February 23, 2016

CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures

Euroclear consultation response

As an important Financial Market Infrastructure subject to the PFMIs, Euroclear welcomes the opportunity to respond to this consultation on cyber resilience. We support the CPMI-IOSCO objective of bringing FMIs' cyber resilience to the highest standards.

Executive Summary

The consultation paper forms an excellent basis for improving cyber security, as it presents a clear framework and sound principles for the promotion of resilient market infrastructures globally. It uses a harmonised terminology and common supervisory expectations, supports a level playing field among market infrastructures and addresses complex technical issues in an easily accessible language. It thereby facilitates awareness outside the sphere of ICT professionals.

We believe that a few issues require further consideration by global regulators before the Guidance is published in final form:

- The notion of criticality and proportionality needs to be given more prominence in the Guidance, especially with regard to relationships between infrastructures and their service providers. This is essential to ensure that the Guidance can be implemented realistically. FMIs should be encouraged to adopt a holistic approach to cyber resilience and to involve stakeholders and all relevant players in their "ecosystem". Regulators should however, accept that CSDs will not always be in a position to impose their own cyber resilience standards to other entities, including third party providers, and that focusing resources on critical providers will be a more efficient way to enhance overall cyber resilience.
- In the area of response and recovery, we agree with the intent of the Design Elements presented in Section 6.3. We do believe however, that some of the proposed examples (such as the option to have parallel systems in place, and to have golden copies) may prove

technically and operationally unrealistic in practice, could impact processing efficiency or increase costs disproportionately. We propose therefore, that each FMI – together with its regulator – should assess design options depending on its system architecture, while respecting the intent of the Guidance.

- Global regulators should make it clear that the Cyber Guidance is not meant to be translated into binding legislation at local level and that, to be effective, it should remain principles-based and allow FMIs to adapt to the dynamic nature of cyber threats. This is especially true of benchmarks such as the 2-hour recovery time objective in case of a cyber-attack. We therefore regret that this objective is likely to be included in the Regulatory Technical Standards related to the EU CSD Regulation (Art 78 of the ESMA RTS proposed to the European Commission in September 2015[1]). Including such objective in law could even be detrimental to cyber resilience as it could lead an FMI to take actions to protect itself against potential sanctions for non-compliance with the law rather than focusing on solutions that limit market impact in case of a cyber-attack.

As a more general comment, while we agree that FMIs should apply the highest standards on cyber resilience, the increased costs and potential lower processing efficiency this brings for FMIs could result in some users being deterred from using FMIs. This could create incentives for market participants to perform activities outside FMIs or through new technologies which may offer post-trade solutions not subject to the Principles for Financial Market Infrastructures (PFMIs). We therefore, encourage the CPMI and IOSCO to seek an appropriate balance between the standards imposed on FMIs and on other financial market players, and to monitor closely the occurrence and growth of activity outside of the regulated FMIs.

1. Introduction

We agree with the CPMI and IOSCO that the proposed "Cyber Guidance" should be seen as a part of the PFMIs rather than as a separate set of standards. As a reference document, the Cyber Guidance can help CSDs and other FMIs in their efforts to comply with the PFMI (especially Principle 17 on operational risk) while promoting a common understanding among supervisors of what is expected of infrastructures in terms of cyber resilience.

As regards settlement finality, we agree with the CPMI and IOSCO that the *"settlement finality principle [should be] treated as a given"* (p.6) and that one of the primary aims of cyber resilience measures should be to preserve the finality of settlement instruments.

[1] Article 78(2) on disaster recovery of the ESMA draft regulatory technical standards on CSD requirements issued on 28 September 2015 states that *"the recovery time objective for each critical function can in no case be longer than two hours"* and that *"A CSD shall ensure that two hours from a disruption, it shall be capable of resuming its critical functions"*. (p. 71).

To be truly effective, the Cyber Guidance must remain principles-based and allow FMIs (and their regulators) to adapt to the dynamic nature of cyber threats. National authorities should not seek to turn the Cyber Guidance into binding legislation but should rather focus on effective supervision and benchmarking of FMIs. For example, the requirement for a CSD to resume critical operations within two hours of a disruption should remain a benchmark only. Achieving such a recovery time objective requires an appreciation of the depth of the disruption as well as other financial stability considerations, and cannot be mandated by law. Including such objective in law could even be detrimental to cyber resilience as it could lead the FMIs to take actions to protect itself against potential sanctions for non-compliance with law rather than focusing on solutions that limit market impact in case of a cyber-attack.

