POSITION PAPER

Brussels, 20 November 2019

Building a real European Single Market for Cybersecurity: A call for a consistent approach – guiding principles

EXECUTIVE SUMMARY

Orgalim stands for a true European single market for cybersecurity and strongly opposes policies at EU and national levels that create fragmentation. Building a true single market for cybersecurity can only be done through a holistic approach with the New Legislative Framework at its heart and must be shaped together with industry and all relevant stakeholders. Our industries call on EU and national decision-makers to adhere to the following seven principles of "Good Cybersecurity Policy" that can serve as guidance to "make the single market fit for the digital age" as outlined by President-elect von der Leyen:

1. A European approach to cybersecurity: to ensure a harmonised framework at EU level with the aim of building a real single market for cybersecurity.
2. Consistent and coherent legal requirements: to avoid patchy, overlapping and inconsistent cybersecurity requirements in European legislation.
3. To that end, we need to set common cybersecurity goals to ensure horizontal consistency: applying to the products, solutions, and processes.
4. A risk-based approach further to the product's intended use: ensuring that technical requirements are set based on the context of use and level of risks.
5. Transparent and internationally recognised standards are key: to ensure that Europe's industry is competitive globally.
6. Build policies on existing industry measures: secure development processes are existing examples of good practice and must serve as the basis for any future cybersecurity policy.
7. Competitiveness depends on enforcement and effective market surveillance: to ensure fair competition in the EU single market.

Orgalim
BluePoint Brussels
Boulevard A Reyers 80
B1030 | Brussels | Belgium

+32 2 206 68 83
secretariat@orgalim.eu
www.orgalim.eu
VAT BE 0414 341 438

INTRODUCTION

Section 1: Shaping a single market for cybersecurity – our industries' vision

Cybersecurity as a competitive differentiator for Europe

Cybersecurity is an essential precondition for all connected products, solutions and processes - and crucial for the continued growth of Europe's economy and its society. As Europe's technology industries, we recognise its importance as well as the ambition shared by business, consumers and citizens to enhance the EU's cybersecurity capabilities.

Representing the largest industrial sector in the EU, Orgalim and its members consider cybersecurity to be a top priority, integrating measures accordingly in the development of our products, solutions and processes, and adopting security-by-design development processes. Providing an adequate level of cybersecurity is crucial for our industries' suppliers and end-consumers in Europe and beyond. We look forward to working with the new European institutions to further address the particular concerns and we outline with this paper the seven guiding principles as a roadmap to shaping together a coherent cybersecurity policy framework.

One of the new European Commission's core objectives is to build a real single market for cybersecurity. This is a goal shared by Orgalim and we are committed to contribute. Ensuring that Europe's technology industries are in a position to continue to innovate and circulate their products freely is a direct benefit of a functioning European market. A real single market for cybersecurity also aims to empower Europe's industry to develop new security solutions and to become a global reference point on cybersecurity. With this paper, Orgalim shares its vision on how best to achieve this objective, enabling Europe to fully unlock the use of cybersecurity as a competitive differentiatior.

A single market instead of multiple markets: a holistic approach with the New Legislative Framework at its heart.

For a true single market to come to fruition, the EU needs a holistic and forward-looking cybersecurity strategy to ensure that we avoid fragmented and diverging requirements, both at European and national levels. Orgalim is calling for a **harmonised, consistent and coherent cybersecurity policy framework** at all levels.

The New Legislative Framework (NLF) has been a success story for the single market for decades and remains the essential basis for manufacturers to place their products on the single market. However, our industries are concerned about indications that policymakers may pursue an approach that would destabilise the current framework by integrating inconsistent cybersecurity requirements in product legislation, becoming a catalyst for fragmentation and unnecessarily creating legal uncertainty for manufacturers. In particular, we are concerned that in parallel to work on the implementation of the Cybersecurity Act (CSA), the Commission is looking at including potential cybersecurity requirements in sectoral legislations under the NLF (such as the Radio Equipment Directive [RED], the Low Voltage Directive [LVD] and Machinery Directive [MD]). This vertical approach risks creating a patchwork of inconsistent requirements with regard to product legislation, thereby increasing the risk of double structures and grey zones.

A consistent approach at EU level for cybersecurity would actually contribute more to the objective of removing roadblocks for industry to placing cybersecure products on the single market. Our industries are convinced that a policy approach aimed at ensuring consistency and coherence for cybersecurity requirements across product legislation would be a better solution than compelling industry to implement multiple layers of cybersecurity requirements which could be especially burdensome to SMEs. It would help companies of all sizes, and especially small businesses, to make the best use of scarce resources[1] to address cybersecurity risks.

