European Cybersecurity Industry Leaders

Recommendations on Cybersecurity for Europe

How can the EU be more trustworthy and digitally secure?

How can Europe support the successful development of European cybersecurity champions?

A report to M. Günther H. Oettinger European Commissioner for Digital Economy and Society

A report to M. Günther H. Oettinger European Commissioner for Digital Economy and Society

Chairman:
Thales – Marc Darmon, EVP Secure Communications and information Systems

Vice Chairman:
Atos – José María Cavanillas, Head of Big Data and Security, Atos

Airbus Group – Axel Krein, SVP, Head of Program & Cyber Security Program Directorate, Airbus Group

BBVA - Santiago Moral Rubio – BBVA Group CISO

BMW – Andreas Sauer, BMW Group Corporate and Governmental Affairs

Cybernetica – Oliver Vaartnou, CEO

Deutsche Telekom – Dr Thomas Kremer, Board member for Data Privacy, Legal Affairs and Compliance

Ericsson – Ulf Ewaldsson, Group CTO and Head of Group Function Technology

F-Secure – Jari Still VP, Research, Development and Operations

Infineon - Thomas Rosteck VP and General Manager, Business Division Chip Card and Security ICs

Table of Contents

The European Cybersecurity Industry Leaders (ECIL) workgroup is a group of leading European industry players who have decided to join forces in spring 2015 to prepare a set of recommendations on Cyber Security for European citizens and businesses, and on a Cyber Security industrial policy, for consideration by the European Commission.

The ECIL members are Airbus Group, Atos, BBVA, BMW, Cybernetica, Deutsche Telekom, Ericsson, F-Secure, Infineon, and Thales.

Introduction

European Companies support the recently adopted strategy of the European Commission for a Digital Single Market. One of the pillars of this strategy is a Cyber Security policy which promotes high standards of protection for European citizens and businesses.

The Digital Single Market strategy comes at the right time as Europe is in danger of falling behind in the international digital economy. To improve its position Europe has to build on its strengths and tackle its weaknesses: Nowadays Europe is known and valued for a high level of data security and privacy. The EU is probably the most trusted area in the world when it comes to those topics. This is a significant competitive advantage that has to be kept and extended.

On the other hand, there are very few market players in the EU that can – e.g. in terms of size - keep pace with big global players especially from the US and Asia. It is necessary to level the playing field for European players with regard to cooperation, consolidation, regulation and market power.

The first part of this paper aims at **measures to make the EU more trustworthy and digitally secure**. This contains:

- Create a Level Playing field within Europe and promote it internationally
- Enlarge European Cybersecurity monitoring and advising
- Recommend additional regulatory measures

The second part focuses on the **successful development of European cybersecurity champions**. To reach this goal, we have to concentrate on the following measures:

- Reinforce cooperation between the European Member States
- Foster EU involvement in Cybersecurity legislation, standardization and labelling
- Support the development of an academic ecosystem for Cybersecurity and utilize Research and Innovation instruments
- Create a supporting financial and fiscal environment for European Cybersecurity areas of excellence
- Positively consider market consolidation to allow the development of European cyberchampions

It is important to keep in mind that these two objectives will also contribute to the establishment of the European Digital Sovereignty. This European Sovereignty will preserve EU and Member States ability to define and impose ambitious and demanding cybersecurity requirements, adapted to the cyber protection of all critical players in Europe.

A. How can the EU be more trustworthy and digitally secure?

Threats to information technology systems are common, and malicious attacks have increased in recent times. This paper presents a set of recommendations to strengthen the Cybersecurity of Europe:

Should be directly concerned by these set of recommendations the European institutions themselves, Critical Infrastructures Players of course, and Corporates (were they large companies or SME) processing sensitive and critical data in the context if their activities, Citizens should be informed at least so as to be aware of the risks they may occur.

