EACH

European Association of CCP Clearing Houses

EACH response to the CPMI-IOSCO consultation paper ‘Guidance on cyber resilience for financial market infrastructures’

February 2016

1. Introduction

The European Association of CCP Clearing Houses (EACH) represents the interests of Central Counterparties Clearing Houses (CCPs) in Europe since 1992. EACH currently has 20 members from 16 different European countries and is registered in the European Union Transparency Register with number 36897011311-96.

EACH appreciates the opportunity to provide feedback to the draft CPMI-IOSCO guideline on cybersecurity for financial institutions. **We particularly welcome the principles-based nature of the draft guidance and agree with CPMI-IOSCO that the dynamic nature of cyber threats requires evolving methods to mitigate these threats.** We also concur with the view that requiring specific measures today may quickly become ineffective in the future. We, therefore, recommend that the **provisions be 'goal-oriented' in order to be applied in proportion to the level of risk** generated by the nature of an FMI's activity and size.

While we generally welcome the guidance proposed, below we include a list of suggestions based on the experience of EACH member CCPs that we hope will be useful to CPMI-IOSCO in finalising this work.

2. EACH responses to specific questions

2.1 Introduction (Section 1 in the guidelines)

2.1.1 Cyber risks are unique (1.1.3)

In our view, these are not the only source of threats. While some attacks can be attributed to individuals, there is actually a spread of adversaries ranging from individuals searching for recognition among fellow hackers, organised groups to state-funded organisations.

2.1.2 PFMI principles (1.1.4)

Having a risk management framework (e.g. ERM) is in our view not sufficient. It has to be used across all lines of defence in a consistent manner (Principle III). A quantitative approach, recognising the relative size of affected entities, may be helpful in the comparisons between relative risks.

2.1.3 ICT controls (1.2.3)

EACH members believe that ICT controls are important but not exhaustive. Process and organisational controls need to capture the linkage between IT and business functions. Process flaws can expose as much vulnerability as ICT weaknesses.

2.2 Governance (Section 2 in the guidelines)

2.2.1 Cyber resilience strategy and framework (2.2)

EACH believes that strategy is indeed a critical area of focus for Financial Market Infrastructures' (FMIs) cyber security. Spelling out strategy and framework as specific and separate products, however, is in our view prescriptive and risks driving firms toward a tick-box approach that creates confusing and overlapping artefacts that do not tie well to tactical practice. **Recognition should be given to the different scales, business focuses, level of risk and cultures that make up FMIs and flexibility should be afforded to allow firms to meet these needs via different approaches in documentation.** Some firms will have a single 'Strategy' document that captures everything intended in a strategy and framework. Others will have reams of procedural documents that incorporate many framework elements while moving strategic elements to mission and vision statements. Still others will be able to involve the Board directly in tactical policies.

The positive intentions of this guidance can be better met by a high-level and goal-oriented strategy which is well documented and informed. Policies and procedures established to execute that strategy should be documented and maintained. It is recommended that mentions of a strategy or framework be consolidated into the single term 'strategy'. We develop these points in more detail below.

2.2.2 Cyber resilience strategy (2.2.1)

We believe that the cyber resilience strategy needs to be integrated in an overall strategy of operational risk management. Aligning cyber risks using an approach of proportionality allows encouraging responsible boards to arrive at a balanced, risk-aware management approach.

This means that the cyber resilience strategy has to be both holistic and adaptive to threat landscape and organisational specific values and weaknesses. More specifically, the strategy needs to value the relative size of an organization to enable a risk-balance approach.

Consequently, there should be no 'one size fits all' approach but an adaptive strategy which allows for cyber resilience to be managed proportional to risk appetite, situation and environment. This certainly requires a two-prong direction: minimum cyber resilience based on threat profile with a scalable incremental set of resilience controls to reflect lower risk appetite.

2.2.3 Cyber resilience framework (2.2.2)

In addition to the points mentioned, EACH believes that a cyber resilience framework needs to recognise cultural awareness of cyber risks and usability as design principles. From experience, cyber resilience controls lose effectiveness if they impose too high of a burden on users specifically and organizations generically.

