WFE Response to the CPMI-IOSCO Consultative Paper:

Guidance on Cyber Resilience for Financial Market Infrastructures

February 2016

Introduction

The World Federation of Exchanges (WFE) is the global trade association that represents 64 publicly regulated stock, futures and options exchanges, including the more than 100 Central Counterparties (CCPs) and Central Securities Depositories (CSDs) operated by them. Our members also include standalone CCPs that are not owned or operated by an exchange group[1].

Our members are both local and global, operating the full continuum of Financial Market Infrastructure (FMI) in both developed and emerging markets. Of our members, 36 percent are in the Asia-Pacific region, 42 percent in EMEA and 22 percent in the Americas. The market capitalisation of entities listed on our member exchanges is $68.5 trillion, and around $26 trillion in trading annually passes through the infrastructures our members safeguard[2].

The WFE works with standard setters, policy makers, regulators, and government organizations to support and promote the development of fair, transparent, stable and efficient markets around the world.

Cyber security matters have been - and continue to be - a matter of great priority for our membership, and one in which significant time, effort and money has been invested. We therefore welcome the opportunity to offer our perspectives and further contribute to the debate in order to secure the shared objectives of fair and orderly markets that promote the safety and resilience of the global financial system.

Summary

As CPMI and IOSCO point out, FMIs play a critical role in promoting the stability of the financial system; therefore the cyber risks faced by them, and their level of preparedness to react, have been prioritised by regulatory authorities. FMIs too have prioritised this issue and support – in particular – the need for a coordinated approach given the interconnectedness of the system.

Global markets require global standards and therefore it is right and appropriate that international bodies such as CPMI and IOSCO lead the regulatory effort. We applaud CPMI-IOSCO's efforts on this important issue and the regular meetings they hold to discuss the views of stakeholders and engage a broad spectrum of the financial markets.

However, the FMI community also acknowledges the importance of industry-led initiatives and solutions, and as such has been proactively sharing experiences, cooperating and collaborating through industry groups such as WFE's Global Exchange (GLEX) Cyber Security Working Group, which contains senior information security representatives from 24 of our member exchange groups.

Below we therefore offer our perspectives on the CPMI-IOSCO consultative paper and the key areas of focus within, and offer suggestions as to next steps and implementation.

---

[1] The WFE membership list can be found here

[2] As at end 2015

WORLD FEDERATION OF EXCHANGES

Section 2: Governance

FMIs globally share the views of CPMI-IOSCO on the importance placed upon having effective arrangements in place to establish, implement and review their approach to managing cyber risk. Also the need to have documented and measurable strategies, frameworks and risk mechanisms in place, backed up by clear lines of responsibility/accountability and cultural buy-in throughout the organisation. In particular, we would note the following:

- **2.2. Strategy and Framework**: The WFE agrees that strategy is a critical area of focus for FMI cyber security. However, spelling out "strategy" and "framework" as specific and separate products risks being overly prescriptive, potentially promoting a "tick-box" mentality. The different scales, business focuses and cultures within each FMI needs to be recognised, and flexibility afforded to allow individual institutions to meet these needs via different documentation methods. For example, some FMIs will have a single "Strategy" document that captures everything intended in a strategy and framework. Others will have interlinked procedural documents that incorporate many framework elements while moving strategic elements to mission and vision statements. Still others will have direct Board engagement in developing tactical policies. Whilst we applaud the positive intentions of this guidance, we consider they can be better met by noting that ***a high-level strategy should be developed, documented, and informed, and that policies and procedures established to execute that strategy should be documented and maintained***. Further, it is recommended that any mentions of a "strategy" or "framework" be consolidated into the single term "Strategy".

- **2.3. Role of the Board and Senior Management:** In an increasingly electronic world, operational resilience – and within that cyber resilience – has naturally become a key area of focus and risk for exchange and CCP Boards and Chief Executives, many of whom speak publicly of the risks and their concerns around the issues. Chief Information Security Officers (CISOs) are regularly and as a matter of course asked to brief their Boards on recent developments and of the level of preparedness at the individual firm level. This has now become part of the "business as usual" within individual institutions.

- **General:** Further, in an acknowledgement of the importance of "connecting-the-dots", we note the wider industry desire and initiatives to share knowledge and best practice within the broader community. At the WFE, for example, there are up to three annual reports from the GLEX to the wider WFE membership – underlining the FMI industry's awareness and desire for education. Similarly, WFE's November 2015 bi-annual Exchange Technology workshop - organized in conjunction with the Massachusetts Institute of Technology (MIT) – drew representatives from 55 member exchanges, many of whom were either CTO or CISO, to a 90-minute strategy & learning session led by CISOs of three systemically important FMIs.

