23 February 2016

WFC Response to the CPMI-IOSCO consultative report on Cyber Guidance for financial market infrastructures

The World Forum of CSDs (WFC) welcomes the CPMI-IOSCO Consultative Report on "Cyber Guidance" for financial market infrastructures (FMIs) issued on 24 November 2015. The WFC is composed of the following five regional CSD associations which, together, represent more than 125 member CSDs:

- Asia-Pacific Central Securities Depository Group (ACG)
- Americas' Central Securities Depositories Association (ACSDA)
- Association of Eurasian Central Securities Depositories (AECSD)
- Africa & Middle East Depositories Association (AMEDA)
- European Central Securities Depositories Association (ECSDA)

Our response focuses on the CSD-relevant aspects of the Guidance. As a reference document, we are convinced that 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.

1. Introduction

The WFC sees that there are a number of aspects which make the Guidance attractive which include the promotion of a harmonised terminology, common supervisory expectations, and steps towards creating a level playing field among market infrastructures. Moreover, it addresses highly technical questions in a way that is clear and accessible. The WFC thus thinks that the Guidance can play a key role in raising awareness on cyber resilience among the FMI community, including outside of the world of ICT professionals.

Taken together, the recommended measures contained in the Cyber Guidance set the bar very high. 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 necessary for smaller CSDs. The Guidance, however, seems to treat smaller infrastructures largely in the same way as it does the more systemically important, cross-border ones. The WFC suggests 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."* The WFC fully supports this statement but believes it should be extended to the whole guidance rather than limited to Chapter 4 on "Protection".

Furthermore, to be truly effective, the Cyber Guidance must remain principles-based and allow FMIs to adapt to the dynamic nature of cyber threats across jurisdictions. National authorities should not seek to turn the specific requirements found in 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. Achieving such a recovery time objective requires an in-depth analysis and a real appreciation of the depth of the disruption in addition to other financial stability considerations. This is not appropriate to be mandated by law. To this end, the WFC 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."*

Finally, 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. The WFC 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

The WFC 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. The WFC 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.

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."* The WFC agrees with this statement but believes that the notion of "independence" should not be interpreted in an overly restrictive way. Indeed, CSDs may find it difficult to appoint a senior executive in charge of cyber resilience from outside the organization. Staff members (e.g. Chief Technology Officer or security officer) should, if the proper safeguards are in place, be considered as sufficiently independent. Conversely, a CSD may consider it worthwhile to appoint a senior executive who is not directly involved in IT operations or to appoint 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. The WFC 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.

Furthermore, CSDs may wish to classify information assets according to their vulnerabilities in addition to their 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 CSD *"participants, linked FMIs, settlement banks, liquidity providers, service providers, critical infrastructure such as energy and telecommunications, vendors and vendor products."* The WFC agrees that collaboration and information-sharing between CSDs, their participants and other stakeholders are fundamental to support cyber resilience efforts. We would like to point out, however, that there will sometimes be practical and legal obstacles to the sharing of information on risks faced by individual entities. In the United States for instance, privacy concerns have been raised in relation to the Cybersecurity Information Sharing Act (CISA) of 2015 which provides legal protection to

companies sharing information about cyber threats with public authorities on a voluntary basis[1]. This illustrates the difficult balance that needs to be maintained between information-sharing and the protection of personal data.

4. Protection

The WFC generally agrees with Section 4 of the Guidance but is of the opinion that the notion of "criticality" is lacking from the references to service providers. In considering the complex interconnections in the ecosystems of FMIs, an efficient cyber resilience framework must take into account the respective risks posed by providers based on a criticality assessment. We thus suggest redrafting Section 4 to reflect this principle more strongly.

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."* The WFC agrees that market infrastructures should take a holistic approach to cyber resilience and involve as many stakeholders in their ecosystem as possible. Nonetheless, regulators should be aware that CSDs will not always be in a position to impose their own cyber resilience standards to other entities, especially since FMIs' standards are particularly strict due to their role as central infrastructures. Directing FMIs' resources to critical providers will be a more efficient way to enhance overall cyber resilience.

The WFC thus suggests that "*At a minimum*" should be replaced by "*Based on a risk assessment*" and that "*critical*" should be added in front of "*service providers*".

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."* The WFC wonders 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. Some exceptions may thus be required.