Moreover, EACH wonders whether it may be beneficial to put more emphasis 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 thus important that, when establishing their cyber resilience framework, FMIs seek to avoid unnecessary duplication with relevant processes related to information security management.

2.2.4 Enterprise risk management (2.2.4)

EACH agrees that physical security frameworks need to be integrated, however, a human-centric approach is potentially more fit-for-purpose in addressing resilience since it recognizes an organization's staff as a critical defence component. Human-centric cyber resilience integrates facility, process, organisation and behavioural elements, thus, it is more far-reaching than only ICT and physical. Besides, cyber risks need to be managed in the operational risk grid of an enterprise wide group management.

Finally, the risk management of cyber risks needs to be aligned across all lines of defences (Business, IS/Compliance/Risk and Internal Audit).

2.2.5 Role of the board and senior management; Skills (2.3.3)

We generally welcome recommendation 2.3.3 with regard to the role of the board and senior management of FMIs. It is important that Cybersecurity is considered at high-level within FMIs. We would however welcome further guidance with regard to the way in which boards and executive members might achieve the adequate skills with regard to cyber threats. Two possible options are: a) encourage Boards membership to include Directors with technology and/ or security experience; b) to give regular and adequate education to the current members of the board. We would encourage both options to be implemented in parallel.

Board and executive committee members need regular and appropriate education about cyber security trends, threats, risks and how the company can be affected. This educational work should be conducted / managed by the C(I)SO, potentially along with Group Risk and Compliance officer(s), using third party security experts if needed, and held at least yearly.

This includes regular reporting of C(I)SO roles to the board, exposing cyber risks regularly and pro-actively. In addition, C(I)SOs need to implement a strong second line of defense a real-time cyber situational awareness. They need to be empowered to enforce cyber resilience controls across ICT and business.

C(I)SOs need to inform not only senior executives and boards but also the supervisory boards as the highest level of corporate governance. They can help to drive the proper tone from the top across all parts of the organization.

2.3 Identification (Section 3 in the guidelines)

2.3.1 Identification and Classification (3.2)

EACH would suggest considering threat intelligence and situational awareness in the Identification phase of security programme management. In addition to merging content and more tightly-aligning with some national initiatives[1] by eliminating the need for a separate Situational Awareness section, this approach 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 FMIs, as much of today's industry guidance around cyber security is informed by the data theft and exfiltration events making headlines around 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, the threat of 'lobbing a grenade' 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, we believe that 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.

We also believe that CPMI-IOSCO should provide clearer guidance on the level of coordination required between an FMI and external stakeholders. For example, information-sharing with stakeholders may be inappropriate in certain cases, for example, where this involves the disclosure of confidential or competitively-sensitive information, and may therefore lead to additional risk exposures for the FMI.

2.3.2 Identification of information assets and related access (3.2.1)

We believe that the identification and classification of critical assets is one part of a bigger equation.

Understanding threat vectors alongside critical assets helps to focus cyber resilience controls to deploy more quickly around the main drivers for attacks:

- to divert financial transactions;
- to obtain critical information;

[1] US Cyber Security Framework developed by the US National Institute of Standards and Technology (NIST).

- to disrupt operations;

As adversaries operate on an international level, the interconnectedness of critical assets has to be reflected when assessing the value of information of an organization. This needs to happen across national boundaries, organizational limits and industry boundaries. Consequently, identification of threats in order to generate cyber situational awareness has to be multi-national and leverage the extended value chain of a FMI.

Identification needs to happen in a much more real-time fashion, driven by change events opposed to just frequency based approaches. This should also introduce change triggers which indicting a worsened risk profile of assets identified. Besides, additional control processes are required to ensure completeness of assets and threat actors.

Because not every organization can afford to deploy cyber intelligence teams (who are supposed to research on new adversaries, threat actors and vectors), collaboration among industry peers should not only be encouraged during operation but also while identifying the relevance of assets. To this extend, interconnections have to cause bi-directional exchange of critical interfaces require special protection.

Finally, not all assets are equal. We suggest taking special pre-caution for crown-jewels, differentiating minimum controls along the identified and labeling-enforced assets identified.

2.3.3 Interconnections (3.3)

Also, the exchange of information should be standardized to facilitate the speed if cyber threat exchange. Here we would see great value in CPMI-ISOCO to orchestrate standardization based on already established market standards such as STIX and TAXII (to pick two examples) but also across jurisdictions.