Three axes are considered in this first set of recommendations:

- Level playing field for enterprises
- European cybersecurity monitoring and advising
- Additional regulatory measures

1. Level Playing Field

In agreement with the NIS Directive and with the objective to promote a cybersecure European Single Digital Market **all players of the Information and Communication Technologies value chain, operating or not from a European Member State, should adhere to equal requirements concerning data protection and cybersecurity.** This is to ensure that European citizens and businesses would have access to products and services with at least a basic adequate security level, independently of the provider. At the same time, it is essential for the competitiveness of European companies to end the situation of a fragmented landscape within the EU which makes it possible for non-European players (like Over The Top players / OTT) to opt for the Member State with the least level of protection (e.g. Ireland). This shall not mean that such harmonized EU levels of protection should be unreasonably burdensome in relation to the importance of the protected data or infrastructure. It is furthermore of equal importance, in order to ensure the global competitiveness of EU-based actors, that the regulatory scenario in the EU does not hamper or constrain the commercial actors and therefore risk to be detrimental to the global competitiveness of EU-based companies. The global competitiveness aspects also points to the need to seek transatlantic economies of scale thus harmonization of standards and best practises with the US is essential to facilitate. The use of industry driven and internationally accepted standards and best practices are recommendable tools. However a fragmented and/or overly detailed regulation risk to constrain the resources of EU based actors in a way that could make it difficult to be competitive from a global market perspective. Therefore, we advocate a co-regulation approach working together with industry. This would also be counterproductive to the EU goals as such to become a global leader in ICT usage overall.

The NIS directive's initiative of creating a secure Cyber Space for the European Union to provide a high level of protection for European Citizens and businesses is one step into the right direction. This is also seen as beneficial to strengthen European cybersecurity industry players in the world stage.

It is important that all market operators of the Digital Economy share the responsibility for a secure cyber space. It has to be ensured that all players involved are committed to secure digital products,

software and services. This includes Network Operators as well as hardware and software Manufacturers and Internet-based services (such as Over The Top). Only if the entire value chain is made secure, the risk of attacks can be mitigated. Additionally, this would allow for a fair sharing of responsibilities and financial burden. **All players serving the European market, irrespective of their location within or outside the European Union shall comply with the NIS directive.**

Central to the goal of promoting a cyber-secure Information and Communication Technologies ecosystem in Europe is the need for a harmonized approach in terms of the definition of the above-mentioned requirements. That is, the rules ought to be equal in all EU member states, so as to avoid citizens and businesses being subject to different levels of security in various member states. The NIS directive defines ambitious objectives that the Member States will have to implement, defining the means to achieve the goals of the NIS directive. In this context, harmonization should be also ensured to guarantee a real European level playing field.

The enforcement of such requirements might be done through an independent control or audit process conducted by member state agencies as long as they all do the enforcement as per the same criteria and rules across all Member States, thus ensuring that there is within the EU a levelled playing field for the benefit of European citizens and businesses independently of their country of residence.

In this context, we agree with the European Parliament[1] that the Safe Harbour Agreement needs a revision, as it may in some cases turn into a loophole to circumvent EU protection standards for data processing. Safe Harbour does not provide EU citizens with adequate effective protection. There is a real need to solve this problem. Lower requirements in the USA would enforce the already significant competitive advantages for US-based companies and therefore, outdistance the European digital economy.

2. European cybersecurity monitoring and advising

The cybersecurity of citizens and businesses depends largely on technology that is secured (free of vulnerabilities) and on adequate security management processes on the part of technology producers, operators and users. However, when all else fails, the response to cyber incidents is equally important.

More could be done to enhance cybersecurity after a fortuitous incident or a malicious attack beyond of existing mechanisms (e.g. CERTs).

As in the previous section, **EU-level harmonization and supra-member state mechanisms are needed with an important prerequisite which is to make sure that European harmonization measures do not lead to a regression of security requirements levels compared to the national existing ones.**

- EU-CERT, in addition to the national existing CERT already exists and should be reinforced in its role and responsibilities

[1] European Parliament resolution on the European Parliament's priorities for the Commission Work Programme 2016 as stated in 83 "An area of justice, security and fundamental rights". See http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B8-2015-0662&format=XML&language=EN

- Exploiting EU-wide knowledge of cyberattacks for the benefit of businesses and citizens alike.
- Facilities for effective centralized real-time publication and consultation of Trust Lists [2]of certified Trust Service Providers

These measures exploit the value of security information sharing among organizations, which has proven as a successful and effective tool to combat cyberattacks, as seen in industry-led initiatives such as ISACs[3].

While an EU-wide, Member States-driven ISAC may be difficult to implement (due to reluctance to share critical and confidential data with other member states), an initiative in the spirit of existing ISACs could be promoted by the Commission:

- In the form of an EU-level ISAC for voluntary participation of public administrations and private sector companies
- In the form of sector-specific ISACs (cross-border) in Europe. Some of these exist today. A Financial Services ISAC is being considered in Europe, mirroring the successful Financial Services ISAC operating in the U.S.

