Data Analytics; IoT; 5G; High Performance Computing; IT/OT convergence; …
- Still large number of Bodies and fragmentation at EU and MS level
- Expected evolution of the cPPP (after 2020) towards a more ambitious governance and wider objectives ("enhanced PPP"), beyond R&D
- Transposition of the NIS Directive (May 9th 2018); application of the GDPR Regulation (May 25th 2018)
- EC proposal for the next MFF (2021 – 2027): May 2018 ➔ May 2019

ECSO is working in cooperation with its members to develop the European cybersecurity ecosystem

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

ECSO definition of EU Cybersecurity

European Cyber Security is our common science, knowledge, trustworthy processes, products, services and infrastructures to protect (in a sustainable way) our nations, industries / economies, citizens and institutions against damaging cyber-attacks while respecting our European Values.

ECSO VISION for EU Cybersecurity in 2027

- **Europe as global leader in cybersecurity**, having developed a **comprehensive EU cybersecurity strategy** built upon a "predict-prevention, protection, detection, respond" approach.
- **Strong, resilient and competitive European industrial (SMEs and European champions) and academic ecosystem**.
- **Cybersecurity recognized as an industrial sector, sustained by an industrial policy for Europe, supported by adequate investments** for increased EU competitiveness and digital autonomy.
- **Cybersecurity solutions effectively deployed at national, regional** / local (city) level (driven by smart specialisation).
- Well **informed European citizens and decision makers** and **highly trained cybersecurity professional workforce**.

OBJECTIVES related to the ECSO VISION for EU CYBERSECURITY

OBJECTIVES FOR CYBERSECURITY IN EUROPE

1. **Dialogue and Cooperation between public and private** stakeholders for the development of the European Cybersecurity Ecosystem
2. Develop and implement a comprehensive **EU cybersecurity industrial policy**
3. Define and implement measures (supported by adequate resources) for a **coordinated EU strategy** based upon a **prevent / predict – protect – detect – respond / remediate approach at EU level**
4. Increase market presence and **competitiveness of European cybersecurity industry / solutions**
5. Increase and target **investments for strategic security, economic and societal relevant sectors**
6. **Validate and promote European solutions** and competence
7. Foster and organise **Public and Private Development of strategic solutions and their procurement**
8. Increased **European digital autonomy** & development / validation of EU trustworthy solutions for full trustworthy European value chain
9. Increased understanding of threats in the different market verticals via **improved risk management and threat intelligence** introducing validated trustworthy innovation
10. Provide **operational support at EU level for operators and users**
11. Support **growth of start-ups and SMEs**, also with dedicated financing tools
12. **Regional / local approaches** and cybersecurity smart specialisation
13. Increase **jobs, education, training and awareness**
14. **Increase R&I** with wide participation of key stakeholders bringing innovation to market

ECSO - Purpose & objectives

- **Short term (2016-2018)**
  - R&I priorities for H2020 (2018-2020 work programme); coordination with other cPPPs
  - EU Certification & Labelling Framework
  - European HR Network (EHR-4CYBER) to foster education and training and support job growth in cybersecurity
  - Develop dialogue, harmonisation of objectives and operations between users / operators, suppliers and public administrations, within an innovative governance
  - Suggestions for the revision of the EU Cybersecurity Strategy and future investments (in the 2021 – 2027 MFF)
- **Medium Term (2017 – 2020)**
  - Prepare for post H2020 (“Horizon Europe")
  - Standardisation
  - Regional approach (smart specialisation & regional funds)
  - Support to SMEs (SME Hub / Platform; investments in start-ups; …)
  - Develop with concrete actions, education, training, awareness and cyber ranges
  - Development of trusted components, systems, services strategic for Europe
  - Support to implementation of NIS Directive; GDPR; …
  - Build International dialogue / cooperation
- **Long Term (2020 – 2027)**
  - Possible cPPP evolution into a new governance for enhanced European competences and capabilities
  - European industry among cybersecurity market leaders in targeted sectors
  - Support to business development and global competitiveness

ECSO membership overview

132 founding members: now we are **236 organisations from 29 countries and counting (included 6 new provisional membership – in brackets)**

