Task Force

Cybersecurity in Finance: Getting the policy mix right!

Tuesday 06 February 2018 | Place du Congrès 1, 1000-Brussels

1. AGENDA FOR THE THIRD MEETING

12:30	Registration & Lunch
13:00	Opening & Welcome **Karel Lannoo,** *CEO, CEPS*
13:05	Opening remarks by the moderator and the Chairman of the Task Force **Sylvain Bouyon,** Head of Fintech and retail banking, CEPS **Richard Parlour,** Principal, Financial Markets Law International
13:20	The Cybersecurity Package and the latest progress on the implementation of the NIS Directive **Jakub Boratyński,** Head of Trust and Security, European Commission, DG Connect
13:50	Security and privacy **Rasmus Theede,** Managing Partner, DigitalNations
14:20	The role of analytics in cybersecurity **David Porter,** Associate Partner, IBM
14:50	Cyber incident reporting **European Central Bank**
15:20	Discussion on the topics covered during the second meeting
16:30	End of the Meeting

2. ACTION PLAN (AS A RESULT OF THE FIRST MEETING)

1. Definition of cybersecurity
   -Different types of cyber attacks (size, objective, methods, type of risk, etc)
   -Differentiation by segment: retail banking, insurance, capital markets, financial infrastructures
   -Some statistics to quantify these dynamics
   -Question of the insurance of cybersecurity risks: would government reinsurance schemes be adapted? The answer might depend on the systemic nature of the cybersecurity risk

2. Overlaps and synergies between rules and supervision related to cybersecurity
   -Analyses of the different overlaps and synergies between European pieces of legislation addressing cybersecurity risks: PSD2, GDPR, NIS, etc
   -Possible solutions to emphasise synergies and limit overlaps
   -Analyses of the possibility to have a single supervisory contact point for reporting obligations

3. An improved regulatory framework for reporting data breaches
   -Analyses of the main challenges and feasibility of implementing the data security content of the GDPR (in particular Article 32, Article 33, Article 34, Article 55 and Article 56(1))
   -Analyses of the way to define a risk threshold beyond which the financial provider has to notify consumers of breaches
   -Focus on specific ambiguous terms (undue delay, likelihood of risk to rights and freedom, etc)
   -Analysis of the possibility to require European states to log national cyber breaches and attacks into a central European database

4. A robust regulatory framework for clouds
   -Analyses of the expected impact and challenges of the Proposal for a Regulation aimed at removing obstacles to the free movement of non-personal data
   -Analyses of the need or not to remove prescriptive regulations on data location (GDPR, Art. 30) within the EU and with third countries

5. KYC processes: a framework that finds the right balance between security and the comfort of consumers
   -Segmentation of consumers by types of behaviour regarding the trade-off between convenience and security (risk-averse consumers versus risk-taking consumers): how should regulation adapt to these different types of consumers?
   -Analyses of possible rules to better monitor innovative processes of identification (static biometrics, behavioural biometrics, etc)