The adoption of the CSA must also be taken into account. Orgalim believes that it can be a useful framework to reduce the current, and potential future, fragmentation of cybersecurity certification in the EU and at national levels. At the same time, and jointly with stakeholders, policymakers and ENISA should also ensure that the certification framework does not overburden SMEs. This must be properly assessed when preparing and elaborating each scheme. To that end, Orgalim is looking forward to working with ENISA and the European Commission to contribute to the success of the EU-wide certification framework.

Additionally, when potentially revising NLF legislation, and taking into account the development of upcoming cybersecurity schemes within the scope of the Cybersecurity Act, policymakers should adhere to the spirit of the NLF for conformity assessment procedures. As the NLF enshrines a flexible approach to conformity assessment procedures, Orgalim also calls on policymakers to ensure that third-party certification and assessment do not become the default for cybersecurity.

Orgalim is concerned that various policy initiatives (e.g. at product level), while they may address valid cybersecurity concerns, could lead to fragmentation that would contradict the objective of raising cybersecurity capabilities. The flexible approach to conformity assessment procedures of the NLF should remain the default situation. In addition, successfully putting in place coherent and overarching cross-sectoral cybersecurity policies will enable Europe to become the global reference point on cybersecurity.

International compatibility and a level playing field are key

A holistic approach to cybersecurity policy also requires an international commitment as cyberattacks know no borders. Our industry is heavily export-oriented and integrated in global supply chains all over the world. Consequently, European and existing international standards must serve as the first reference point and be treated as an important cybersecurity principle. This is a key element for making the cybersecurity framework a success story for Europe.

[1] ISACA forecasts that by 2019 there will be a global shortage of two million cybersecurity experts worldwide. Across Europe, a shortage of 350.000 cybersecurity experts is expected by 2022.This outlook demands the efficient use of resources and necessitates consistent cybersecurity policies.

Moreover, the impact of European cybersecurity legislation affects businesses worldwide. It has considerable effects on their business practices and international value chains. A consistent and coherent approach to new cybersecurity requirements becomes even more crucial in this context. Policy approaches enshrining this enabling principle will provide industry with the necessary legal and regulatory certainty to invest in, innovate, and deploy state-of-the-art cybersecurity techniques for their connected products, solutions and processes.

In this context, it is crucial to ensure that European businesses are not disadvantaged vis-à-vis non-EU market actors that are placing their products on the single market. This level playing field can be guaranteed through effective and efficient market surveillance of products. To that end, sanctions aimed at dissuading market actors from disregarding market access rules significantly contribute to protecting consumers and businesses in Europe from cyberattacks.

Cyber threats know no borders and European policies must be internationally compatible. Orgalim calls on EU policymakers to take into account international developments and to shape policies that also build on its strong industrial base. The key element to ensure that our companies can remain competitive in innovating in European cybersecurity solutions is market enforcement. In this context its effectiveness must also be strengthened.

Europe's technology industries as part of the solution

It is Orgalim and its members' vision that a proactive, longer-term and strategic perspective on cybersecurity is the way forward for Europe to put in place a holistic cybersecurity strategy to truly raise the cybersecurity levels.

We are convinced that **Europe's industry needs to be part of the solution**. We can play our part by leading the way in advancing the uptake of cybersecurity development processes in global supply chains, for example by influencing international standardisation. At the same time policymakers need to ensure that cybersecurity policies are able to respond to the rapidly evolving market realities. These policies should be building on the industries' security know-how, especially in the development of industrial security and embedded security. This synergy between policymakers and industry will pave the way for Europe to set the world's highest standards in cybersecurity. At the same time, a strong governance structure involving all relevant stakeholders must be put in place. This is particularly relevant in the discussion around strategic value chains, both at EU and national levels, which could be a useful strategic leverage for Europe to further boost its cybersecurity capabilities.

To shape a real single market for cybersecurity this must be done jointly between policymakers and all relevant stakeholders. Our industries' contribution is a set of seven principles that should be seen by policymakers as both guidance and our benchmark for any upcoming cybersecurity initiatives.

Section 2: Key Principles of Good Cybersecurity Policy

This is our industries' call for the development of consistent and coherent cybersecurity policies in Europe. Every future initiative should be reflect the following **seven principles** in order to ensure a holistic approach to cybersecurity.

1. A EUROPEAN APPROACH TO CYBERSECURITY

Member States have already introduced national initiatives which, even if these are voluntary, contradict, hinder or otherwise interfere with the free circulation of goods and services. This is especially relevant with respect to national requirements, labels, testing and certification. As a consequence, companies are compelled to adapt the design of their connected products, solutions and processes. This will make the management of supply chains more difficult and hinder the free flow of goods and services, increase their production costs, and make them more expensive for the end-customer. To avoid this, Orgalim calls for a consistent approach to cybersecurity policies at the European level.