WORLD FEDERATION OF EXCHANGES

Section 3: Identification

The industry agrees that identification is a key component of cyber preparedness, resilience and recovery. WFE members regularly review, identify and update processes and business functions to ensure they are aware of, and are tackling, any new risks in addition to monitoring existing ones. In particular, we would note the following:

- **3.2. Identification and Classification:** The WFE notes that "Situational Awareness" and "Threat Intelligence" – as described in section 8 - may be better considered in the Identification phase of security programme management. In addition to merging content and more tightly-aligning with the US National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) by eliminating the need for a separate Situational Awareness section, this also shifts the focus of the identification process from the "*keys to the castle*" approach of asset discovery and classification to the "*what are they after?*" approach of identifying threat actors and potential vectors of attack. This is particularly important for FMI, as much of today's industry guidance around cyber security is informed by events in the retail space (e.g. theft and exfiltration of personal and payment card data). While other industries are right to focus identification efforts on assets, FMIs should have a different and specific focus on availability and avoiding tamper or disruption. For FMIs, this threat is much more relevant and the choice of specific asset to target is less important than disrupting any of many interconnected links that would result in outage or instability. To that end, ***identification efforts should be focused on identifying threat actors and categories, tools, and methods so defences may be properly positioned and tested*.** Under this approach governance and risk assessment fit well into the Identification section as well.

- **3.3. Interconnections:** WFE members agree on the importance of considering the risks presented by the wider ecosystem, and consequently WFE's GLEX Cyber Group regularly discusses industry risks with each other at the CISO level, and participates in industry-wide testing events. However, we caution that, given FMIs operate in an ecosystem with multiple other (FMI, and non-FMI) actors, there is a finite amount any single organization can achieve outside its own system. We therefore ***support efforts by, and encourage, regulators to foster cooperation and support coordination by ensuring there are common standards*** as technology is deemed a key differentiator for most FMIs.

Section 4: Protection

FMIs agree with the need for strong and robust controls that are proportionate to, and consistent with, the FMI's risk appetite and role in the system. Sitting as they do at the junction of finance and the real economy, FMIs are aware of their systemic significance and as such invest time, resource and management attention on protection measures including security controls and systems and processes. These processes continue to evolve along with the development of the markets. Indeed, in a joint IOSCO-WFE member survey, 89 percent of respondents said cyber-crime can be considered a potential systemic risk, demonstrating the heightened need for protection; as such, within WFE GLEX members, the majority of the annual cyber budget is spent on protection measures.

However, we caution that not all FMIs are at the same stage of development and so risk tolerance, threat landscape and systemic roles vary from market to market. For example, WFE GLEX members range in size from the Colombo Stock Exchange to Intercontinental Exchange (ICE), illustrating the diversity of protection needs and efforts. As such ***we advocate that regulators, whilst rightly fostering a focus on protection, should remain sensitive to the fact that being overly prescriptive, or offering a one size fits all approach, will not likely be successful***. In particular, we would note the following:

- **Section 4.2.3. Strong ICT controls:** We agree that this section should not attempt to be prescriptive or comprehensive. However, we consider the four examples chosen – which helps to focus and prioritise - can be improved upon. In particular, it is our view that FMI and regulatory examination should focus on more than just encryption, patch management and system hardening. All are important where appropriate, and other ICT controls that are generally also important for FMIs include:

    - ***Access Control***: Documented, repeatable, and audited processes should be in place governing the process, from requesting through granting and recertifying access to sensitive systems or data;
    - ***Intrusion Detection and Visibility***: Networks that are used for critical functions - and thus likely to be employed in attacks - should have appropriate instrumentation and be monitored for suspicious activity and abuse;
    - ***Internet Egress***: Discretionary content filtering should be in place to dynamically identify malicious web sites and block access from employee and datacentre systems;
    - ***Web Application Security***: Where Internet-based connectivity to internal systems is present, network-based systems independent from web servers should have visibility into traffic and the ability to identify and block malicious activity;
    - ***Network Segmentation***: A default-deny philosophy should be enacted via the use of firewalls and access control devices that prohibit unnecessary communication among systems; and
    - ***Remote Access***: Internet-based remote access for employees should require multi-factor authentication to nullify the value of credential capture.