Furthermore, if possible, a CSD should be able to rely on existing assessments of critical service providers (CSPs), such as independent assurance reports, to demonstrate compliance with the Guidance. Taking this step would not only avoid a multiplication of questionnaires between CSDs and their providers, but it would also make the process more efficient and reduce costs. Relying on such

[1] See for example Ryan W. Neal "On Cybersecurity, a Divide Between Wall Street and Silicon Valley", Wealthmanagement.com, 15 January 2016.

assessments should however not prevent CSDs from asking additional questions to their critical providers whenever required.

As regards Paragraph 4.4.2 (p. 13) on insider threats and employees, we agree with the proposed guidance and we remark that FMIs may have to foresee penalties and disciplinary actions for employees not in compliance with cyber policies.

5. Detection

As regards the detection of cyber incidents, the WFC welcomes the recognition by the CPMI and IOSCO that FMIs may seek to use different tools depending on their size and systemic importance. The establishment of a Securities Operations Centre (SOC) to monitor abnormal 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. CSDs, especially smaller ones, should have the possibility to outsource their SOC to a third party if appropriate.

Similarly, 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. Realistically, smaller CSDs cannot be expected to commit the resources necessary to detect zero-day exploits.

It may be possible for some of the smaller infrastructures to leverage on the cyber capabilities of other entities, such as an exchange within their corporate group. However, it is clear that this will not always be the case. The expectations of regulators should reflect the resource-related constraints faced by less systemic infrastructures. It would be preferable for CSDs to be encouraged to mutualise resources and to take part in joint ventures to enhance their cyber intelligence whenever possible.

6. Response and recovery

Paragraph 6.2.2 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."* The WFC agrees that the 2-hour recovery time objective (RTO) should constitute a benchmark for CSDs globally, in line with Principle 17 of the PFMI. As has been 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 RTO cannot be met. This is especially important with

respect to the integrity[2], rather than the availability of FMI services. Rather than seeking to make such situations illegal by codifying them in law, regulators should focus on ensuring 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. The WFC believes that CSDs will always do their best to resume operations as soon as possible. Although the 2-hour RTO is a helpful benchmark, regulators must recognise that exceptional crises may be of such scale that that 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. Furthermore, 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".* Additionally, Paragraph 6.4.5 further imposes the need for "*system logging policies*" to facilitate forensic investigations.

The WFC supports the substance of the recommendations under Chapter 6, but we believe that the plans, policies and procedures referred to in this section as well as in other parts of the report should not necessarily constitute the requirement of separate formal documents. 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.

As a general remark, FMIs may consider it worthwhile to subscribe to insurance contracts specifically aimed at mitigating the effects of a cyber-attack as part of their overall approach to incident response, resumption and recovery.

7. Testing

The WFC agrees with the drafting of point (c) of Paragraph 7.2.2 on penetration tests. We remark that, in some instances, internal tests performed by FMIs may fail to address some security issues and that the performance of penetration tests by specialized external companies may be required.

[2] Attacks on the integrity of FMI data (cf. cyber extortion) can have even more damaging consequences on the market than attacks on the availability of FMI services.

8. Situational awareness

No comments.

9. Learning and evolving

No comments.

10. Glossary

No comments.

About the WFC

On April 15, 2011, at the closing of the CSD11 conference in Cape Town, South Africa, the five regional CSD associations announced the formation of the World Forum of CSDs (WFC) in order to further enhance inter-association communications. The WFC provides a forum for regional CSD associations to exchange information, discuss issues of common interest and increase their influence and engagement on cross-regional and global developments.

The Forum has a Board composed of 10 members, namely the Chairs and Vice-Chairs of each of the five regional associations. Mr Jorge Hernán Jaramillo of Deceval (Columbia) is currently acting as WFC Chairman, with Mr Eddie Astanin of NSD (Russia) as Vice-Chairman.

For further information, please contact: Tanya Knowles (Strate), WFC Secretary, at tanyak@strate.co.za or your regional contact person
For ACG: Shariq Naseem, ACG Secretariat: shariq_naseem@cdcpak.com
For ACSDA: Bruce Butterill, ACSDA Executive Director: bbutterill@acsda.org
For AECSD: AECSD Secretariat (NSD): aecsd@aecsd.com
For AMEDA: Riham G. Khedr (MDCR): riham.g@mcsd.com.eg
For ECSDA: Soraya Belghazi, Secretary General: info@ecsda.eu