AUSTRIA	7	ITALY	26 (+2)
BELGIUM	13	LATVIA	1
BE - EU ASSOCIATIONS	9	LITHUANIA	1
BULGARIA	1 (+1)	LUXEMBOURG	4
CYPRUS	4 (+1)	NORWAY	4
CZECH REP.	3	POLAND	6
DENMARK	5	PORTUGAL	3
ESTONIA	7	ROMANIA	1
FINLAND	8	SLOVAKIA	2
		SLOVENIA	1
FRANCE	24 (+1)	SPAIN	32
GERMANY	21	SWEDEN	2
GREECE	5	SWITZERLAND	5
HUNGARY	3	THE NETHERLANDS	17
IRELAND	3	TURKEY	3 (+1)
ISRAEL	2	UNITED KINGDOM	8

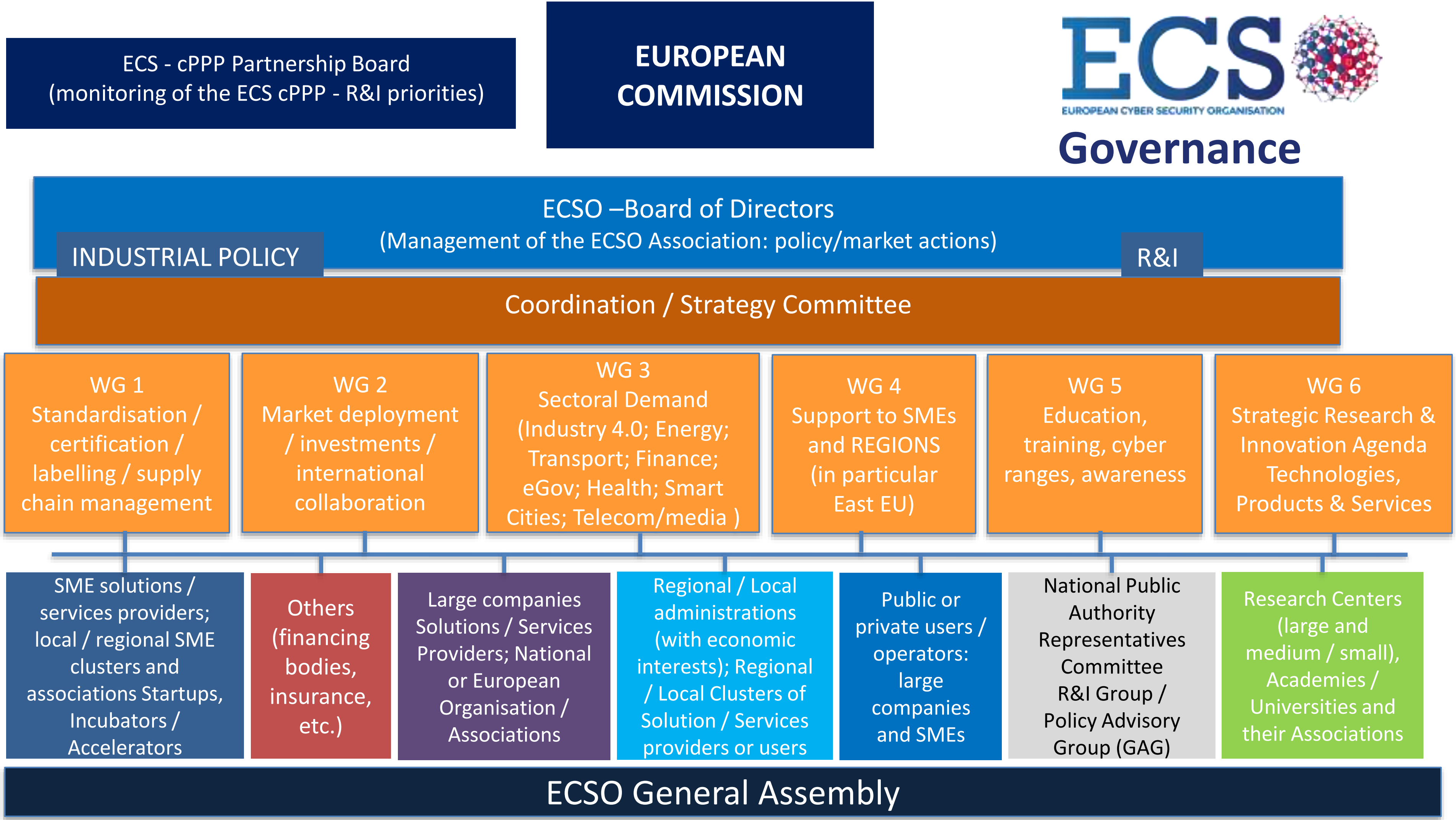
- Associations : 21
- Large companies and users: 70
- Public Administrations: 20