2. CONSISTENT AND COHERENT LEGAL REQUIREMENTS

All European legal requirements dealing with cybersecurity need to be elaborated in a consistent way especially when they address the same products, solutions or processes with the same intended use, including testing and evaluation procedures by notified bodies. Moreover, several legislative requirements have already been laid down or will be developed in the near future. Consistency is especially important for connected products, solutions and processes, even if they belong to separate product groups.

3. TO THAT END WE NEED TO SET COMMON CYBERSECURITY GOALS TO ENSURE HORIZONTAL CONSISTENCY

Common cybersecurity goals require consistency at EU level:

1) In order to achieve horizontal consistency, **we have to adhere to common cybersecurity goals** which are for example based on secure development processes – and a risk-based approach. This gives a direction for manufacturers to select the most adequate cybersecurity requirements for their product, solution or process. In addition, the manufacturer can add technical cybersecurity requirements.

2) A consistent approach to product legislation **shares horizontally the same principles but allows for specific solutions**. Complementary approaches – for areas such as health or the automotive industry - should be allowed with sectoral or product-specific standards, in so far as they do not create an inconsistent, patchy and overlapping set of requirements.
3) This must be **supported by European and international standards**, jointly developed by operators, ENISA, national authorities, consumer organisations, and the manufacturing industry.

This approach guarantees that every consumer and business can rely on a solid level of cybersecurity for the products, solutions, and processes that they use. Likewise, every product, solution, and process inherently contributes to a more cybersecure society and economy.

4. A RISK-BASED APPROACH FURTHER TO THE PRODUCT'S INTENDED USE

Cybersecurity is shaped by multiple factors, including:

- functions, capabilities, and robustness of a product or a solution,
- the cybersecurity threats that may affect a given operational environment, the products involved and their components,
- the ability of the manufacturer, operator and final user to detect and react to security events ,
- the level of awareness of the operator or user about the appropriate cybersecurity measures that could be taken,
- degree and number of interfaces, connectivity and integration into external platforms
- a multi-layered approach to network security through components embedding multiple levels of security measures.

Together, these factors form the cybersecure operational environment of a product, solution, or process. It follows that a product, solution, or process operating in different environments should meet different security requirements at all levels: functionality, capability, and process. The higher the risk, the higher the requirements have to be. This in turn is being addressed by the manufacturer through the intended use of the product or solution. A risk-based approach takes these two aspects (intended use and operational environment) into account and does not set fixed requirements for a product regardless of its use. Consequently, the approaches to cybersecurity are likely to differ in the consumer or in the industrial context.

5. TRANSPARENT AND INTERNATIONALLY RECOGNISED STANDARDS ARE KEY

As mentioned in the third principle above, it is the role of standards to provide the technical details that will help manufacturers to implement the most suitable technical solutions. These standards need to be developed in a process that is transparent, inclusive and democratic. They can be sector and even product specific, but need to be based on the same principles. Moreover, many international standards already exist. These have to be harmonised at EU level while remaining globally compatible - standards of the European Standardisation Organisations adhere to these principles and have to be the preferred choice.

The development of upcoming cybersecurity schemes in the framework of the Cybersecurity Act should first consider market-adopted international and European standards. For instance standards on cybersecurity development processes already exist and are relevant. For example;

- ISO/IEC 62443 on security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements,
- ISO/IEC 27034 –secure development life-cycle process for application.

Standards should be developed through the transparent and democratic participation of all stakeholders along the value-chain. Nevertheless, it also has to be acknowledged that the work on cybersecurity standards must be done efficiently to take into account the limited cybersecurity resources available globally.

6. BUILD POLICIES ON EXISTING INDUSTRY SECURITY MEASURES

Industrial players proactively perform cybersecurity vulnerability assessments and integrate cybersecurity solutions into their products, including in the development of products and after-sales plans. Establishing cybersecurity development processes (e.g. based on IEC 62443 on security for industrial automation and control systems - Part 4-1: secure product development lifecycle requirements) is the starting point. The broad use of such cybersecurity development process standards would increase cybersecurity in the long-term, in particular by stimulating innovation and spurring investments into cybersecurity solutions.
New mandatory measures should only be introduced further to thorough business impact assessments in line with the European Commission's commitment to better regulation.

7. COMPETITIVENESS DEPENDS ON A LEVEL PLAYING FIELD AND MARKET SURVEILLANCE

Every market actor active in the EU should apply European market access rules, regardless of whether their home base is within or outside Europe. Europe is capable of setting globally-relevant standards, however, without effective market surveillance and enforcement Europe cannot have a level playing field. This is crucial for the success of European businesses which are at risk of losing competitiveness at home. Enforcement has to be based on an effective and efficient market surveillance of products. Dissuasive sanctions will make public and private initiatives effective in protecting European companies and consumers from cyberattacks.

For more information, please contact:
Christoph Luykx, Director - Innovation and Digital Transformation
Christoph.luykx@orgalim.eu