Such collaboration would encourage and facilitate security information exchange between the Members States and Industry critical sectors to create a more EU cyberspace for businesses and citizens. This would include:

- Confidential sharing of cyberattacks; malware, etc. between member states and industry / CIPs
- For Member States (existing or future) without CERT infrastructures, the EU should support them to acquire the capacities to have their own CERT capacities, so as to allow EU-wide response capabilities (Cybersecurity capacity building supported by the EU)
- Member State-level harmonization of CERTs, where multiple CERTs exist.

Monitoring the status of cybersecurity at EU level by a European independent body would additionally foster **the EU position.** By establishing a **European Cybersecurity Situation Centre**, dependent on the EU-CERT, which deeply monitors security situation and also gives advice to all citizens and companies EU would create beneficial impact.". Whether this function could be carried out by an existing entity (EU agency or other) is a matter to be discussed.

3. Additional regulatory measures

Any possible regulatory measures have to be commensurate with the risks to be addressed and the related market segments. Where necessary, a differentiation between markets (e.g. Defense Government or financial market) has to be put in place as each one may have different regulators and specific security risks. Civil markets shall be part of the Digital Single Market meaning same standards, compliance methods and principles for regulatory oversight shall apply across the EU.

[2] https://ec.europa.eu/digital-agenda/en/eu-trusted-lists-certification-service-providers
[3] Information Sharing and Analysis Centers

The adoption of the General Data Protection Regulation (GDPR) will be a step in the right direction to harmonize protection standards across the EU. Together with the NIS-Directive, the GDPR builds an important instrument to safeguard the high EU standards of security and protection of data.

In some situations, self-regulation cannot be the tool of choice, as it was not effective in the past. In these cases, there may be a need for a legislative approach. The following presents some suggestions to structure the discussion of potentially necessary regulation:

Security of systems and services:

- Regulation at European and National level must address the problem of out-dated and vulnerable hard- and software in operation, which is increasingly targeted to attack critical infrastructures and digital services. Manufacturers of hard- and software as well as critical infrastructure providers should be required to resolve vulnerabilities or mitigate or control the risk derived from them.

- For particularly **critical components the security of the products could be evaluated by an independent test centre as per the Common Criteria approach**. However, the component level assurance is only valid for that component in a specific configuration and release. Thus, the entire system/solution design, operational and service performance could be a more important contributor to the security of a critical service. Here there are best practices and current (Telecom Directive 2009) and proposed (NIS Directive) regulatory instruments to secure service performance. .There should be **no dependency on the individual manufacturers of critical network components**.

- **Promote a "Secure-by-design" approach: Compel technology vendors, service providers and companies providing online services to develop and issue "secure by design" products and software** in the same way as the rest of "physical" markets such as automotive, construction, retail, etc.

Security of data flows:

- Crossborder operations of Telco-Services are the future. Therefore, a European legislative or regulatory approach is necessary to combine national security needs (Critical Infrastructure, Lawful Interception, Confidential Governmental communication, etc.) on the one hand and the possibility to run multinational networks from only one or several countries on the other hand. As proposed by the Commission in its DSM-Strategy unjustified restrictions to the free flow of data within the EU should be avoided. In order to enhance trust and a more secure infrastructure, data traffic that has its origin and its destination in the EU should not be diverted through other judicial areas. Nonetheless, the Internet remains open; access to servers located outside Europe must not be impeded or blocked.

- Looking to the future, protection of sensitive or personal data in transit and its integrity in storage will become a requirement. This can be handled independently on different layers, e.g. encryption as an application defined, running between the endpoints defined by the application, and also by default included as part of the subscription to the communication

service. To the user, end-to-end encryption may be quite complicated and the level of protection achieved to the data, how, where and by who may by quite obscure. Therefore more research is needed to exploit the capabilities of encryption in the end-to end scenario. Furthermore communication service providers must have the opportunity to offer encryption services from the user device and across the service provider network.

Supporting the fight against cybercrime:

- Harmonization of legal frameworks to combat cybercrime: EU-level regulation or member state level harmonization of legal frameworks would be very helpful to ensure cybercrime can be prosecuted efficiently. Criminal organizations and individuals take advantage of differing legal frameworks to conduct their actions. Europe can be better prepared to combat cybercrime is law enforcement agencies throughout Europe can share a common base to work with, enabling easy sharing of information that facilitates the identification of the sources of criminal activity.