- **Section 4.3. Interconnections**: As previously indicated in our comments to section 3.3 above, whilst we note the interconnectedness risk and support a framework that seeks to build in protections from external third-party risks, it would be unreasonable to expect an individual FMI to be able to wholly ensure their service providers meet the same level of cyber resilience as the FMI itself. S4.3 operates under the premise that service providers have elevated, if not unfettered, access to sensitive systems and as a result tasks FMI with ensuring the security of providers reaches the same level of control as the internal programme. A more realistic approach to vendor and partner risk would be to segment and minimise access outright and monitor the relatively small residual vectors of access closely. ***Focus should be on mitigating controls, including where appropriate treating external connections similarly to Internet-based connectivity, terminating them outside the network perimeter, only allowing specific required and approved protocols and sources, and monitoring the resulting traffic with behavioural analytic tools***.

- **Section 4.4.1. Security analytics:** Analytics - particularly behavioural - are rightly emphasised here. The practical "Insider threats" in the context of this guidance are those that result in destruction or destabilisation. As such, we consider that ***s4.4.1 would be better served by focusing on behavioural monitoring, determining baseline activity patterns with regard to systems and data accessed, and alerting any deviation from those patterns***.

Section 5: Detection

Detection remains a key frontier for FMIs in the battle to contain cyber threats. WFE acknowledges the need for strong controls and standards, and further supports CPMI-IOSCO's perspective that these controls and standards should be proportionate and consistent to the FMI's relative size, systemic importance, risk tolerance and specific needs.

Section 6: Response & Recovery

FMIs acknowledge the responsibilities related to their role in supporting financial stability - including their ability to settle obligations when they are due. The focus of all FMIs' response and recovery strategy is to ensure that critical systems resume to full operation as soon as is possible and without further compromising the orderliness of the market. Whilst working towards a swift resumption, it is however important to note that conditions will vary from incident to incident and from FMI to FMI. Within this, we respectfully note that FMIs are already incentivised to return to full and orderly operation as soon as possible for systemic, business and reputational reasons. In particular we would note the following:

- **Section 6.2.1. Incident Response Planning:** WFE supports CPMI-IOSCO's approach on incident response planning. FMIs should thoroughly investigate any incident even while taking immediate action to contain the problem as a standard course of action, feeding back any "lessons-learned" via industry groups such as the GLEX, where possible and appropriate. The industry also backs stringent efforts on contingency planning and preparation including consulting with stakeholders before establishing final plans.

- **Section 6.2.2. Incident Response – resumption within 2 hours:** We consider the general premise of operational impairment and recovery are well-addressed in existing guidance and regulation, where recovery time objectives (RTOs) are appropriately and adequately considered. For the purpose of cybersecurity-specific guidance, however, ***the notion of resumption within two hours is inappropriate***. The scenarios that this document considers are analogous to acts of terrorism and events that add a malicious human element, making it near impossible to quantify recovery objectives. We therefore advocate that ***RTO should be left where it already exists in general and operational guidance and omitted from cyber-specific materials***.

- **Section 6.3.2. Data Integrity:** Different businesses will have different applications of integrity checking and re-establishment. For some businesses and scenarios, recording participant intent and replaying it will be appropriate. For many others, however, the only realistic path is to establish a point of reliability loss, invalidate transactions submitted after that point, and return to a previous checkpoint to resume processing. As such, ***there needs to be sufficient flexibility to allow each FMI to determine what is appropriate not only for their business but***

for the specific scenario and impacts they face. Further, in many cases it is the participants of the FMI that are the only entities properly positioned to conduct reconciliation activity, and this is often a real and regular part of daily processing in safeguarding against (non-cyber) operational error. ***Allowing participants to drive and inform reconciliation requirements directly is self-policing and successful already***. Tasking the FMIs with "independent reconciliation" is therefore prescriptive, unnecessary and potentially ineffective.

Finally, as an industry we support having a clear and timely plan for any crisis communications. These should be developed in advance, be operational in real-time given the nature of cyber issues and their impact on investor confidence, and clearly define the decision making procedures in advance.

Sections 7-9: Testing, Situational Awareness and Learning & Evolving

The proposed CPMI-IOSCO guidance references and ties to the NIST CSF very closely, with three notable additional areas of focus: Testing, Situational Awareness, and Learning & Evolving. We consider that the latter two items can be incorporated into NIST categories - namely Identification - and in the process stress the flexibility of the CSF and use the Guidance as a practical example of adapting the CSF to an area of focus. This would leave Testing as the only outlier. ***Since Testing is applicable to all of the NIST categories, we suggest subsuming those activities into the existing categories where they most appropriately fit***. On this topic, we had one additional comment:

- **Section 7.3. Co-ordination**: The emphasis on information sharing, collaboration, and exercise is rightly stressed. However, we consider that Phrasing should be changed from "*promote, design, organise and manage*" to "*participate"* to recognise the more reasonable approach of leveraging existing facilities without the threat of creating a mass of conflicting and redundant activities. In practice industry groups are already active and the appropriate duty for most FMIs is to identify and participate in these activities.

