CPMI IOSCO Bericht „CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (Guidance)"

Results of Germany's Consultative Forums

The interview process in Germany covered two financial market infrastructures, as well as one stock exchange and two financial institutions as participants in these infrastructures.

Overarching

All consulted institutions agreed that the Guidance deals with exactly these topics which are relevant for cyber resilience and provides the requirements which are necessary to receive cyber resilience. However, the institutions criticized that the guidance is on a highly superficial level and that clearer and more detailed expactations might help to push the awareness for cyber resilience within the FMIs and within the whole ecosystem. In addition the institutions saw the need to better clarify the expectations of the guidance with regard to manufactures of IT products as these are strongly relevant for the cyber resilience of the ecosystem.

Institutions asked by when these requirements will be applied to FMIs.

Introduction

One institution mentioned that a more specified description of risk scenarios (which risks for FMIs, what does the regulator expect by when) would help.

Governance

One institution emphasized the importance of the CISO being independent from the IT department.

Identification

The concept of "critical business/processes/functions/assets" is seen as useful.

One institution mentioned that a more specified description of the ecosystem (especially in the "interconnections" part) would help. It should be noted that there are limitations to getting information related to cyber resilience from the ecosystem especially e.g. from ancillary industry such as Microsoft.

Protection

The requirement for having leading cyber resilience and information security practices to prevent, limit or contain the impact of a potential cyber event should not imply that FMIs are forced to go for the most modern technology due to those can have unknown bugs, i.e. can result in higher risks.

The concept of "resilience by design" is seen as useful as well as ambitious. This should be considered in the time frame of implementing the guideline.

The section 4.2.4. (Layered protection that facilitates response and recovery) indicates substantial modifications of current processes hence more details concerning time frame and others would be desirable.

The screening/background checks can only take place in the context of the respective legal environment.

The topic Training (4.5.) should be emphasized as the awareness of the employees is key for effective cyber resilience.

Detection

The detection of a cyber-attack is the pinnacle of cyber resilience.

One institution proposed to match chapter 8 (Situational Awareness) with chapter 5 (Detection) as these topics are closely related.

Response and recovery

One institution proposed to include restoration of damaged reputation in this chapter.

Depending on the attack a period of two hours as recovery time objective are very ambitious and there might be cases where these two hours are impossible to achieve. Furthermore, the interdependencies with other FMIs have an influence on the recovery of an FMI.

Within an FMI's disclosure policy related a cyber-attack the trade-off between the reputational risks for the single FMI and the protection of the ecosystem.

It was cautioned that a "golden copy" should not be seen as a panacea. One institution mentioned that the idea of maintaining an uncorrupted "golden copy" of critical data has limitations in the case of an APT.

Testing

The elements of this section are seen as important element of cyber resilience. However, it is unclear by when authorities expect these requirements to be applied as well whether a single institution can achieve it on its own.

It should be noted that there are legal constraints related to scenario-based testing.

It was also highlighted, that these kinds of tests are costly as well as bear risks to the functioning of an FMI.

Situational Awareness

Regarding Cyber Threat Intelligence, a well-functioning information network was considered to be crucial by all consulted institution. While contacts between (cross sectoral) market participants have already been established, setting up an international network with the participation of authorities and the responsible government agencies could be desirable.

Learning and evolving

The benchmarking in the field of cyber resilience is a new topic where sound guidance/solutions are not yet available. The existing competition among FMIs may also not allow for benchmarking.