- There is also a need to develop the appropriate legal framework for telecom operators and other service providers to proactively protect (i.e. block access to proven malicious/illegal sites) both citizens and companies online activities.

B. How can Europe support the successful development of European cybersecurity champions?

There certainly exist numerous hidden champions within the EU and many potential future champions. To support their development and to make them competitive at a global level an appropriate environment has to be created. We put forward recommendations in four key aspects:

- Cybersecurity certification pillars
- Member state cooperation
- Supporting ecosystem for cybersecurity
- Policies toward market consolidation

1. Cybersecurity certification pillars: legislation, standardization and labelling

Fragmentation of the European market is currently the main barrier to the creation of strong European businesses on cybersecurity. The growth of an innovative start-up may be conditioned by the ability to obtain multiple different required certifications (per member state) to sell its products and services in each member state (and even in different regions within certain countries). This results in significant costs, but more importantly, consumes the energy of the innovators in dealing with repetitive processes, undermining the further development of innovations to meet and exceed the offer of competitors which often originate outside the EU.

This recommendation is **for establishing voluntary certification processes at the European level based on commonly agreed criteria between member states, such that a certification, seal, label or standard obtained in any one member state should be EU-level and valid and recognized throughout the EU, without the need for any further certification processes of any kind.**

2. To this effect, we present three pillars for EU-wide cybersecurity certification

i. Legislation

Today legislation is in place in the public domain, for public procurement. Different procurement requirements are present in each member state. Harmonization is needed EU-wide so that a cybersecurity product, solutions or service delivered in compliance with a single set of requirements can be compliant throughout the EU.

The scope today concerns mainly critical infrastructure protection. Other domains such as autonomic drive, car-to-car communication, telematics and mobile health services, navigation and positioning should be also considered in a near future.

ii. Security standards

Industry-led security standards exist in several sectors today (financial services, healthcare, border control, road pricing, telecom, etc). It is important to ensure the participation of European businesses and start-ups in global standardization task forces, so as to promote European solutions through such standards to gain relevant positions in the worldwide market.

Furthermore, new domains where Europe is leading are emerging, and the creation of security standards will be beneficial for creating European champions (e.g., e-calls, car to car communication)

Options to multiply European influence on global standardization exist: With the support of an EU-driven initiative for the promotion of standardization activities in the EU, companies could involve themselves more deeply and bring European influence on global standardization to an appropriate level. EU should establish a delegate-system that enables European companies (including SMEs) to bundle their forces and to act as representatives for the EU in standardization committees to transfer the heavy-weight of the EU to the European industry experts and make them heard on a global level.

iii. European cybersecurity Labels

We put forward a proposal for the creation and operation of European Cybersecurity Labels, a mechanism for voluntary certification against a published set of criteria or requirements for each labeled level. It would benefit label holders as a seal of guarantee of security in the company's products or services, and would help corporates and consumers identify secure providers. The labels would be for manufacturers of products, solutions and service providers only. End users, consumers, customers or companies of these products would not be obliged in any way by law or regulation to buy security products with these specific labels. End users, consumers, customers or companies would be free to choice what security products they can use.

Labels will not require the development of new security recommendations or requirements. They can be built on best practices and other internationally recognized existing certifications. The added value of this European label resides in its EU-wide recognition and acceptance, thus helping in the defragmentation of the European market, and with the creation of stronger market positions for trustworthy companies and creating competitive advantages.

Different levels of labels can be devised, corresponding to increasing levels of security in the organization's products and services.

Where labels have been used, compliance with the label requirements should be monitored and regularly checked. The set of requirements ought to be defined at the EU level, coordinated by an EU-level agency, while enforcement checking could be delegated to national agencies in charge of cybersecurity practices. Compliance validation would be conducted in the same manner by any one national agency, and would be recognized EU-wide. It is important to highlight that companies are not obliged to have security labels, but if they do, then they must comply with the requirements imposed.

Setting up and operation of this labeling mechanism would imply some costs, so resources should be allocated to put this mechanism in place.

The requirements for each level of label could be defined by an EU-level agency in agreement with national security agencies of member states. The set of requirements will be a single one for the whole of Europe (baseline). Member states cannot request additional criteria/requirements at the national level to the baseline requirements, as this would defeat the purpose of the label. However, some critical infrastructures at the national level might require some specific local criteria. In this case, additional local criteria would come on top of the baseline ones.