Additional Comments

Alongside those elements considered in the proposed guidance - which deal comprehensively with the main areas of cyber-defence - we submit the following two related sets of comments:

1) Information technology also lends itself to other kinds of defences including, for example, deflection. FMIs deal with data that has a lot of inherent economic value. Obtaining the data has value; modifying the data still more so. However, a well-designed system in today's world can be effective in deflecting or avoiding certain kinds of attacks reasonably easily, making it uneconomical for the attacker to gain any meaningful benefit from an attack and therefore reducing the chances that someone will try. Deflection of cyber-attacks is of particular value because of the naturally large attack surface that today's connected world provides to the attacker. As such, we consider it generally good practice for FMIs, where practicable, to deploy alternative strategies – including deflection - to sit alongside those proposed within the guidance. For example, it may also be worth considering avoiding static networks and routes, thereby reducing the ability for persistent attackers to probe for and map weak paths.

   However as previously noted, ***we caution against being overly prescriptive, and therefore advocate for these alternative defences to be considered to be built into FMIs' cyber***

strategies on a case-by-case basis, to ensure sufficient flexibility to meet the individual needs of FMIs, the markets they service, and the challenges/threats they face.

2) Whilst PFMI Principle 23 (Transparency - Disclosure of rules, key procedures, and market data) is not referenced as a key PFMI informing the guidance[3], the WFE would nevertheless like to raise an important issue relating to that particular PFMI and its read-across to cyber-related matters.

   PFMI 23 notes that "*All relevant rules and key processes shall be publicly disclosed…*" to enable participants to have an accurate understanding of the risks, fees and other material costs incurred by participating in the FMI.

   Here, with regard to cyber-resilience, we respectfully suggest that transparency for transparency's sake is not always a desirable outcome and may not achieve the wider PFMI public policy objectives "*…to enhance safety and efficiency in payment, clearing, settlement and recording arrangements, and more broadly, to limit systemic risk and foster transparency and financial stability*". Whilst acknowledging the benefits of transparency generally, ***any requirement to publicly disclose details on cyber resilience could be potentially detrimental to the objective and must be conducted in a carefully considered manner*** to ensure disclosure of such information doesn't better equip potential attackers and *increase* cyber resilience-related risk.

Conclusion

WFE and its members are committed to ensuring the trading and clearing environments they operate are secure, stable and designed to withstand shocks, and applaud international efforts to assist in that objective. Investor confidence in public markets is crucial for the industry and, as markets evolve - with technology bringing down costs for investors and allowing them to further mitigate risk - FMIs continue to be proactive and vigilant in ensuring these risks are actively managed.

Within that context we note that, notwithstanding regulatory initiatives to strengthen the system, given the important role they play, FMIs are already incentivised and motivated to ensure their systems are robust, resilient, stable and regularly tested. Our members invest significant amounts of time and money to ensure they are vigilant and can operate safe and orderly markets, while recognizing that efforts must be evolutionary and walk hand-in-hand with the development of markets.

As such, global practitioner groups such as WFE's GLEX have already proactively sought to identify and connect the key individuals at each organization to ensure there is a continuous and real-time dialogue and knowledge sharing on risks and issues that are specific to FMIs.

Given the universality of the issue and its systemic significance, global organizations and regulators must play a key role developing, fostering and promoting consistent industry-wide standards. Simultaneously industry groups should work together on education to ensure the common standards are the highest possible and consistently applied to ensure strength in the system. Ultimately, we are working towards the shared objectives of achieving fair, robust and resilient markets in which

[3] Box 1, page 5 of the Consultative Report: Guidance on cyber resilience for financial market infrastructure

investors can have confidence and so WFE and its members stand ready to work with international agencies to ensure this. However, within that:

- We note that different markets are at different stages of development, and so this needs to be taken into account when drawing up standards – including ensuring reasonable timescales for expected preparedness;

- We remind regulators and standard setters that threats and risks for FMIs are often different to those for wider financial institutions, and so policies and guidelines need to take into account the specific hazards to those businesses;

- We caution against being too prescriptive – whether in terms of strategies, frameworks, documentation, or recovery/resumption expectations. Different markets have different models and different needs, and incidents are unpredictable in nature. Further, technology moves quickly. As such, there needs to be an element of flexibility so that FMIs can react quickly as and when needed; and

- We urge national regulators – inasfar as national laws and regulations allow them – to not deviate from the final global principles to enable consistent international application and support the objective of ensuring there are no "weak-links" in the system.