2.4 Protection (Section 4 in the guidelines)

Different FMIs have different levels of maturity. Therefore, the level of ICT controls should be handled proportional to the previously discussed risk-balanced model. Different FMIs may have varying degrees of maturity, driven by different market size, market conditions and threat exposure (e.g. driven by their attractiveness the threat actors).

We would suggest to choose again a dual approach: minimum protection requirements for everyone (protecting the downside) with the ability to allow risk acceptance for certain (cyber) risk levels by respective boards, especially of smaller organizations. We appreciate the current set of controls suggested by CPMI-ISOCO, however, assuming FMIs collaborate with each other on a regular basis, ICT controls are a component but not the only element of a successful cyber resilience strategy.

2.4.1 Resilience by design (4.2.2)

We recommend amending the suggested technical approach with state-of-the-art cyber defence processes. Those should reflect the cyber kill chain and the related attack vectors. Essential resilience processes include (but are not limited to):

- Vulnerability Management;
- (Privileged) Access Governance;
- Cyber Analytics;
- Anomaly Detection;
- Application and Device hardening;
- Threat hunting;

2.4.2 Strong ICT controls (4.2.3)

Strong ICT controls are without doubt an essential building block in creating an enterprise resilient against cyber threats. However, as important is the collaboration with other organisations around cyber situational awareness, threat defence (and counter attack).

In EACH's view, this recommendation wisely does not attempt to be prescriptive or comprehensive around ICT controls, but the specific examples cited will communicate priority and focus. **ICT controls should be risk based and should take into account best practices and standards, and to that end, highlighting four examples chosen could in our view be improved upon.** In particular, so far FMIs and regulatory examination has been focused on encryption, patch management, and system hardening.

Complementary to ICT controls are (non-exhaustive):

- Governance and Risk Management
- Human security controls (awareness, personal defence, etc.)
- Supplier security controls (enforcing security standards with suppliers and outsourcing relationships
- Physical security controls (incorporating facility related defences, travel security and safety)

We appreciate the currently planned requirement of minimum ICT controls which have to be enforced across the entire supply chain. It would be particularly valuable to provide guidance which controls should be provided by outsourcing/cloud providers as their control model often precludes introspection and client-driven approval processes (e.g. for sensitive data).

Furthermore, we see a need for special controls in the area of data protection, especially because national data privacy laws create a challenging environment with respect to location of critical data and controls requirements. It would be desirable to work on international standards which types of confidential or personal information is suitable for outsourcing.

2.4.3 Interconnections (4.3.1)

EACH agrees with the need for CCPs to implement protective measures to mitigate the risks arising from the entities within its ecosystem. We also believe that CCPs should indeed implement measures to mitigate effectively the risk arising from its connected entities.

We understand however that recommendation 4.3.1 operates under the premise that service providers have elevated, if not 'carte blanche', access to sensitive systems and thus tasks FMIs with the difficult task of ensuring provider security reaches the same level of control as the internal programme.

In order for the guidelines to ensure a robust cyber security regime for FMIs which can be realistically implemented, we would call for **these provisions to be applied with a certain degree of proportionality and that they focus on critical service providers** (e.g. provider of back-up facilities), rather than on all types of providers (e.g. office cleaning services), as it seems the case in the current draft guidelines which under paragraph 4.3.1(b) state 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. Cyber considerations should be integral part of the FMI's arrangements for managing vendors and vendor products in the areas of contracts, performance, relationships and risk. 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 provide.'*

In addition to the proportionality approach suggested above, we believe that **the approach to vendor and partner risk could be to either segment and minimise access outright and monitor the relatively small residual vectors of access closely or to allow vendors to make attestations and provide indemnification**. Focus should be on treating external connections similarly to Internet, terminating them outside the network perimeter, only allowing specific required and approved protocols and sources, and monitoring the resulting traffic with behavioural analytic tools.

2.4.4 Insider threats (4.4)

Prevention against insider treats need to reflect a motivational model for insider threats. Insider threats frequently correlate with personally compromised individuals, e.g. disgruntled employees/service providers, blackmailed individuals, etc.