Some such requirements may include:

- Organizations must implement a security management process (including procedures, necessary resources, etc.) in the operation of their services or development of their products
- ISO 2700x certifications in place
- "Secure-by-design" or "Privacy-by-design" principles followed in the development of product/services as stated in the NIS Directive.
- Internationally recognized ones such as ITIL, SAS 70 or NIST based.

3. Cooperation between European Member States

Cooperation at European level is a key success factor to facilitate the creation of a European single cybersecurity market:

- Cooperation between State members on CERT activities would reinforce European added value and expertise (incident reporting, regulatory obligations, threat intelligence). Effective cooperation and transparency between the Europe Members States will contribute to a stronger cybersecured EU.

- In other to promote cyber resilience of those companies who do not have CERTs already, that are big in size, operational risky or a clear target of cybercrime an incentive program should be put in place to promote Cyber Emergency Response Teams(CERT) in their organizations.

- An EU Cyber Situation Centre (see above) that provides a real-time overview of the situation (see above) would be beneficial. The centre could also conduct consolidated awareness measures etc. In combination with respective incentives it could foster the willingness of companies – also on SME-level – to establish functions responsible for cybersecurity within their organization. This EU Cyber Situation Centre should be integrated within National and European CERTs.

- At European State level, cooperation in the definition of selection criteria for Cybersecurity products/solutions/services and application of European cyber guidelines and labels.

- Definition of European criteria should be led by a body like ENISA, and then validated by all stakeholders.

- A collaboration process should be defined to enhance collaboration and information sharing between member States: definition of the type of information shared, legal requirements (when the incident report has sufficient legal evidence) and process to share personal data (such as IP addresses) and the reactivity requirements, protection mechanism concerning the usage of critical information.

4. Supporting ecosystem for cybersecurity

i. Through academic and research involvement

- Tier 1 Engineer and Business schools to support start-up development and innovation
- **Creation of European cybersecurity Chair with the support of European industry leaders. This will contribute to preparing the next generation of cyber experts for Europe.**
- Europe should also attract external talent. European training programs in different Member States Universities or Tier 1 schools of the EU could be a competitive advantage versus Asian or US training programmes.
- Cybersecurity has to become part of general university education. Akin to technicians having to learn basic economic rules, it has to be assured that also business students (company leaders in the future) and engineers, in general, are well aware of the implications of cybersecurity. It is necessary to ensure professionals will be conscious about cybersecurity when entering the work force, whether in management positions or production environments. The community cannot expect that a small number of cybersecurity experts will cover the demand for this discipline.
- Awareness can and should start earlier: Cybersecurity has to be an integral part of the school education and forming part of a broader "Citizens Cyber Skills" curriculum. Here the understanding of issues like personal privacy, rights and responsibilities when acting in the cyber world should be part of the general societal maturity aspects of the school education and not just part of using IT technology as such. Teachers should be supported by being equipped with respective materials for the different school grades. A voluntary EU-wide campaign could be some kind of "big bang" and prevent discussions about mandatory embedding into the curriculums.
- Market awareness and board room "education" material would also be beneficial. In this sense, ENISA in coordination with public and private companies could develop materials better suited for European businesses (large and small), while also supporting the Member States with less developed capabilities in cybersecurity through European training and awareness programmes.
- Supporting financial and fiscal environment for areas of excellence and utilize Research and Innovation instruments
- Research on 5G - technology and the following generation of mobile standards would foster cross-sectorial cooperation between CIP-relevant sectors like energy or transport. The development of a common, cross-sectorial, security environment is crucial for the roll-out of, for example, Smart City or Industry 4.0 projects that require a secure, high performance and resilient technology platform.

The EU should create conditions to support and develop European start-ups and emerging/promising cyber-technologies (e.g. European SIEM, multi-sovereign probes, etc.).