We therefore suggest adding the following sentence at the end of paragraph 1.3.6 on page 8: *"Authorities should however be aware that several elements of the Cyber Guidance constitute best practices and will often not be appropriate for inclusion in binding legislation."*

2. Governance

In section 2.2, we believe that more emphasis should be put on the close relationship between an FMI's cyber resilience framework and its information security framework, as mentioned in Principle 17 of the PFMI. Information security frameworks are usually based on ISO 2700x standards and cover areas such as the identification of information assets (mentioned in paragraph 3.2.). It is important that, when establishing their cyber resilience framework, FMIs can avoid unnecessary duplication with relevant processes related to information security management.

In 2.2.4, we recommend mentioning other examples to illustrate the need for consistency between the cyber resilience framework and the enterprise risk management (ERM) framework of FMIs. The last sentence of this paragraph could be redrafted to include measures restricting the ability to install rogue devices and policies to deal with extortion threats towards employees.

As regards the *"relevant metrics and maturity models"* that CSDs are encouraged to use in 2.2.8, we agree with the proposed wording and merely note that there are currently many metrics and models on offer in the market. We expect that some of these models may over time become industry standards.

As regards 2.3.3 of the Guidance, we agree with the requirement that *"the board and senior management (…) should contain members with the appropriate skills and knowledge to understand and manage the risks posed by cyber threats, while ensuring that those skills remain current"*. It is realistic however to assume that Board members do not always possess those skills at the time they are appointed. Training should be provided whenever necessary to ensure that Board members are skilled in assessing and understanding cyber risks. The appointment of independent consultants to

advise the Board of Directors of an FMI on cyber resilience can be a good practice to ensure that the skills of Board members remain current.

In 2.3.4, we assume that the appointment of one senior executive for the cyber resilience framework for a corporate group of FMIs (such as Euroclear group) would be deemed appropriate.

3. Identification

Section 3.2 (p.11) requires a CSD to list (1) critical business functions and (2) information assets by order of priority and to carry out risk assessments. CSDs may either wish to list critical business functions one by one, or to work with "priority classes" grouping several functions having the same level of criticality. Both possibilities should be allowed in the Guidance.

Section 3.3 states that a CSD should be able to identify the risks posed by (and to) other entities such as CSD *"participants, linked FMIs, settlement banks, liquidity providers, service providers, critical infrastructure such as energy and telecommunications, vendors and vendor products."* We agree that collaboration and information-sharing between CSDs, their participants and other stakeholders are fundamental to support cyber resilience efforts. Nonetheless, the term of "*service providers*" used in the Guidance is very broad and could encompass many entities, most of which will not pose cyber risks to CSDs. CSDs and other FMIs should thus be given a certain degree of discretion, in agreement with local regulators, as to which service providers are critical for cyber resilience purposes.

We would also like to point out that there could be practical and legal obstacles to the sharing of information on risks faced by individual entities. This is because some of the necessary information on individual systems and security measures may be of a sensitive nature, e.g. when shared with competitors. We wonder for example, whether individual market players will be willing to share the findings of their annual IT audits with other entities, and whether such findings can easily be centralised to be shared with relevant actors.

These limitations should nonetheless not prevent CSDs from assessing all potential sources of risk and from sharing cyber intelligence with relevant stakeholders. It is also important that regulators are aware of the constraints faced by market infrastructures when performing cyber risk assessments.

4. Protection

In Section 4 of the Guidance, we believe that the notion of "criticality" or "proportionality" is missing from the references to service providers. Given the complex interconnections in FMIs' ecosystems, an efficient cyber resilience framework must take into account the respective risks posed by

providers based on a criticality, risk-based assessment. We suggest redrafting Section 4 to reflect this principle more strongly.

For instance, 4.3.1 (p.13) states that *"At a minimum, an FMI should ensure that its service providers meet the same high level of cyber resilience they would need to meet if their services were provided by the FMI itself."* We believe that this will not always be realistic. Indeed, CSDs may not always be in a position to impose their own standards to third party providers (e.g. when a CSD is a small customer of a provider and does not have the market power to force the provider to amend its practices), and may have a limited choice of providers. In fact, the financial and technical implications of demanding an equally high level of cyber resilience from all providers could even have negative effects if this prevents CSDs from working with certain – otherwise reliable – providers due to excessive costs and complexity. The statement *"if their services were provided by the FMI itself"* seems to refer to those service providers to which an FMI outsources some of its operations and systems, not service providers such as telecom or electricity providers, but this is not entirely clear. We therefore recommend replacing the phrase *"At a minimum"* by *"Based on a risk assessment"* and replacing the phrase *"service providers"* by *"critical service providers to which FMIs outsource operations or systems"* in order to ensure a more realistic implementation.

