Committee on Payments and
Market Infrastructures

BANK FOR INTERNATIONAL SETTLEMENTS

Press release

Press enquiries: +41 61 280 8188
press@bis.org
www.bis.org

Ref no: IOSCO/MR/17/2016

29 June 2016

CPMI-IOSCO release guidance on cyber resilience for financial market infrastructures

The Committee on Payments and Market Infrastructures (CPMI)[1] and the Board of the International Organization of Securities Commissions (IOSCO)[2] today released the final report *Guidance on cyber resilience for financial market infrastructures* ("Cyber Guidance").[3] This Cyber Guidance is the first internationally agreed guidance on cyber security for the financial industry. It has been developed against the backdrop of a rising number of cyber-attacks against the financial sector and in a context where attacks are becoming increasingly sophisticated.

"This is a landmark report for the financial industry. FMIs have come to the fore as financial sector hubs at a time when cyber resilience is a key priority for the financial industry. This is indeed a timely document, and FMIs should take action immediately to implement its recommendations," said Benoît Cœuré, Chairman of the CPMI.

The aim of the Cyber Guidance is to add momentum to the industry's ongoing efforts to enhance financial market infrastructures' (FMIs') ability to pre-empt cyber-attacks, respond rapidly and effectively to them, and achieve faster and safer target recovery objectives if the attacks succeed. Another goal is to ensure that these efforts to build resilience are similar from one country to another. Thus, the Cyber Guidance provides authorities with a set of internationally agreed guidelines to support consistent and effective oversight and supervision of FMIs in the area of cyber risk.

Ashley Alder, Chairman of IOSCO, said: "Implementation of the guidance represents an important step in strengthening the cyber resilience of FMIs and the ecosystem within which they operate."

The safe and efficient operation of FMIs is essential to maintaining and promoting financial stability and economic growth. If not properly managed, FMIs can be a source of financial shocks, such as liquidity dislocations and credit losses, or a major channel through which these shocks are transmitted across domestic and international financial markets. In this context, the level of cyber resilience, which contributes to an FMI's operational resilience, can be a decisive factor in the overall resilience of the financial system and the broader economy.

Key concepts built into the Cyber Guidance include the following:

- Sound cyber governance is key. Board and senior management attention is critical to a successful cyber resilience strategy.
- The ability to resume operations quickly and safely after a successful cyber attack is paramount.
- FMIs should make use of good-quality threat intelligence and rigorous testing.
- FMIs should aim to instil a culture of cyber risk awareness and demonstrate ongoing re-evaluation and improvement of their cyber resilience at every level within the organisation.
- Cyber resilience cannot be achieved by an FMI alone; it is a collective endeavour of the whole "ecosystem".

Notes

1. The CPMI promotes the safety and efficiency of payment, clearing, settlement and related arrangements, thereby supporting financial stability and the wider economy. The CPMI monitors and analyses developments in these arrangements, both within and across jurisdictions. It also serves as a forum for central bank cooperation in related oversight, policy and operational matters, including the provision of central bank services. The CPMI is a global standard setter in this area. The CPMI secretariat is hosted by the BIS. More information about the CPMI, and all its publications, can be found on the BIS website.

2. IOSCO is the leading international policy forum for securities regulators and is recognised as the global standard setter for securities regulation. The organisation's membership regulates more than 95% of the world's securities markets in more than 115 jurisdictions (http://www.iosco.org/).

3. The Cyber Guidance was prepared for the CPMI and IOSCO by a working group comprising representatives from CPMI central banks and IOSCO securities commissions. The working group is co-chaired by Coen Voormeulen (Netherlands Bank) and Hern Shin Ho (Monetary Authority of Singapore). The Cyber Guidance builds on previous studies conducted in this area by both the CPMI and IOSCO and is intended to be supplemental to the Principles on Financial Market Infrastructures (PFMI), primarily in the context of governance (Principle 2), the framework for the comprehensive management of risks (Principle 3), settlement finality (Principle 8), operational risk (Principle 17) and FMI links (Principle 20).