Eurosystem and International developments on Cyber Resilience
Cyber Resilience Strategy for FMIs

1. FMI Readiness
   - Overseers should work with FMIs to enhance their cyber posture to ensure their safety and soundness against an increasingly sophisticated threat landscape

   Tools:
   - Cyber survey,
   - European Red Team Testing Framework TIBER(EU)
   - Cyber Resilience Oversight Expectations

2. Sector Resilience
   - Enhance and mature the collective cyber resilience capability of the Eurosystem financial sector, through cross-border/cross-authority collaboration, information sharing and exercises

   Tools:
   - Market wide cyber exercises
   - Info-sharing network
   - Sector-mapping

3. Strategic Regulator-Industry engagement
   - Develop a joint strategic and Board level pan-European FMI Regulator-Industry forum to establish trust and collaboration amongst participants, to catalyse joint initiatives to enhance sector capabilities and capacities, and increase cyber awareness.

   Tools:
   - Establishment of the Euro Cyber Resilience Board for pan-European FMIs (ECRB)
TIBER-EU

- May 2018: Published the TIBER-EU framework
- Aug. 2018: Services Procurement Guidelines

Cyber Resilience Oversight Expectations for FMIs (CROE):

- Sets up a more detailed elaboration of the CPMI-IOSCO Cyber Guidance to aid FMIs and overseers in operationalising the Guidance
- Addressees: FMIs (mainly payment systems) operating in the Euro area and T2S
- Provides the basis for overseers to work with FMIs over longer term to raise the FMI’s cyber maturity level;
- Can be used as (a) Assessment Methodology for overseers; and (b) Tool for self-assessments for FMIs.
- FMIs are expected to continuously evolve on the cyber maturity scale;
UNITAS crisis communication exercise

• Facilitated discussion around a two-phased scenario that was a cyber-attack on financial infrastructures, resulting in loss of data integrity and a knock-on effect on other financial infrastructures

• Participants: pan-European financial infrastructures (payment systems, CSDs, CCPs) and Critical Service Providers

• Main objectives:
  ➢ raise awareness on data integrity issues
  ➢ discuss how impacted entities could work together during and after a cyber attack
  ➢ assess the need for external communication strategies
UNITAS crisis communication exercise

• Follow-up actions:
  ➢ Enhance the European crisis management arrangements;
  ➢ Explore how best to conduct a coordinated recovery and reconciliation process, with common market practices, processes, tools and communication protocols;
  ➢ Establish or update oversight MoUs or other forms of arrangements with other authorities;
  ➢ Establishing arrangements for sharing of imminent threats and threat intelligence; and
  ➢ Exploring best practices around training and awareness.
G7: Publications on Cyber Resilience for the financial sector

• Supports efforts to facilitate coordination across the financial sector and develop a G-7 view on effective practices for cyber resilience in the finance sector

• Oct. 2016: G-7 Fundamental Elements of Cybersecurity for the Financial Sector (‘G7FE’);

• Oct. 2017: G-7 Fundamental Elements of Effective Assessment of Cybersecurity in the Financial Sector (‘G7FE-Assessment’): provide entities with a set of outcomes demonstrating good cybersecurity practices, as well as high-level elements to use when assessing their level of cybersecurity.

• Oct. 2018: G-7 Fundamental Elements of Threat-Led Penetration Testing (‘G7FE-TLPT’): provide organizations with a guide to assess their resilience against cyber-incidents by using simulated events

• Oct. 2018: G-7 Fundamental Elements of Third Party Cyber Risk Management (‘G7FE-TPCRM’): provide best practices to manage cyber risks posed by third parties to both private and public entities in the financial sector;
International developments

Financial Stability Board (FSB)

• **Nov. 2018: FSB Lexicon** that would be useful to support work in the following areas.

  • *Cross-sector common understanding of relevant cyber security and cyber resilience terminology.*
  
  • *Work to assess and monitor financial stability risks of cyber risk scenarios.*
  
  • *Useful in efforts to enhance Information sharing.*
  
  • *Work by the FSB and/or SSBs to provide guidance related to cyber security and cyber resilience, including identifying effective practices.*
Links

Eurosystem’s Cyber Resilience Oversight Expectations (CROE, public consultation document)

Eurosystem’s TIBER-EU
Framework
Services Procurement Guidelines

G7 Cyber expert Group
Fundamental Elements of Cyber security in the Financial Sector
https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en
Fundamental Elements of Effective Assessment of Cybersecurity in the Financial Sector
http://www.mef.gov.it/in evidenza/documenti/PRA_BCV_4728453_v_1_G7_Fundamental.pdf
Fundamental Elements of Threat-Led Penetration Testing
G-7 Fundamental Elements for Threat-led Penetration Testing
Fundamental Elements of Third Party Cyber Risk Management
G-7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector

FSB Cyber Lexicon document

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