ECSDA
European Central Securities Depositories Association

23 February 2016

ECSDA comments on the Cyber Guidance for financial market infrastructures

On 24 November 2015, the CPMI and IOSCO issued a consultative report with proposed guidance for financial market infrastructures (FMIs). This paper constitutes ECSDA's response to the consultation, focusing on the perspective of European central securities depositories (CSDs).

Executive Summary

The "Cyber Guidance" issued by the CPMI and IOSCO provides useful principles for the promotion of resilient market infrastructures globally. European CSDs see the Guidance as a useful complement to the 2014 Principles for Financial Market Infrastructures (PFMI). Among the main benefits are the fact that it promotes a harmonised terminology and common supervisory expectations, it supports a level playing-field among market infrastructures, and it addresses complex technical issues in easily accessible language, thereby facilitating awareness-raising outside the sphere of ICT professionals.

Nonetheless, we believe that a few issues require further consideration by global regulators before the Guidance is published in final form. In particular:

- The Guidance should put **more emphasis on the principle of proportionality**, acknowledging that smaller infrastructures with a lower risk profile and lower systemic importance (e.g. because of a primarily domestic focus) cannot be expected to have the same level of detail and sophistication in their cyber resilience framework as large, cross-border infrastructures.

- Conversely, the Guidance should put **less emphasis on the formalisation and documentation of plans, policies and procedures.** CSDs generally agree with the description of the different components of the cyber resilience framework provided in the Guidance but believe that regulators should not systematically require separate formal documents for each of these components. In the case of smaller CSDs in particular, the various plans, policies and procedures could in some instances form part of the cyber resilience framework document to avoid introducing unnecessary paper work and complexity.

- **The notion of criticality should be introduced in those parts of the Guidance dealing with the relationships between infrastructures and their service providers.** This is essential to ensure that the Guidance can realistically be implemented. Market infrastructures should be encouraged to adopt a holistic approach to cyber resilience and to involve stakeholders and all relevant players in their "ecosystem". Nonetheless, regulators should be aware that CSDs will not always be in a position to impose their own cyber resilience standards to other entities, including third party providers. Focusing resources on critical providers will be a more efficient way to enhance overall cyber resilience.

- Global regulators should make it clear that **the Cyber Guidance is not meant to be translated into binding legislation at local level**. 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 objective in case of a cyber-attack.

These adjustments are necessary to avoid that the Guidance results in deterring the use of financial market infrastructures due to too high costs and complexity. Disproportionate costs to comply with the Guidance could create incentives for market participants to perform activities outside FMIs or through new technologies, such as distributed ledgers. We thus encourage the CPMI and IOSCO to seek an appropriate balance between the standards imposed on FMIs and on other financial market players.

1. Introduction

ECSDA agrees with the CPMI and IOSCO that the proposed "Cyber Guidance" should be seen as a part of the Principles for financial market infrastructures (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.

Taken together, the recommended measures contained in the Cyber guidance raise the bar considerably for some CSDs. Whereas some of these measures can legitimately be expected of all FMIs, other best practices such as the establishment of a Security Operations Centre or the maintenance of several separate plans, policies and procedures as part of the cyber resilience framework may not be practical or feasible for smaller CSDs. We thus suggest that the final Guidance should put **more emphasis on the principle of proportionality**, acknowledging that FMIs with a lower risk profile and lower systemic importance than, say, large FMIs with cross-border operations, cannot be expected to have the same level of detail and sophistication in their cyber resilience framework. Under Section 4.1 (p. 12), the report helpfully states that: *"These measures should be proportionate to and consistent with an FMI's risk tolerance, threat landscape and systemic role in the financial system."* ECSDA fully supports this statement but believes that it should be extended to the whole Guidance rather than limited to Chapter 4 on "Protection".

As regards **settlement finality**, ECSDA fully agrees 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 instructions.

To be truly effective, the Cyber Guidance must remain principles-based and allow FMIs to adapt to the dynamic nature of cyber threats. **National authorities should not seek to turn the Cyber Guidance into binding legislation**, as is sometimes done in the European Union, 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. Achieving such a recovery objective requires an appreciation of the depth of the disruption as well as other financial stability considerations, and cannot be mandated by law. ECSDA therefore suggests 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."*

Furthermore, in order to allow for a tailored implementation depending on the systemic relevance of the financial market infrastructures and the level of readiness of the local "ecosystem", the **timing** for implementing the Guideline should be decided jointly by infrastructures and their regulators in local markets. ECSDA thus welcomes the recognition in the Cyber guidance that *"FMIs may be at different levels of cyber resilience capability, and enhancing resilience could take time."*

2. Governance

ECSDA understands from Chapter 2 of the report that all CSDs are expected to maintain two separate documents: a cyber resilience strategy and a cyber resilience framework, both of which should be endorsed by the Board of Directors. ECSDA agrees with the distinction made in the Guidance between the strategy and the framework. However, we believe that it can make sense to combine both into a single document, with the cyber resilience strategy outlining the vision and the principles for addressing cyber risks, and the cyber resilience framework documenting how the CSD plans to effectively identify the risks, determine its cyber resilience objectives, its risk tolerance, and the methods of recovery. Making the strategy part of the framework and having a single document could be beneficial by facilitating consistency between both aspects, including in terms of the endorsement process by the CSDs' Board.

Moreover, ECSDA wonders whether it may be beneficial to put more emphasis, in section 2.2, 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 section 3.2). It is thus important that, when establishing their cyber resilience framework, FMIs seek to avoid unnecessary duplication with relevant processes related to information security management.

In paragraph 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 paragraph 2.2.8, ECSDA agrees with the proposed wording and merely remarks that there are currently many metrics and models on offer. We expect that some of these models may over time become industry standards.

