EUROPEAN CENTRAL BANK

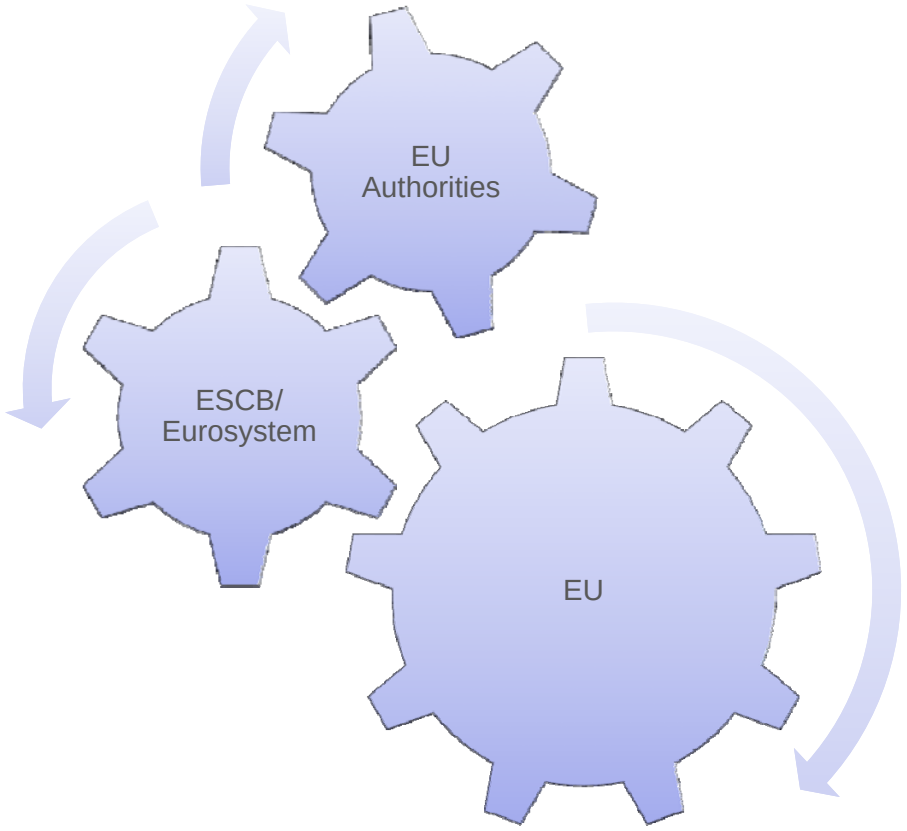
EUROSYSTEM

Helmut Wacket
Head of Oversight Division

Cybersecurity: regulatory framework and central bank initiatives in the EU

Cybersecurity in the EU

- Securing network and information systems in the EU is essential to ensure prosperity as well as safety, efficiency and trust in the online economy.
- The European Union tries to ensure cyber security in Europe from different angles:
  - European Commission
  - EU Authorities
  - Central banks



EU policy: Cybersecurity Strategy for the European Union

- Adopted by the EC in 2013
- outlines the EU's vision in this domain
- clarifies roles and responsibilities
- proposes specific activities at EU level
- addresses international cooperation as a key priority since cybersecurity is a global challenge

- **Objective:** to ensure strong and effective protection and promotion of citizens' rights so as to make the EU's online environment the safest in the world.

EU legislation: Directive on Network and Information Security (NIS)

- A regulatory initiative launched in 2013 by the EC
- contains legal measures and incentives aiming at making the EU's online environment secure
- Aims at strengthening preparedness, cross-border cooperation and information exchange
- builds on previous EU initiatives in this area
- Proposes steps to the system operators of critical infrastructures to manage security risks and report serious cyber incidents with significant impact to competent authorities

