# FACING UP TO CYBER THREATS – THE EU STRATEGY

12 October 2017

**Cyber threats are occuring more and more frequently with potentially devastating consequences. The EU is taking this issue very seriously addressing it with a new strategy aiming to increase cooperation among EU Member States and to reinforce the digital single market.**

**This snapshot will assess the impact of the EU's new Cybersecurity Strategy on companies and the challenges and opportunities it will create.**

*Alejandro Sanchez heads the Cyber-Security team at FTI Consulting in Brussels*

## Introduction

On 13th September, the European Commission (EC) published its new strategy to tackle the increased cyber threats by aligning the national governments, industry and civil society in a more unified European approach.

The EC highlights that cybercrime will cause 3 billion euros in damages by 2020. In addition, tens of billions of "Internet of Things" devices, such us smart phones, connected cars or smart door locks, are expected to be connected to the Internet by the end of this decade, but cybersecurity is not yet prioritised in their design.

In 2017 alone, the WannaCry ransomware attack affected more than 400,000 computers in over 150 countries, with the NHS or German state railways among those hardest hit; one month later, Petya ransomware attack hit Maersk, Saint-Gobain and WPP. In the case of Maersk the damage could amount to more than $300 million.

The approach set out in the EC's strategy aims at enhancing the EU's capabilities to deal with these threats. The ultimate objective is building greater resilience and strategic autonomy, boosting capabilities in terms of technology and skills. It also seeks to help building a strong single market, fostering the consumer's trust in emerging technologies.

# Creating a single cybersecurity market

### ENISA's enhanced mandate

The EC proposes strengthening the European Union Agency for Network and Information Security (ENISA). This proposal comes at a time when EU Members States are in the process of transposing the Directive on the Security of Network and Information Systems (the "NIS Directive") into the respective national legal orders by May 2018.

Today, operators of essential services (e.g. energy, finance, health, transport and internet infrastructure services) could face the risk of high compliance costs due to different interpretations of the NIS Directive from one Members State to the next.

The proposal to enhance ENISA's role in the NIS implementation phase could harmonise cybersecurity requirements across the EU, and thus decrease compliance costs for operators of essential services.

### A certification framework

ENISA will also support EU policy developments on information and communications technology (ICT) cybersecurity certification schemes, in an attempt to move towards a Single Cybersecurity Market.

The Certification framework aims to overcome the lack of cybersecurity certification schemes recognised across the EU to build higher standards of resilience into products, services and systems. The EC highlights the following benefits for business:

- Avoiding the need to go through several certification processes when trading across borders, thereby limiting administrative and financial costs.
- Making high standards for cybersecurity a source of competitive advantage.
- Building increased resilience for daily used ICT products and services ranging from medical devices, cars and airplanes to power plants and industrial control systems in factories.

That being said, Digital Europe, a key voice of the European tech industry has voiced its concerns warning of the potential negative consequences that an EU framework for cybersecurity certification could have. It defends the importance of having common international standards and certification, not regional frameworks that could hamper European competitiveness in the global market. Similarly, another prominent voice from the industry, BSA-The Software Alliance, has conveyed its scepticism about the proposed EU certification framework, arguing that any scheme must be flexible, consensus-based, industry-led and global in reach.

While at this stage, the proposal suggests that adherence to the certification scheme should be voluntary; industry should keep a close eye on the matter to prevent the adoption of mandatory regulatory obligations on cybersecurity products or service providers further in the legislative process.

> "I want high cybersecurity standards to become the new competitive advantage of our companies."
>
> *Marya Gabriel, Commissioner for the Digital Economy and Society*

### Security by design and duty of care principle

The certification schemes are aimed at creating a level playing field among ICT service providers by ensuring that all products would be built using state of the art secure development methods, integrating the "security by design" principle. This means products and services will undergo adequate security testing against common pre-established criteria before reaching the market. Ultimately, the aim is to foster a "duty of care" from the vendors committed to updating their software in the event of newly discovered vulnerabilities or threats.

A joint Commission-Industry body would be set up to develop the "duty of care" principle following a set of objectives and criteria including

- Creating an economy of "long term maintenance"
- Using secure development lifecycle processes and
- Developing criteria for disclosing updates and patches to address previously undiscovered vulnerabilities and fast update and repair.

This Joint-Initiative could be the opportunity for ICT vendors to set common vulnerability disclosure requirements across the EU (which can range from no disclosure to full real time disclosure; the middle ground being disclosure after the development of the necessary patch) to establish a level playing field amongst ICT security providers. This would be another step towards the development of a strong and competitive single market for cybersecurity products and services.

## Public-Private Cooperation against Cybercrime

One of the most important challenges the European cybersecurity space faces is the lack of information sharing on cyber vulnerabilities between private and public sectors. This is often due to the risks of compromising sensitive business information and the potential reputational damages when sharing information with public authorities.

In order to overcome this, the EC proposes to set up Information Sharing and Analysis Centres in Member States to facilitate information sharing with national private sector stakeholders. We are far from a dedicated European cybersecurity information sharing law, which is what the United States has with the CISA (Cybersecurity Information Sharing Act). However, this is a first attempt to enhance wider cooperation and information sharing among multiple critical infrastructure sectors in order to build trust between private and public stakeholders. The corporate governmental affairs functions are called to play an important role in this process.

In addition, the EC suggests creating a Cybersecurity Emergency Response Fund designed to assist with cyberattacks response and recovery, following the example of crisis mechanisms in other EU policy areas. The exact mandate and budget remain to be determined.
Different national law enforcement agencies and many players across a variety of national jurisdictions such as attorneys and judges, question the EU's effectiveness in mitigating cybercrime due to response fragmentation. Indeed, cybersecurity competences are still the remit of Member States. At the same time, European companies' daily operations and cybercriminals' activities are borderless. Cybercriminals actively exploit this loophole for their activities.

In this sense, the EC tries to address cybercrime by setting up and supporting the establishment of public-private partnerships and cooperation mechanisms, such as the Online Fraud Cyber Centre and Experts Network implementing information sharing model and standard in order to analyse and mitigate electronic crimes risks and online frauds.

Finally, the EC also aims to tackling cross boarder cybercrime by facilitating information sharing on cyber incidents by private undertakings with national law enforcements organisations and EUROPOL. One example of this current and incipient cooperation is the recent EU data protection reform (GDPR), which will enter into application in May 2018. This framework, provides a set of rules setting out the conditions under which law enforcement authorities and private entities can cooperate in the event of a data breach.

## Conclusions

The EC Communication provides an opportunity to enhance cybersecurity preparedness, response and recovery across the EU but also with third countries in an attempt to secure its increasingly digitalised society and thus the Digital Single Market.

It is clear, on the other hand, that the EC tries to put "ad maximum" the full cooperation of the Member States (and the different EU structures) and industry in order to maximise targeted measures that will further strengthen the EU's cybersecurity structures and capabilities.

This will increase opportunities not only for the cybersecurity and ICT industry, but also to all those companies which produce millions of devices connected to the internet and used by European consumers.

In addition, we applaud the role of ENISA in the NIS implementation process for operators of essential services, which clarifies reporting obligations of national authorities in case of serious incidents.

However, much remains to be done. The mere fact that security and cybersecurity competences remain at Member States level risks hampering the EC's efforts. Thus, without a mandatory legal framework, the EC can only call on Member States willingness to comply and act in the areas where they have the primary responsibility, such as the allocation of national resources for cybersecurity or the provision of cybersecurity-related training in the public and private sector.

Finally, the EC will have to deal with ICT Industry's concerns about having to comply with EU technical or even lighter process cybersecurity certificates. The risk could be that companies operating globally will face regional segmentation which would potentially induce high duplication costs. The role of industry in the certification process also needs to be clarified; this is barely mentioned in the proposal.

Alejandro Sanchez
+32 2 289 04 22
Alejandro.sanchez@fticonsulting.com

About FTI Consulting

EXPERTS WITH IMPACT™

FTI Consulting Inc. is a global business advisory firm dedicated to helping organisations protect and enhance enterprise value in an increasingly complex legal, regulatory and economic environment. FTI Consulting professionals, who are located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges in areas such as investigations, litigation, mergers and acquisitions, regulatory issues, reputation management and restructuring. The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting Inc., its management, its subsidiaries, its affiliates, or its other professionals, members or employees.

www.fticonsulting.com