The EU could create a European Agency in charge of supporting R&D developments from very early stage of research to operational and business applications, focusing on the creation of a European investment fund dedicated to cybersecurity: market intelligence, competitive analysis and innovation screening, investment and support to early stage development, financing support, etc.

ii. Through policy and investment instruments

Identification of areas of excellence of the Cybersecurity European industry and focus on these components of the value chain to increase European added value and differentiation, focusing on scale, complexity, future-proofing solutions and in vertical and cross-sectorial aspects of cybersecurity, using a number of vehicles and instruments:

- Utilization of research and innovation instruments like Horizon 2020
- Precommercial public procurement
- Cross-sectorial cybersecurity trials and exercises
- Contractual Public-Private Partnership 4 in cybersecurity
- Creation of a European Cybersecurity Laboratory to conduct research, testing solutions and analysing threats between industry and European research centres. This EU-level Cybersecurity Laboratory could pool resources from existing national cybersecurity excellence centres.

Creation of incentives financial and fiscal conditions to make sure strategic assets and companies remains in Europe and do not relocate to US or Asia to operate their business once developed.

- Eg: lower taxes on labour costs for Managed Security Service Provider (MSSP) businesses operated in European countries to avoid offshoring trends

- Also, companies could be incentivized to establish dedicated cybersecurity representatives (see above) by free support of the "EU Cyber Situation Centre", tax reduction for respective costs, assurance rebates, etc.)

- Ensure Europe is/remains attractive for start-up and cybersecurity experts/gurus to avoid talents migrating outside Europe. A competitive job market is needed in Europe to attract talent, much like talent is drawn today to major technology hubs in the world, where competitive innovation is happening.

5. Initiatives towards market consolidation

Market consolidation should be positively considered in the field of cybersecurity to allow most competitive European companies to scale up faster and efficiently and allow keeping pace in front of dominant US players. Therefore European mergers rules must be adapted accordingly.

- The current competition and merger policy in the EU does not foster the EU-wide pooling of resources, by for example, adopting the "Airbus approach" in the telecommunications industry. The fragmentation of the European market (around 200 providers against only four in the US) has enhanced the dominance of US-players not only from the competition

[4] http://ec.europa.eu/research/industrial_technologies/ppp-in-research_en.html

perspective but also in the fields of data protection and cyber security. We need a level playing field regarding privacy and security between Europe and United States.

- The facilitation of mergers, leading to a better consolidation of the market must enable European operators to achieve the economies of scale which are needed to invest in future network infrastructures and to compete with "Over the top" providers. Mergers will also have an immediate effect from R&D budget which will be able to do more for the same money rather than developing competing technologies in competing companies.
- Therefore European merger rules must be updated. Turnover should not constitute anymore the best or the unique criteria to assess the impacts of a merger. Latest market developments and global industrial dimensions are to be taken into account by competition authorities.

APPENDIX

Additional contributions from European leading cybersecurity players and Security Agencies

This section consolidates comments received from Cybersecurity players and Security agencies and gives an overview of additional recommendations that could also be considered

Comments provided by: Zurich Insurance Company Ltd, Credit Suisse, Nordea, British Telecom, Federal Ministry of the Interior of Germany, Bundesamt für Sicherheit in der Informationstechnik (BSI) / Germany, Government of Sweden, INCIBE Spain, Telefónica Spain, CNPIC Spain, Bosch Germany, Secunet.

i. Information sharing

"*We would very much welcome an EU-level ISAC cooperation platform between the Member States and private companies, which would promote and enable confidential sharing of cyberattacks. Indeed, more information is needed from private sector victims of cyber-attacks, in order to better understand the nature of rapidly evolving risks and the impact they can have. Also, more information sharing is needed to further develop cyber insurance products.*"

"*Whilst sharing of such information occurs to some extent, a concern that information could become public, damage reputations or create liability issues poses a major barrier. This is particularly true in data sharing arrangements with the public sector. To address this issue and incentivize information sharing, recommendation around liability limitation for companies that share information should be considered.*"

ii. Public Private Partnership

"The important role of more generalist multi-stakeholder dialogue forums, whose strategic focus includes global governance, cyber risk management and thought leadership, should be acknowledged. For insurers, policymakers should consider how to support important information sharing work within the industry, such as that of the Chief Risk Officers (CRO) forum. Through the CRO Forum, the insurance industry is currently establishing infrastructure, through the Chief Risk Officers' Forum. This work will help to capture better statistical cyber risk and loss data, and create common classifications of cyber risk, alongside common cyberreporting standards."

iii. Collaboration between Insurance sector and Cybersecurity industry players

For CNI, support the development of collaboration between Cybersecurity European industry companies with Insurance companies to create new Cybersecurity Insurance for CNI, taking into account the level of cybersecurity implemented.