Cybersecurity: regulatory framework and central bank initiatives in the EU

- The ECB/Eurosystem supports the aim of the proposed NIS directive
- ECB issued a legal opinion on NIS
- Main observations:
  - the NIS directive should be without prejudice to the existing regime for the Eurosystem's oversight competence of payment and settlement systems (PSS).
  - Central banks/prudential supervisors are responsible for:
    - the assessment of FMIs' security arrangements in conjunction with other Operational Risk requirements
    - Developing oversight requirements regarding cyber security and resilience including risk management and security requirements
    - Receiving incident notifications from PSSs and payment service providers (PSPs) about cyber related issues.
  - PSSs and PSPs should not be subject to potentially conflicting requirements in this area imposed by national authorities (i.e. NIS)

Eurosystem/ESCB Activities

- Contributes and actively participates with other central banks / prudential supervisors and EU authorities in the establishment of harmonised policies and regulations in this particular field (e.g. guidelines, technical standards, oversight frameworks, etc.).
  a) SecurePay: European forum on the **secu**rity of **re**tail **pay**ments
     - Its aim is to facilitate a common knowledge and understanding with respect to the safety of electronic payment services and instruments
  b) CPMI report on Cyber Resilience in FMIs (2014)
  c) CPMI-IOSCO WG on Cyber Resilience (Est. 2014 – ongoing)

Eurosystem/ESCB Activities

- Elements of cyber risk have already been part of the Eurosystem oversight standards with respect to operational risk (information security, data integrity, authentication, non-repudiation, etc.)
  - SIPS Regulation – Article 15
  - Oversight Framework for retail payment systems - based on PFMI Principle 17 (applicable to PIRPS and ORPS)
  - SecuRe Pay Recommendations
- Existing standards will be complemented by CPMI-IOSCO guidance on cyber resilience once finalised and taken into account in respective assessments

Eurosystem/ESCB Activities

- 2014: Launched an evaluation of overseen FMIs as a follow-up to the CPMI report on Cyber Resilience
  - The objective is to evaluate the FMI approach to cyber resilience and especially towards the measures described in the report (i.e. scope, cyber governance, measures/control taken).
  - Initially the evaluation focuses on systemically important payment systems (SIPS)
  - Later, the scope will be extended to SSSs and CCPs and other relevant authorities will be involved
  - The evaluation will be based on the feedback overseers will receive from the SIPS on the basis of a questionnaire

The UK Approach - CBEST

What is CBEST?

- is a framework to deliver controlled, bespoke, intelligence-led cyber security tests.
- It aims at improving participating firms' understanding of cyber threats and allows crafting of appropriate and firm specific responses
- a solution that fills a gap, that the UK financial market was unable to fulfil itself (intelligence):
  - The inclusion of specific cyber threat intelligence will ensure that the tests replicate, as closely as possible, the evolving threat landscape and therefore will remain relevant for its participants.
- Establishes accreditation developed with CREST for key services supporting cyber defenses
  - To ensure that financial services and infrastructures providers have access to detailed and consistent cyber threat intelligence that has been ethically and legally sourced.

The process

- CBEST identifies vulnerabilities that can be exploited, and then seeks to exploit them using the tactics, techniques and procedures of threat actors known to have an interest in the target organisation
- looks for potential network entry points from the target organisation's website, social media, any information that is publicly available
- Test is scoped by Supervisors and firms/FMIs
- reports are the property of firms/FMIs AND the regulators
- results will follow a template and include the use of a common set of KPIs

Who

- The "core" of the UK financial system will be targeted (initially).
- This includes systemically important FMIs
- CBEST is a voluntary test supported by BoE, HM Treasury and FCA

Thank you!

For more information please visit:

EC's Cybersecurity strategy: http://ec.europa.eu/digital-agenda/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace

EC's proposed directive on NIS: http://ec.europa.eu/digital-agenda/en/news/commission-proposal-directive-concerning-measures-ensure-high-common-level-network-and

CPMI report on Cyber resilience in FMIs: http://www.bis.org/cpmi/publ/d122.pdf
CBEST: http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx
ECB legal opinion on NIS: https://www.ecb.europa.eu/ecb/legal/opinions/html/act_13357_amend.en.html
ECB Regulation on SIPS: https://www.ecb.europa.eu/ecb/legal/pdf/oj_jol_2014_217_r_0006_en_txt.pdf