INTERNATIONAL CYBER-SECURITY INITIATIVES IN THE FINANCIAL SECTOR

International cooperation on financial sector cyber-security covers three crucial areas: establishing regulatory standards and requirements, developing practices and tools, and preparing risk analysis models for financial stability. It takes place in several venues, reflecting the various levels of sectoral and national competences. The main forum for market infrastructures and payment systems is the Bank for International Settlements (BIS) Committee on Payments and Market Infrastructures (CPMI); matters of supervision are dealt with by the Financial Stability Board (FSB) and the BIS Basel Committee for Banking Supervision (BCBS). The G7 also plays an important role and has published a set of non-prescriptive principles.[1]

The FSB is conducting a study of the regulatory systems and supervisory practices of 25 countries as well as the cyber-security guidelines issued by 10 international organizations.[2] It is also preparing a cyber lexicon, to be published by the end of 2018, which is expected to facilitate future regulatory efforts.

The G7 is drawing up a protocol for international cooperation among authorities to govern responses to cross-border incidents. It has set up a discussion panel with private sector representatives to decide on the best regulatory measures and on methods of exchanging information. One important development will be the creation of a technical frame of reference for a set of exercises to test the effective ability of public and private financial institutions to protect against, register and respond to cyber-attacks, along similar lines to the stress tests already carried out on the banking system.

At EU level, the European Systemic Risk Board (ESRB) ensures high-level liaison on financial stability between the European Commission, the appropriate European authorities,[3] the Eurosystem and the national macroprudential authorities. The European Cyber Risk Group has been set up within the ESRB to analyse the potential systemic impact of cyber-attacks, particularly in respect of the European economy.

In the field of banking supervision, the EBA has issued guidelines for the authorities on the assessment of IT risk and recommendations on the outsourcing of cloud computing services; it has also drawn up security requirements for payment service providers and harmonized supervisory rules. The observance of these requirements by significant banks is monitored within the Eurosystem by the Single Supervisory Mechanism (SSM), which also gathers reports of significant cyber incidents and has set up a specific task force (the Cyber Crisis Group) to handle incidents classified as major. The SSM initiates inspections

---

1 G7, *Fundamental elements of cybersecurity for the financial sector*, 2016; G7, *Fundamental elements for effective assessment of cybersecurity for the financial sector*, 2017.

2 FSB, *Stocktake of publicly released cybersecurity regulations, guidance and supervisory practices*, 2017.

3 European Banking Authority (EBA), European Securities and Markets Authority (ESMA), European Insurance and Occupational Pensions Authority (EIOPA).

to analyse cyber-risk in response to specific risk indicators based on incident reports or problems identified during off-site supervision.

Regarding payment systems and other financial market infrastructures, the CPMI-IOSCO working group on cyber resilience (WGCR) is currently monitoring the implementation of the Cyber Guidance issued by the CPMI-IOSCO in 2016[4] and disseminating it beyond the G20 countries. Furthermore, following several serious instances of cyber-fraud,[5] the CPMI has recently released a security strategy for reducing the risk of wholesale payments fraud related to endpoint security.[6] In 2017, the Governing Council approved the Eurosystem Oversight Cyber Resilience Strategy for European market and payment infrastructures to harmonize the implementation of the CPMI-IOSCO Cyber Guidance within the EU and to strengthen the readiness of individual financial institutions and their service providers to respond to cyber-attacks. It also promotes cooperation between the public and private sectors and has set up the European Cyber Resilience Board for that purpose.[7]

In 2017, the Bank of Italy set up the GCSC (Gruppo di coordinamento sulla sicurezza cibernetica – Cyber-Security Coordination Group), membership of which is also extended to IVASS (the Italian Insurance Supervisory Authority). The GCSC recently drew up a document detailing the action taken by the Bank and IVASS in the field of cyber-security and how it fits into the international, European and Italian context.[8]

---

4 CPMI-Iosco (International Organization of Securities Commissions), *Guidance on cyber resilience for financial market infrastructures*, 2016.

5 These include cases such as the fraud perpetrated against the Central Bank of Bangladesh in 2016; see BIS, *Central banks are reviewing wholesale payments security*, 2017.

6 CPMI report, 'Reducing the risk of wholesale payments fraud related to endpoint security', published on the BIS website on May 2018, https://www.bis.org/press/p180508.htm

7 Cyber Resilience Oversight Expectations (CROE) are now being drawn up, along with a plan for advanced cyber-security testing (EU Threat Intelligence Based Ethical Red Teaming, TIBER-EU); ECB, *Views on the regulation of cyber security*, 2017.

8 GCSC, *Documento quadro sul rischio cibernetico*, forthcoming.