  AT, BE, CY, CZ, DE, EE, ES, FI, FR, IT, SK, FI, NL, NO, PL, UK, BG, SE, GR +

  observers at NAPAC (DK, HU, IE, LT, LU, LV, PT, RO, SI, MT, …)
- Regional clusters: 6
- RTO/Universities: 63 (+1)
- SMEs: 51 (+5)

ECS
EUROPEAN CYBER SECURITY ORGANISATION

Governance



ECS - cPPP Partnership Board
(monitoring of the ECS cPPP - R&I priorities)

EUROPEAN COMMISSION

ECSO –Board of Directors
(Management of the ECSO Association: policy/market actions)

INDUSTRIAL POLICY

R&I

Coordination / Strategy Committee

WG 1
Standardisation / certification / labelling / supply chain management

WG 2
Market deployment / investments / international collaboration

WG 3
Sectoral Demand (Industry 4.0; Energy; Transport; Finance; eGov; Health; Smart Cities; Telecom/media)

WG 4
Support to SMEs and REGIONS (in particular East EU)

WG 5
Education, training, cyber ranges, awareness

WG 6
Strategic Research & Innovation Agenda Technologies, Products & Services

SME solutions / services providers; local / regional SME clusters and associations Startups, Incubators / Accelerators

Others (financing bodies, insurance, etc.)

Large companies Solutions / Services Providers; National or European Organisation / Associations

Regional / Local administrations (with economic interests); Regional / Local Clusters of Solution / Services providers or users

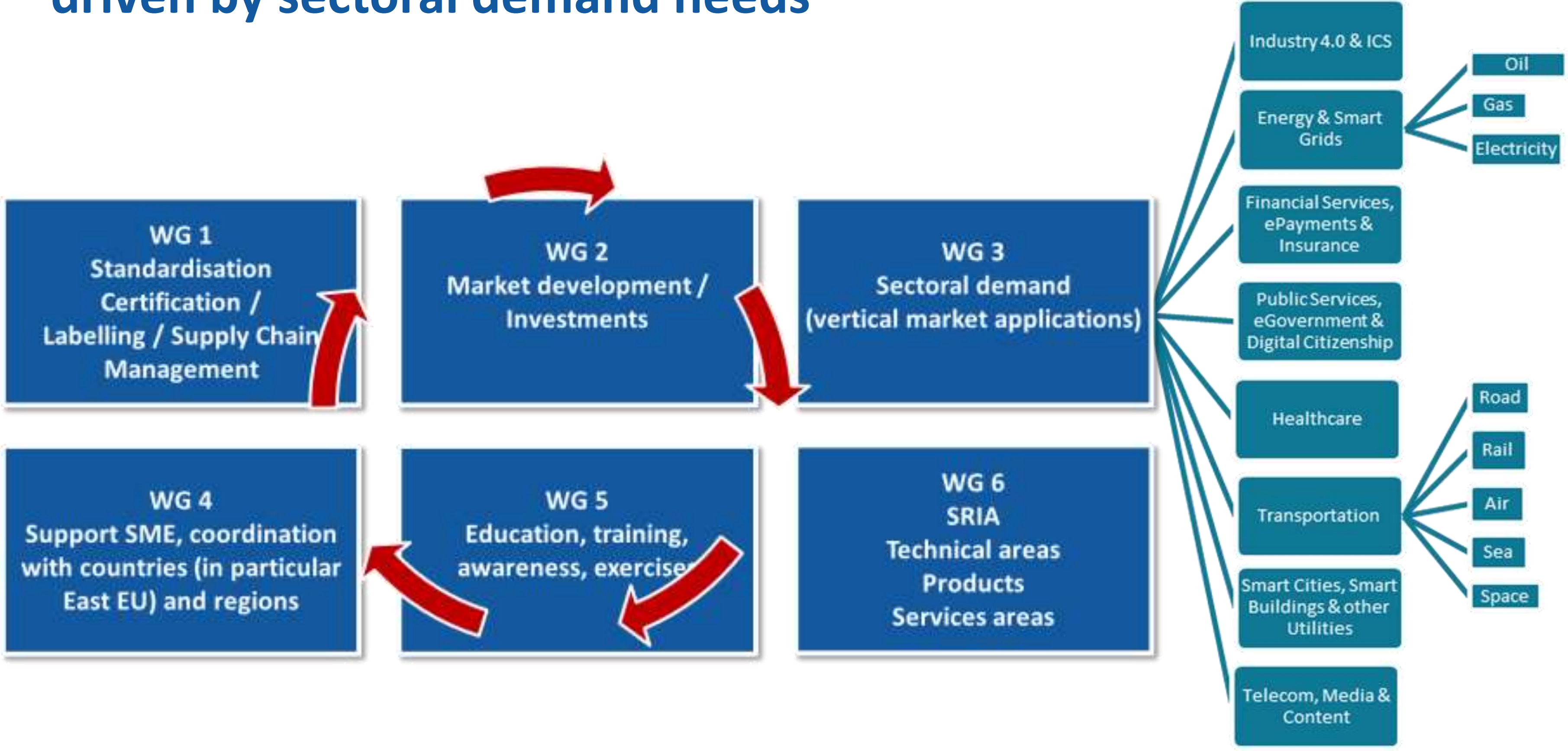
Public or private users / operators: large companies and SMEs

