The Digitalisation of Finance

Speech by ENISA's Executive Director, Prof. Dr. Udo Helmbrecht – Annual Conference on the Digitalisation of Finance organised by CEPS

BRUSSELS, BELGIUM
JUNE 2018

Ladies and gentlemen,

On behalf of ENISA, I would like to thank you for the opportunity to address you today.

In my intervention, I plan to discuss cybersecurity as an enabler for a more resilient Europe, and in particular the Finance sector as part of the operators of essential services. I will share our views on how new EU legislation and the proposed Cybersecurity Act support the efficient cyber incident reporting in the Finance sector and pave the way for a more open, secure and trustworthy information sharing. Information sharing is key component in preparing and preventing cyber incidents. I will also talk about the proposed blueprint and how it will help in case a major cross-border cyber incident occurs.

The finance industry has always been the prime target for attackers. Due to the ever-growing complexity of the industry, the interconnections of different players, and the introduction of the new fintech players further raises the risk of a major cyber-attack. A major cyber incident could potentially disrupt the financial sector and cause great damages to the sector and the society.

We need to be sure that the complex financial system will operate in a secure and safe manner.

We need to trust that the integrity of the transactions in the financial systems are done with a certain confidence level and in a fast way.

We need to build resilience into the system.

In September 2017, the European Commission presented the Joint Communication on resilience, deterrence and defence: Building strong cybersecurity for the EU: The new EU cybersecurity strategy. This Communication aims at building a strong digital single market through:

- an EU cybersecurity certification framework,
- a blueprint plan for operationalising cybersecurity response,
- strengthening ENISA's role and developing international cooperation for EU leadership on cybersecurity.

In the past, you needed a gun to rob a bank, today an equivalent amount of damage can be achieved from the action of a fingertip on a keyboard. This exercise can be performed from any place in the world. Crime, espionage, sabotage and even international conflicts move from the so-called real world into the virtual cyber world. On top of this, **criminals are getting money out of the financial systems through attacks on financial market infrastructures, like the well-known attack on SWIFT**.

We are not 100% secure and it is difficult to be so. The trust in the digital financial ecosystem is at risk now and even if experts expressed their concerns in the past, their opinions were not listened to. Today we need to do more.

The Banking and Financial Market infrastructures are identified as essential sectors in the NIS Directive, which EU Member States should consider when planning and implementing cyber security measures.

We recommend and strive to align policy requirements with the national cybersecurity strategy to avoid ambiguities relating to lines of responsibilities, duplication of structures and measures, and waste of resources. Some sectors are more cyber-mature than others.

Undoubtedly, the Finance sector is amongst the most mature sectors. We have to mention that we took note with enthusiasm on the advanced developments this sector has in terms or cyber security, both security measures and incident reporting.

A focused approach rather than a "cover everything" approach can provide several advantages. EU Member States can make fast progress by rolling out cyber security measures in sectors, which are already in an advantageous position, such **as the Finance sector**. These sectors can provide a positive example, when approaching stakeholders of other critical sectors at a later stage.

Harmonising cybersecurity certification approaches at European level can **increase the transparency of information on the security level of ICT products and services** in the digital single market for all its participants.

The proposed certification framework will provide **EU-wide certification schemes** as a comprehensive set of rules, technical requirements, standards and procedures. This will rely on agreement at EU level for the evaluation of the security properties of specific ICT-based products, services or even processes.

By undergoing a certification process, we will be able to **attest** that ICT products and services **meet specific cybersecurity requirements**. The resulting certificate will be recognized in all Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of products and services. Should these cybersecurity requirements are based on internationally accepted standards, the resulting certificate would also provide a certain level of assurance outside EU.

We believe that the financial sector across the EU will benefit from the provisions of the Cybersecurity act and the proposed certification framework in particular. Allow me to explain, and give you the following reasons:

First, the harmonised EU wide certification framework will inherently promote the cross-border flow and exchange of secure ICT products and services, based on the security by design paradigm. Financial institutions will be able to deal with a homogeneous system and thus require less resources in dealing with diverse compliance schemes.

Second, the level of consumer trust that will be brought by the new certification framework and the strong willingness of the EU to handle cybersecurity as a priority at a strategic level will boost the confidence of consumers in EU products. And this not only affects the EU internal market, but also the global one.

Another important provision of the Cybersecurity act involves the role of ENISA in supporting sectorial **Information Sharing and Analysis Centers (ISACs)** and **Public Private Partnerships (PPPs)**. The importance of involving both the public and the private sector and establishing trust relationships between industries and other stakeholders is evident.

The September 2017 Communication by the European Commission states: 'At European level, Sectoral Information Sharing and Analysis Centres (ISACs) **can play a key role in preparing for and responding to cyber incidents**. To ensure effective information flows on evolving threats and to facilitate the response to cyber incidents, ISACs should be encouraged to engage with all relevant bodies.'[1] How is this suggested cooperation even possible, when only several ISACs on EU level exist, or are still in development? Here ENISA's role becomes a necessity; a role that positions the agency in a central spot as a facilitator. **ENISA already positions itself as an expert or facilitator in the existing sectorial EU-level ISACs**. ENISA has already been involved with the creation of many ISACs, but one of the oldest ones is the EU Financial ISAC (FI-ISAC). Recently, in April 20187 the FI-ISAC celebrated its 10 years anniversary. The existing EU-ISAC Members welcome ENISA's participation because of its status as an independent expert (not a regulator), its overview of current developments within the sector on EU level, and its network.

