What is the Eurosystem’s cyber resilience strategy?

Wiebe Ruttenberg
European Central Bank
Ensuring cyber resilience of FMIs in Europe: an urgent need

Cyber attackers penetrating the financial system…

… step by step approaching the core…
“FMIs should immediately take necessary steps (....) to improve their cyber resilience, taking into account this Guidance.”

CPMI-IOSCO Guidance on Cyber Resilience for FMIs (June 2016)
Eurosyste…cyber resilience strategy for FMIs March 2017

Cyber Resilience

FMI Resilience

Sector Resilience

Strategic Dialogue

CPMI-IOSCO Cyber Guidance

The strategy will be rolled out in the period 2017 - 2019 at Eurosystem and national level
Pillar 1: FMI Resilience

- Cyber survey for payment systems, CSDs and CCPs

- Governance
- Identification
- Protection
- Detection
- Response and recovery
- Testing
- Situational awareness
- Learning and evolving
Pillar 1: FMI Resilience

- Cyber Resilience Oversight Expectations (CROE): defining the three levels of an FMI’s cyber maturity

- **Evolving level**
  - All payment systems must meet the Evolving expectations, aspiring to move to Advancing level

- **Advancing level**
  - Evolving maturity level *Plus*
  - All SIPS must meet the Advancing expectations, aspiring to move to Innovating level

- **Innovating level**
  - Evolving level *Plus*
  - Advancing maturity level *Plus*
  - Ultimate level
Pillar 1: FMI Resilience

- **TIBER-EU**
  EU Threat Intelligence Based Ethical Red teaming

  Definition of ethical hacking/red-teaming
  Recommendations how to do it
  Guidelines how to hire ethical hackers
Pillar 2: Sector resilience

- UNITAS - market-wide exercise
  Scenario: cyber attack on financial infrastructures; loss of data integrity and knock-on effect

Observe reactions
Draw conclusions
Provide recommendations
Pillar 2: Sector resilience

- Info-sharing network
- Sector mapping
Pillar 3: Strategic regulator-industry engagement

- Euro Cyber Resilience Board for pan-European FMI

Who?
- pan-European FMIs
- critical service providers
- different European authorities

What?
non-technical discussion at Board level about cyber-related topics
Pillar 3: Strategic regulator-industry engagement

• Euro Cyber Resilience Board for pan-European FMI

Objectives:

• *foster trust and collaboration* among FMIs and between FMIs and authorities

• *catalyse joint initiatives* to enhance sector capabilities and capacities, to develop solutions and increase cyber awareness

• decisive, but not necessarily formally decision-making
The international perspective

**Cyber resilience** is a high priority in the international working groups. The ECB is actively involved in the different work streams:

- CPMI-IOSCO Cyber Working Group
- G7 Cyber Expert Group
- FSB Cyber Lexicon Working Group
- CPMI End-point Security

Policies, standards and initiatives from the international arena help inform the Eurosystem overseers and vice versa.
Cyber risk, cyber crime will not go away no matter what we do

Cyber resilience of the financial ecosystem is a joint effort of institutions, infrastructures and authorities, but …

… the responsibility to ensure cyber resilience is and stays with the respective financial institutions and financial market infrastructures
Questions
Useful links

CPMI-IOSCO “Guidance on cyber resilience for financial market infrastructures”
www.bis.org/press/p160629.htm
www.bis.org/cpmi/publ/d146.pdf

TIBER-EU Framework


Mandate ECRB

CPMI Report “Reducing the risk of wholesale payments fraud related to endpoint security”
www.bis.org/press/p180508.htm
www.bis.org/cpmi/publ/d178.pdf

G7 Fundamental Elements of Cyber security in the Financial Sector
https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en

ECB Cyber Resilience Oversight Expectations (CROE, public consultation document)

FSB Cyber Lexicon Consultative document