Include the role of insurance in providing insurance and risk management solutions to cyber risks: as experts on risk and risk management, the insurance industry has an important role to play in promoting new thinking and insights on cyber security. Such insights will help inspire action to control further cyber risks and thus increase the potential for investment in cyber technology going forward.

iv. Cybersecurity by design

"We welcome the secure by design approach: resilience and risk management should take place throughout product cycles rather than be built in retrospectively. Namely, if a product is not secure, it will be uninsurable and thus increase risks for both consumers and businesses."

v. Competitiveness and standardization / certification

The conflict between raising standards and maintaining global competitiveness is not addressed.

EU-wide common certification level is only possible if we can establish certification bodies which are independent from national interest of member states.

Public procurement services should consider SW/HW and Professional Services that have the EU labels as a priority

vi. Support R&D

We, as national level, are creating a catalogue for academic CS researches available to enterprises to temporal contract researchers/experts to further develop new products and services. The same apply for patents and proof of concepts.

VC or other Investments are needed (more seed than others, not mentioned). However, funding is not the only issue for startups. They need customers, get market share, be on procurement tools (i.e: Gartner) and probably that they have to be created as a standard company (sales, etc.). Merger acquisitions could help, but foreign companies and funds are fighting today. We have to speed up the process. Be careful, merger should not mean several people being fired.

vii. People / Talent Management

In terms of talent, we have to better:

- Identify and manage current talent
- Make real retention. In CS best talents are between 20-40 years old, >30 with high experience, are really deploying/creating high potential startups as they have real field experience and contacts. Salaries and being a good continent for experts
- We need to train teachers as never before; CS is high speed road. It is not an easy task
- Not only engineers, but an end to end skill is needed. Lawyers, experts in cybersecurity as well as other profiles (mainly in all sectors connecting with The Internet).

viii. European Cybersecurity Situation Centre & National Cybersecurity Situation Centre

We think the establishment of European Cybersecurity Situation Centre (ECSC), it is not presented in the right way. The document states that it should ¨give advice to all citizens and companies EU". We think this should be a competence of National Cybersecurity Situation Centers (NCSC).

The ECSC could have another role by delivering its services just to NCSCs:

- to give advice, training and to share best practices among NCCs
- to develop agreements of intelligence sharing with similar entities worldwide
- to alert NCCs on possible new threats or intelligence collected

- to be the last instance backup or escalation level for NCCs

"Collaboration model between EU CERT and country CERTs missing."

ix. Certification of Service Providers (IT and Cybersecurity professional services)

The document focuses on obligations by technology manufacturers for avoiding failures and vulnerabilities on their developments. However, some failures come from a weak implementation of these technologies (by misuse, lack of proper security training). We think it should be useful to rule the responsibility of organizations which are implementing and using these technologies.

For instance, a compulsory vulnerability analysis should be performed for some critical infrastructures or online services with a defined scope. For less critical installations, it could be possible to rule different categories of official certifications, issued by private consultants with the proper administrative authorisation. So, users can compete with having the highest level possible of security certification, showing its end-customers or business partners the level of safety/risk the interaction with them can have. This could work as is described for developers or service operators, with different EU labels for each category

x. SCADA cybersecurity

- Establish different types of cybersecurity audit in critical infrastructures to determine whether subsystems are vulnerable or not.
- Certification of professionals working in critical infrastructure cybersecurity in Industrial Control Systems / SCADA.
- Comparing cyber resilience between IT and OT to consolidate requirements.

xi. Digital Identity Management

All participants (persons and objects) being part of a communication needs to have a digital identity as a requirement for authentication. A certificate in combination with the digital identity can also be used to do end-to-end encryption for securing the data flow.

xii. Data Encryption

Effective data encryption relies heavily on PKI infrastructure services. The usage of PKI infrastructures from outside of the EU should be dealt with. It is known that foreign PKI service providers may be forced to break the security of their own product to allow state organisations to look into traffic which is encrypted by the service of these PKI providers. So the favoured usage of EU internal PKI infrastructure should be promoted and backed up by EU certifications or audits.

xiii. Labels

"Where labels have been used, compliance to the label requirement should be monitored and regularly checked" – This should not be an option if a label is used. Suggestion: "Where labels have been used, compliance to the label requirement must be monitored and regularly checked."


THALES
Atos
AIRBUS GROUP
BBVA
MINI
CYBERNETICA
ERICSSON
F-Secure
infineon