National Public Authority Representatives Committee
R&I Group / Policy Advisory Group (GAG)

Research Centers (large and medium / small), Academies / Universities and their Associations

ECSO General Assembly

ECSO Working Groups are interlinked and driven by sectoral demand needs


WG 1
Standardisation / Certification / Labelling / Supply Chain Management
WG 2
Market development / Investments
WG 3
Sectoral demand (vertical market applications)
WG 4
Support SME, coordination with countries (in particular East EU) and regions
WG 5
Education, training, awareness, exercises
WG 6
SRIA
Technical areas
Products
Services areas
Industry 4.0 & ICS
Energy & Smart Grids
Oil
Gas
Electricity
Financial Services, ePayments & Insurance
Public Services, eGovernment & Digital Citizenship
Healthcare
Transportation
Road
Rail
Air
Sea
Space
Smart Cities, Smart Buildings & other Utilities
Telecom, Media & Content

GDPR & CYBERSECURITY

Art 5 “**Personal data shall be processed in a manner that ensures appropriate security of the personal data”**

→ Technical & operational measures must be taken

Data controllers and processors are required to carefully think about the ways to effectively secure personal data and take all necessary steps in this respect.

→ They are expected to make risk assessments and mitigation plans

→ Data controllers and processors must pay attention to the state of the art and the cost of implementing them. In a hyper connected world this magnifies the potential of secure networks to be compromised

In some cases, it will be necessary to use encryption and pseudonymisation of personal data, adopt instruments for restoring availability and access of data, and create processes of for evaluating the effectiveness of data security measures.

A multi-layered approach to cybersecurity is more effective

→ Develop robust data processing strategies (implement strong protocols to check the balance of power between the controller and the processor)

What does GDPR do?

- Increases the individual’s expectation of data privacy and the organisation’s obligation to follow established cybersecurity practices.
- Requires organisations to appoint a Data Protection Officer (DPO) who will be involved in “regular and systematic monitoring of data subjects on a large scale” → creation of a new role inside of an organisation
- Enshrines “privacy-by-design” as a required standard practice for all activities involving protected personal data.

GDPR & CYBERSECURITY

What does this mean for the future of cybersecurity and how is the digital economy going to be impacted as a whole?

How will GDPR shift the landscape of cybersecurity?

With the cyber threat landscape fast evolving, regulations such as GDPR could be considered as a positive development. It will force companies to pay close attention to data security and data management.

Ultimately cybersecurity and GDPR have a common denominator: data management

WG activities: achieving wider objectives in a wider dialogue across public – private stakeholders

WG1 - standards / certification / label / trusted supply chain (135 members from 27 countries with 289 experts).