The Guidance further states that *"contractual agreements between the FMI and its service providers should ensure that the FMI and relevant authorities are provided with or have full access to the information necessary to assess the cyber risk arising from the service provider."* We want to stress there may be cases where a given service provider may not be able to provide full and unrestricted access to certain information items in relation to the cyber risk arising due to legal or practical obstacles. In addition, the reference to *"full"* access will also need to be considered in light of the criticality of the service provider and of the required information. Some exceptions may therefore be required.

Furthermore, it should be possible for CSDs to rely on existing assessments of critical service providers (CSPs), such as independent assurance reports, to demonstrate compliance with the Guidance. This would avoid a multiplication of questionnaires between CSDs and their providers, make the process more efficient and reduce costs. Relying on such assessments should however not prevent CSDs from asking additional questions to their critical providers whenever required.

5. Detection

As regards the detection of cyber incidents, we welcome the recognition by the CPMI and IOSCO that FMIs may resort to different tools depending on their size and systemic importance. The establishment of a Securities Operations Centre (SOC) to monitor anomalous activities in real time, or near real time, will require a different level of financial and human resources depending on the scale a CSD's activities.

Likewise, the requirement under paragraph 5.2.2 that a CSD *"should seek to detect both publicly known vulnerabilities and vulnerabilities that are not yet publicly known, such as so-called zero-day exploits"* should be considered as an objective or best practice.

6. Response and recovery

Paragraph 6.2.2 states that *"an FMI should design and test its systems and processes to enable the safe resumption of critical operations within two hours of a disruption and to enable itself to complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios."* We support a general 2-hour recovery objective but stress that such objective should constitute a benchmark for CSDs, in line with Principle 17 of the PFMI.

As rightfully recognised by the CPMI and IOSCO, there may be situations where *"critical people, processes or systems may be unavailable for significant periods"* and where the 2-hour cannot be met. This is especially true of attacks on the integrity (rather than the availability) of FMI services. Regulators should ensure that CSDs and other FMIs have solid contingency plans in place to resume and recover operations in the most rapid and safest possible way, as suggested in paragraph 6.2.3.

Paragraph 6.3.1 states that "*the possibility to resume operations in a system that is technically different from the primary system may be one of the options taken into account*." We believe that if may not be technically feasible to foresee – for each system – a parallel system for use in case of cyberattack. Moreover, a sophisticated cyberattack may succeed in compromising the parallel platform as well. Furthermore, such an option would need to be maintained at a sufficient level of readiness as to be reliable and could therefore be very costly.

Paragraph 6.3.2 further states: "*As an example, FMI's systems and processes could be designed to maintain an uncorrupted "golden copy" of critical data (including to the extent possible, application source code)*" and "*In addition, the FMI's cyber resilience framework should include data recovery measures, such as keeping a copy of all received and processed data (including the original intent of instructions being sent to the FMI for processing), maintaining transaction replay capability."* Here also, it may not be realistic to have such arrangements in place for each system. For example,

- we are unclear on how to maintain a golden copy in a transactional system in which information is updated in real-time;
- CSDs may find such "replay" facilities particularly challenging to implement due to potential conflicts with finality rules (cf. the Settlement Finality Directive in EU markets), i.e. the fact that committed transactions are irrevocable.

We therefore propose that each FMI – together with its regulator - assesses design options depending on its system architecture, while respecting the intent of the Guidance. The Guidance should not mandate specific design options.

Finally, although the introduction of the Guidance includes a reference to the need for FMIs to understand the legal risks associated with cyber threats, we believe it may be useful to add a consideration of legal risks in Chapter 6 on response and recovery. Indeed, it is important that FMIs and their regulators understand the potential legal constraints under which FMIs may need to conduct response, recovery, or investigations. This includes ascertaining any liabilities a CSD may have towards clients, or other third parties.

With regard to Section 7 Testing, 8 Situational awareness and 9 Learning and evolving, we agree with the Guidance.

Glossary

We suggest adding a definition of "confidentiality" to complement the existing definitions of "availability" and "integrity". The NICCS Glossary defines confidentiality as "*a property that information is not disclosed to users, processes, or devices unless they have been authorised to access the information*" as well as the act of "*preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information*".

As for the definition of "cyber risk management" (p. 24), we suggest adding the phrase "or impact" after the word "likelihood" to be consistent with sections 2.2.2 and 4.2.1 of the Cyber Guidance.

For further information, please contact:

- Paul Symons, Head of Government Relations – Euroclear SA/NV +44 (0)20 7849 0034

- Ilse Peeters, Director, Public Affairs – Euroclear SA/NV +32 (0)2 326 2524