INTESA SANPAOLO

# European Parliamentary Financial Services Forum

# Lunch debate on Cybersecurity

*Brussels, 19 June 2018*

1. *How will the entry into force of new EU legislation (eg GDPR, NIS Directive) affect the way the financial sector currently deals with cybersecurity issues?*

   The evolution of the EU regulatory Framework on cyber security has added a lot of complexity and has requested the Financial Institutions to review their processes and introduce new ones to be compliant. The business transformation that has been generated from this complexity has brought both benefits and new challenges to face.

   Among the most **important benefits** we can list:

   - **an increased attention of top management on Cyber security matters**: this new attitude led to assign a greater relevance to security processes, to consider the CISO as a strategic role in the organization and to became aware of the necessity to train and educate people on cyber security basic measures to adopt;
   - **the evolution of governance models**: cybersecurity is nowadays conceived as a corporate wide responsibility and it is no more restricted to the security of ICT systems and services;
   - **a clear need of collaboration and cooperation among financial institutions** and even with other stakeholders to find the best possible options to create common initiative towards an enhanced Cyber Resilience. Several initiatives grew in the recent years like ECSO[1] (European Cyber Security Organisation), a non-for-profit organization where also Intesa Sanpaolo (ISP) is involved and which represents the counterpart to the Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP).

   While, among the most **relevant challenges** we consider:

   - **new obligations:** legislations like PSD2, GDPR and NIS introduced the need for Financial Institutions to consider a wider set of stakeholders and their specific rights:
     - PSD2 introduces strict security requirements for the initiation and processing of electronic payments and the protection of consumers financial data;
     - GDPR requires new consent standard, new “privacy by design”, a more deep eye on big data and “profiling”, new individuals Data subject rights (e.g. data portability and the ‘right to be forgotten’, new rules for cross-border data sharing, new rule for data breach notification, and for data protection officer role);
     - NIS requires specific obligations in information security, risk management and incident reporting.

   - **the fragmentation generated by the process of transposition of European legislation into Member States laws**: this factor provided a considerable increase of the number of new prescriptions to be compliant, with specific measures to implement and different authorities to report. International firms, like ISP, has to consider the complexity to timely answer to all the requirements of national and international authorities, not leaving behind the need to be compliant with central authorities.

[1] Established in June 2016, involving a wide variety of private and public sectors institutions whose objective is to support all initiatives and projects aiming to develop, promote, encourage European Cyber Security.

- **lack of harmonization in incident reporting requirements:** we detect an urgent need to converge on an harmonized framework that takes into account the definition of a common data set & taxonomy to describe the same information for the different Authorities and a common template to be distributed to the appropriate stakeholders.

2. *What measures are financial players taking to protect themselves? Is further regulatory action needed to support this?*

Financial Institutions (FIs) must cope with existing regulations and directives. They shall **cooperate with other FIs** encompassing several Member States and even beyond EU. FIs need also be update with new technologies and tools to properly face new cyber-attacks techniques; and to protect Data and people rights. **Collaboration is the key word and this implies also active collaboration among public and private sectors** even with the creation of operative frameworks.

On these basis we have defined our measures to mitigate the cyber risk and regularly we assess the controls and verify their effectiveness. Since cybercrime became a cross border phenomenon with very worrisome growing rate affecting all industries, we believe that the **prevention should be a continuous activity not relegated to IT Security department** but should involve all levels of the organisation. To achieve the maturity level that will allow an adequate cultural awareness it is of utmost importance to educate all the people belonging to the organisation.

In this respect, **no further regulations are needed but it is necessary to have consolidated Best Practices** specifically addressing the measures to adopt for management of Cyber Security Processes that encompass Info sharing, Incident Reporting Management, Crisis Management, Supply Chain Management, Risk Management and Education&Training. ENISA may provide support in the consistent implementations of the recent regulatory evolution.

3. *What is the role of the financial sector in helping increase society's cyber-resilience? Is it a multi- sectorial approach needed?*

Financial services are key to the development of a Digital Society. They are not only a strategic enabler of digital services, but they can become a trusted party that supports the exchange of new types of "digital value". Think of sharing economy, IoT, crowdsourcing: as soon as these approaches become mature, there is an evolution of the exchange of value. **The financial sector should evolve to support the increasing needs of trusted parties in the digital space** considering not only specific needs of Financial sector, but having a multi-sectorial approach**.** A trusted, secure and proactive financial sector is a powerful accelerator for innovation and digital transformation. In order to achieve this goal, **it is crucial to have customers confident in the use of new technologies** since their information are controlled and safeguarded by the Financial Institutions and their providers.

**Trust and security should be guaranteed in a transparent and measurable way for each stage of product and service lifecycle**, and especially for **customer data usage**. It is essential to openly communicate what data is collected, how it is protected and who is accountable of the management. This is an area where smart regulation should enter the game.

Regarding the multi-sectorial approach, many companies belonging to different sectors are sharing the same challenges. Very often threats are cross-sector and cross border, leveraging infrastructures and services (including cloud). Multi-sectorial approach might help, in particular in the area of knowledge and capacity sharing that can boost the detection of threats and reinforce skills to put in place in case of undesired events.

4. *What future challenges do you expect in the area of cybersecurity in financial services?*

Describing the ISP journey in Cyber Security, I have already touched on what we consider the challenges of the financial sector. Let me summarize them:

1. **Evolution of the regulation**: we need a "smart regulation" approach that can help financial institutions to continue improving their cyber security posture and capabilities, introducing also new tools to address the most challenging areas (development of new capabilities, capacity, etc.)

2. **Skill shortage**: this is an issue across all EU member states, but in some countries this is worse than others. There are not enough experts with the right background. Whilst it is easier to find IT engineers with Cyber Security technical skills, experts with law/economy/management background are rare. There is also a tough and competitive market, so also retention is a challenge.

3. **Coordination with national and international bodies**: every financial institution has multiple bodies to report to. The situation becomes worse when the financial institution is global. Even at an EU level, managing interactions with multiple governments/regulators/institutions is a challenge. A better harmonization and coordination between all bodies would be a great added value, improving efficacy of communication/interactions, but also enabling a more efficient sharing of information and knowledge.

4. **Supporting real cooperation between financial institutions, regulators and government authorities:** right now the attention of regulation has been on incident disclosure. While this might be good for the institutions, it is not an incentive to share information. A legal framework to promote information and knowledge exchange should be considered: financial institutions need a "safe harbour" where they can share delicate information that might help to identify and fight new forms of attack.

5. **Adoption of new technologies**: it is of utmost importance in the operational area but also in the security. Among all, we can mention that artificial intelligence tools can be very effective to detect malware softwares or to carry out dynamic risk analysis while machine learning tools can be applied to prevent undesired events through the analysis of behaviours and trends of internal environment and cyber space. We also consider the block chain an important technology for the increase of trust in the digital workspace because it offers a totally different approach to storing information, making transactions, performing functions, and establishing trust, which makes it especially suitable for environments with high security requirements and mutually unknown actors.

Finally and in conclusion, I consider large scale cyber-attacks the most relevant cross sectorial challenge. To this concern, we believe that the Blue Print (*the Commission recommendation on coordinated response to large-scale cyber security incidents and crises*) is the first right step into this direction. We would like to focus the attention on this important document that should be implemented and on the crucial role the private sector should play in case a large scale cross border incident or crises related to cyber security occur.

In these unfortunate situations, **we would like that the private sector** (or at least, the sectors falling in the category of "operator of essential services" under the NIS directive) **will be actively involved in the operational scheme described in the Blue Print.**