As regards paragraph 2.3.3 (p. 10) of the Guidance, ECSDA agrees 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"*. We remark, however, that Board members may not always possess those skills at the time they are appointed and that trainings should be provided whenever necessary to ensure that Board members are skilled in assessing and understanding cyber risks. In some cases, the appointment of independent consultants to advise the Board of Directors of an FMI on cyber resilience can be a good way to ensure that the skills of Board members remain current.

Paragraph 2.3.4 (p. 10) of the Guidance requires CSDs to appoint a senior executive responsible for the cyber resilience framework of the company. This person should *"have sufficient authority, independence, resources and access to the board."* ECSDA agrees with this recommendation. The person responsible for the cyber resilience framework should possess adequate knowledge and relevant credentials to competently plan and execute the cyber resilience initiatives. As regards the notion of "independence", ECSDA believes that it should be assessed flexibly. Depending on the level of a CSD's resources and organisational capabilities, it should be possible to appoint a member of the staff (e.g. security officer) or an external service provider as *"executive responsible for the cyber resilience framework"*.

3. Identification

Section 3.2 (p. 11) requires a CSD to list (i) critical business functions and (ii) information assets by order of priority, and to carry out risk assessments. ECSDA understands that, in some cases, CSDs may wish to list critical business functions one by one, but that most CSDs are likely to work with "priority classes" grouping several functions having the same level of criticality.

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

ECSDA generally agrees with Chapter 4 of the Guidance but believes that the notion of criticality 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 assessment. We thus suggest redrafting Chapter 4 to reflect this principle more strongly.

For instance, paragraph 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."* Whereas ECSDA generally agrees with this statement, we believe that it may 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 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. ECSDA thus recommends 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."* Once more, ECSDA fully supports the spirit of the Guidance, but we wonder whether there may be some cases in practice 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 from their activities, whether 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 thus 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, ECSDA 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 of 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 a best practice. Smaller CSDs cannot realistically be expected to commit the resources necessary to detect zero-day exploits. Whereas some of the smaller infrastructures may be able to leverage on the cyber capabilities of other entities (e.g. an exchange) within their corporate group, this will not always be the case. CSDs should be encouraged to mutualise resources and to take part in joint ventures to enhance their cyber intelligence whenever possible, but regulators' expectations should reflect the specific constraints on resources faced by less systemic infrastructures.

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."* ECSDA agree that the 2-hour recovery objective should constitute a benchmark for CSDs globally, in line with Principle 17 of the PFMI. Nonetheless, local regulators should not seek to mandate this objective by law, as has been done in the European Union[1]. 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. Rather than seeking to make such situations illegal, 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.

In the case of the 11 September 2001 terrorist attacks in the United States for instance, some of the banks operating from New York's Twin Towers took between 36 and 48 hours to resume operations. We believe that CSDs will always do their best to resume operations as soon as possible. Although the 2-hour recovery objective contained in the PFMI is a helpful benchmark, regulators must recognise that exceptional crises may be of such scale that the benchmark cannot be met, irrespective of the cause (whether a cyber-attack or another event).

Paragraph 6.2.4 suggests that CSDs should maintain three separate plans: a response plan, a resumption plan, and a recovery plan, all of which should be regularly updated. Moreover, paragraph 6.4.4 states that CSDs should have a disclosure policy and procedure *"to enable the responsible disclosure of potential vulnerabilities following a risk-based approach".* Paragraph 6.4.5 further adds the need for "system logging policies" to facilitate forensic investigations. ECSDA supports the substance of these recommendations but believes that the plans, policies and procedures referred to in Chapter 6 as well as in other parts of the report should not be understood as systematically requiring separate formal documents. Indeed, and especially for smaller CSDs, the plans, policies and procedures could form part of the cyber resilience framework document, and the maintenance of separate documentation may only be required for the largest and most complex CSDs.

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*." ECSDA agrees with the wording of the guidance but remarks that such an option, even if technically feasible, will present its own risks. A sophisticated cyber-attack may succeed in compromising the alternative platform, potentially

[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)

rendering it unusable. Furthermore, such an option would need to be maintained at a sufficient level of readiness to be reliable.

Paragraph 6.3.2 further states: "*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.*" ECSDA agrees with the proposed wording but would like to highlight that CSDs may find such "replay" facilities particularly challenging to implement due to potential conflicts with finality rules, such as the Settlement Finality Directive in the EU, which make certain committed transactions irrevocable.

Finally, although the introduction of the Guidance includes a reference to the need for FMIs to understand the legal risks associated with cyber threats, ECSDA wonders whether it may be useful to add a consideration of legal risks in Chapter 6. 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.

7. Testing

ECSDA agrees with the Guidance on testing and expects that the frequency of tests will vary depending on the systemic importance of the CSD and on the expectations of the relevant regulators as regards the "*comprehensive testing programme*" to be established under paragraph 7.2.1.

8. Situational awareness

ECSDA does not have any comments on the Guidance as regards situational awareness.

9. Learning and evolving

ECSDA does not have any comments on the Guidance as regards "Learning and evolving".

10. Glossary

ECSDA finds the glossary on pages 23 to 26 very helpful. 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 paragraphs 2.2.2 and 4.2.1 of the Cyber Guidance.

About ECSDA

The European Central Securities Depositories Association (ECSDA) represents 41 central securities depositories (CSDs) across 37 European countries. As regulated financial market infrastructures, CSDs play a vital role in supporting safe and efficient securities transactions, whether domestic cross-border. If you have any questions on this paper, please contact Ms Soraya Belghazi, Secretary General, at info@ecsda.eu or +32 2 230 99 01.