We have been working on the topic and recently published two dedicated studies on cooperative models for ISACs and PPPs highlighting relevant challenges, but more importantly providing recommendations on the developments of such initiatives.

It is important that financial sector regulators and law enforcement align their objectives to protect at the best the proper functioning of the financial system, its reputation and stability.

We believe that, the coordination of financial sector regulators and law enforcement objectives is key, for instance, for the fight against money laundering. Being cryptocurrencies increasingly used to finance and conduct criminal activities, joint efforts and alignment of objectives are paramount to deal with these recent challenging criminal trends.

Policies and strategies are just preparing the ground; actual hands-on experience is sorely needed in this cyber hostile environment. In 2010 we organized the first Pan European exercise that brought 30 European countries against a common enemy that wanted to bring chaos in the Information systems in the EU. Since then a major exercise is organized every 2 years. Last exercise involved cross-sector players, but also companies from the financial sector. A fast and effective response relies on the cyber readiness and the swift information exchange between all key players. Cyber Europe is testing standard operating procedures on cross border information exchange focusing each time on a different crisis scenario, like for example targeting the energy sector or air transport. Experience from these drills resulted into the recently announced EU Blueprint[2] that **explains how cybersecurity is addressed in existing Crisis Management mechanisms** and sets objectives and modes for cooperation between MS.

I would like to take the opportunity to highlight the significance of the work on harmonising the different provisions of legislation in EU. The most recent involvement of ENISA was in the working groups of the European Banking Authority (EBA) and ECB on incident reporting – through the SecuRePay forum. The incident reporting guidelines involved the active contribution of ENISA.

Efficient and effective cross-border collaboration, harmonised mechanisms for incident reporting, EU-wide cooperation on strategic issues regarding cybersecurity, are some of the many benefits of the harmonized legislations.

[1] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16546
[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2017:450:FIN

As part of an EU-wide cybersecurity strategy and the Network and Information Security (NIS) Directive, the **collaboration across the EU has been sought as an important step in building resilient Europe.** For example, the NIS directive establishes an EU level Cooperation Group, to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence. Also it creates an EU level network of the national CSIRTs and CERT-EU, in order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation.

As a permanent member of the Cooperation Group and assurer of the CSIRTS Network secretariat, ENISA is involved on a constant basis on almost all activities undergoing now at EU level related to NIS Directive. The 3 working subgroups developed within the cooperation group - Identification of OES the group responsible for defining the guidelines to be used for the identification of the essential operators, minimum Security measures for OES the group responsible for defining guidelines on minimum security measures for essential operators and mandatory incident notification the group responsible for defining the incident notification guidelines (thresholds, parameters, process to follow etc.). These 3 working groups along with ENISA assures the collection and analysis of necessary data and drafting the final framework for the NIS directive implementation. As the **FINANCE&BANKING INDUSTRY** is one of the concerned sectors of the NISD, I am sure you have heard already about certain questionnaires, or have been asked to participate in some calls with our experts.

On another hand, the **CSIRTS Network level** as where ENISA is secretariat, is involved in the operational activities of the NIS directive. ENISA has a strong experience in dealing with CSIRTS as our experts have dedicated many years in developing the EU CSIRTS community. Even though the CSIRTS Network was just established work has already begun on topics like: Network cooperation, common taxonomies etc.

In conclusion, I would like to say the following: by being secure, we can be safer, we can be better.

I would like to summarize with some key messages that I would like you to take:

- Cyber-attacks are borderless.
- Costs of not improving cybersecurity can be very high, just look at Wannacry and NotPetya.
- For European businesses, good cybersecurity is a major opportunity, because European businesses have a reputation for high standards and high security.
- Especially with the uptake of new players in the Banking and Finance industry, cybersecurity will become even more important.
- Delivering technological innovation with the right cybersecurity will give Europe a competitive advantage.
- The NIS Directive aims at improving cybersecurity across the board and making sure there is an EU-wide infrastructure of collaboration and information exchange.
- The EU wide cybersecurity certification proposal aims at helping European businesses address /cybersecurity challenges and use cybersecurity as a competitive advantage.

Since ENISA was founded in 2004, we have been working closely with the European Commission, the Member States and industry to improve cybersecurity across Europe. We act as a **facilitator**. We support policy makers with setting cybersecurity policy both at national and at EU level. We also work closely with industry to help them address crosscutting challenges.

The Commission's proposal for a new and permanent mandate for ENISA, with more resources, is an important step for us. Once it is adopted, ENISA will be better equipped to help Europe address the growing challenges in cybersecurity.

Looking into the future, we see many new cybersecurity risks and many challenges. Especially with all these new technologies like Blockchain.

We definitely see that the stakes are rising.

But let us not forget that cybersecurity is also a business opportunity and a market differentiator for European companies.

Our job is to maximise the opportunities whilst keeping the risks under control. In this speech, I have outlined some actions that need to be undertaken in order to achieve this goal. As the EU Cybersecurity Agency, ENISA will support this process and will work together with policy makers and industry to make sure that cybersecurity is an enabler of, and not a barrier to economic progress.

Thank you for your attention.

ENISA

European Union Agency for Network
and Information Security
Vasilissis Sofias 1
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Vasilissis Sofias 1 Str, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu