Committee on Payments and Market Infrastructures | BIS

IOSCO/MR/37/2022

29 November 2022

CPMI and IOSCO report on financial market infrastructures' cyber resilience finds reasonably high adoption of cyber guidance but highlights one serious issue of concern and four issues of concern

- The report finds reasonably high adoption of the *Guidance on cyber resilience for financial market infrastructures* ("Cyber Guidance") by FMIs.
- The report finds one serious issue of concern and four issues of concern. The serious issue of concern relates to a small number of FMIs not fully meeting expectations regarding the development of cyber response and recovery plans to meet the two-hour recovery time objective (2hRTO). The four additional issues of concern relate to shortcomings in established response and recovery plans to meet the 2hRTO under extreme cyber-attack scenarios; lack of cyber resilience testing after major system changes; lack of comprehensive scenario-based testing; and inadequate involvement of relevant stakeholders in testing.
- These findings highlight clear challenges for FMIs' cyber resilience that should be addressed with the highest priority.

The Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) today published an assessment showing reasonably high adoption of their Cyber Guidance by FMIs.

The report – *Implementation monitoring of the PFMI: Level 3 assessment on Financial Market Infrastructures' Cyber Resilience* – presents the results of an assessment of the state of cyber resilience (as of February 2021) at 37 FMIs from 29 jurisdictions that participated in this exercise in 2020–22. The Level 3 assessment covered all FMI types, ie, systemically important payment systems (PSs), central securities depositories (CSDs), securities settlement systems (SSSs), central counterparties (CCPs), and trade repositories (TRs).

The report finds one serious issue of concern and four issues of concern. The serious issue of concern relates to a small number of FMIs which have not yet developed their cyber response and recovery plans to meet the 2hRTO. That is, those plans were not designed to enable the FMI to ensure that critical IT systems can resume operations within two hours following disruptive events even in the case of extreme but plausible scenarios.

The report also highlights four issues of concern among some of the assessed FMIs:

- shortcomings in established response and recovery plans for meeting the 2hRTO under extreme cyber-attack scenarios;
- a lack of cyber resilience testing (eg integrity of backup data, vulnerability assessments or penetration testing) after a significant system change;
- a lack of comprehensive scenario-based testing;

- inadequate involvement of relevant stakeholders (eg FMI participants, critical service providers or linked FMIs) in testing of their responses.

Considering their aggregate impact, these (serious) issues of concern seem to pose clear challenges for FMIs' cyber resilience. The CPMI and IOSCO urge the relevant FMIs and their supervisors to address these issues with the highest priority. As set out in the PFMI, the relevant supervisory authorities are responsible for ensuring that individual FMIs implement the Principles.

The assessment focuses on the implementation of Principles 2 (Governance), 3 (Comprehensive framework for the management of risks) and 17 (Operational risk) and relevant Key Considerations of the PFMI.

To gain a better understanding of the extent to which the Cyber Guidance has been used by FMIs, this assessment also focuses on three important components of the cyber resilience framework: (i) governance, (ii) testing and (iii) learning and evolving.

As the survey of FMIs was carried out during the Covid-19 pandemic, a section of the report highlights the challenges recognised by FMIs in this period (eg due to increased remote working arrangements and the use of personal devices) and outlines some of the measures implemented or being implemented to address potentially heightened cyber risks.

MEDIA ENQUIRIES

Carlta Vitzthum	+ 34 91 787 0419
Outside office hours	+ 34 697 449 639
Email:	carlta@iosco.org
Website:	www.iosco.org
Follow IOSCO on	Twitter here