Industry organizations or citizens with no specific knowledge need to be able to quickly assess if an item will provide confidence that required Security and Privacy is provided

Security certification as a means of security assurance demonstrates conformance to a security claim for an item. Many certification schemes exist, each having a different focus (product, systems, solutions, services, organizations ...) and many assessment methodologies also exist (check-list, asset-based vulnerability assessment ...). WG1 launched in October 2016, has created two documents in the initial phase of the work:

•State-of-the-Art Syllabus (SOTA)

lists all standards and specifications related to Cybersecurity known to and deemed relevant to be used for assessing the security strength of an item.

•Challenges of the Industry (COTI)

Privacy is mentioned multiple times, especially in the light of GDPR, asking for “Privacy by Design” to be considered

Basis for a Meta-scheme approach to certification which encompasses many of the existing certification schemes (e.g. component certification, process certification, service certification, etc.). It does so by evaluating the level of confidence in the security strength of a product, system, solution, service or organisation that results from a scheme used, and map this onto a harmonized set of levels defined by ECSO. These levels represent the level of confidence and the scope of security functionality of the item certified.

WG activities: achieving wider objectives in a wider dialogue across public – private stakeholders

WG3 - verticals: Industry 4.0; Energy; Transport; Finance / Bank; Public Admin / eGov; Health; Smart Cities; Telecom/Content/Media (121 members from 24 countries with 266 experts):

With the deployment of the digital world and its ubiquitous connectivity, Security and Privacy is now a concern for every business and every citizen.

STATUS: Four sector reports finalised; concrete project to develop common application for incident reporting and information sharing (led by banks but applicable to other sectors); non-paper on recommendations for implementation of GDPR foreseen

OBJECTIVES 2018: Sector specific reports on users' needs / SOTA; Report on NIS implementation and harmonisation of incident reporting; Sector-specific guidelines on implications of GDPR on cybersecurity and privacy (avoid duplication of reporting obligations for companies with NIS); Support to ISAC's implementation; envisaging operational platforms

WG activities: achieving wider objectives in a wider dialogue across public – private stakeholders

WG5 - Education, training, awareness, cyber ranges (98 members from 26 countries with 202 experts):

STATUS: Cyber range study assessing capabilities and motivations. Position Paper on Gaps in Education & Professional Training. EHR4CYBER Network White Paper on Information and Cyber Security Professional certification ongoing, recommendations / mapping for a European framework for education and competences (matching profiles and skillsets);

WG6 - Strategic Research and Innovation Agenda (157 members from 28 countries with 351 experts):

“The industry must seize the opportunity of the GDPR to achieve the right balance between Privacy and Innovation”. (Chris Combemale)

2017 ECSO submitted SRIA to EC: Cyber Technical Projects

- Data Security and privacy technologies

Secure and privacy aware data processing and storage
User friendly (i.e. also for non expert users) transparency and control options incorporated as “standard features” across all storage solutions
Balancing privacy needs and business demands
Facilitate the implementation of the regulatory context, e.g., the GDPR

WG activities: achieving wider objectives in a wider dialogue across public – private stakeholders

- <u>Distributed Identity and Trust Management</u>

Privacy-respecting identity management schemes
Further steps towards interoperable, scalable identity management schemes
Authentication operates in a distributed fashion without single points of failure on critical paths
Large adoption of distributed trust management frameworks
Citizens will enjoy the privileges of services needing strong authentication
Increased trust in the cyber world
Requirements for trusted security credential provisioning (e.g trusted secure elements)
More efficient online Business

- <u>User centric Security and Privacy (referenced throughout Secure Societies WP)</u>

Increased awareness
Fewer cases of identity theft
Security and privacy as an implemented and not just claimed human right for everyone
Best practices in authentication are supported by usable technologies embedded seamlessly into applications, including the management of different levels of authentication and dynamicity.
New tools and technologies for both digital service providers and end users that enable User centric security and privacy.

Conclusion

Raise awareness: GDPR is an opportunity to educate / train

-

Be adaptable: today is about compliance but tomorrow is about adapting to the cyber threat landscape

-

Keep a holistic approach: implication of GDPR in certification mechanisms, R&I, exchange of information, education

-

Collaborate through a Public-Private Partnership

CONTACT US
BECOME MEMBER!

European Cyber Security Organisation 10, Rue
Montoyer
1000 – Brussels – BELGIUM

www.ecs-org.eu

E-mail:
Ms. Eda Aygen
Head of Communications &
Advisor to the SecGen
media@ecs-org.eu

Follow us
Twitter: @ecso_eu