As not all insider threats are solely related to employees, controls need to include background checks long before employment (for both HR and sourcing functions).
The suggested guidelines are necessary baseline controls. However, we believe they should be amended to extend beyond directly observable deviation from standard behaviours. Tracking for derailment situations assumes observable standard behaviour. Specifically, service providers with lower loyalty levels pose a much higher risk than employees.

Thus, different threat profiles of employed persons need to be reflected in adaptive control sets, recognizing loyalty levels, role (including threat potential), verifiable history, security rules compliance – and – behavioural changes.

2.4.5 Security analytics (4.4.1)

EACH believes that analytics, particularly behavioural, are rightly emphasised. **We believe that this recommendation would be better served by focusing on behavioural monitoring, determining baseline activity patterns with regard to systems and data accessed and hours and alerting on deviation from those patterns.**

Different roles carry different threat potential (this is why privileged users require special monitoring). Risk-based, adaptive cyber analytics help to focus and speed up analytics. Besides, data privacy requirements may restrict / alter the analytics processes (some legislation require worker's council involvement).

2.4.6 Changes in employment status (4.4.2)

This section should also include service providers and temp workers.

2.4.7 Access control (4.4.3)

We fully support the controls outlined to combat insider threats, we suggest amending them towards risk/attribute based authentication, reflecting out-of-country or out-of-context (e.g. off-hour) access which often indicate behavior changes.

2.5 Detection (Section 5 in the guidelines)

2.5.1 Detecting an attack (5.2)

Proper detection of an attack needs FMIs to understand the cyber security kill chain. Besides motivation of an attacker (group) it is critical to understand the typical attack vectors, indicators for attack pre-cursors (not only indicators of compromise) and long-term attack indicators.

Preparedness (cyber resilience) rules need to be triggered when pre-cursors are being detected as actual attack vectors might only occur when defences have already been breached. We suggest amending the model to include an early warning system.

2.5.2 Networked detection (not in paper)

Additionally, detection should programmatically include pro-active networking with peers and ecosystem partners. Selected managed security services could improve lead time to an attack and therefore improve the effectiveness of a FMI’s response.

2.6 Response and Recovery (Section 6 in the guidelines)

2.6.1 Incident response, resumption, and recovery (6.2)

EACH believes that the general premise of operational impairment and recovery are well-addressed in existing guidance and regulation where recovery time objectives are appropriately and adequately considered.

While EACH members understand the need for CCPs to resume critical operations as soon as possible in order to complete settlement by end of the day, EACH believes that the two-hours timeframe indicated in the guidance and included in the Principles for Financial Market Infrastructures (PFMIs) would be too short in certain circumstances. The scenarios that this document extends consideration to are analogous to acts of terrorism and events that add a malicious human element, making it near impossible to quantify recovery objectives.

The proposed two-hours timeframe could potentially lead to additional problems and not leave enough time for CCPs to analyse in detail the situation and implement adequate solutions, especially if the integrity of the system has been compromised. In addition, not all parts of the business chain of an FMI might be equally critical (and vulnerable). Therefore, recovery targets require a proportional factor, representing the market stability expectations. Consequently, areas of lower criticality could afford lower resilience targets.

As an alternative, we would suggest that the guidelines propose a goal oriented that is tied both to operational capability and integrity timeframe depending the type of attack. While some attacks may indeed allow the CCP to recover its critical operations within two hours, others, such as the integrity attacks referred to above would generally require a longer recovery time. For the latter types of attacks, a qualitative rather than a quantitative measure of recovery could be proposed. In such circumstances, we suggest that the Guidance should focus on the goal of ensuring that the systems are restored in a manner which preserves their integrity, confidentiality and availability. Therefore whilst FMIs should use a best efforts basis to meet the two hours deadline, they should be given the flexibility to exceed two hours where necessary to preserve the integrity of the system, confidentiality and availability.

The remaining emphases on incident response planning, contingency planning, and addition preparation are in our view appropriate and adequately comprehensive.

2.6.2 Design and business integration (6.3.1.)

We are in agreement with the suggested requirements. However, technically different backup systems are commercially not necessarily viable and should not be a requirement.

2.6.3 Data Integrity (6.3.2)

EACH members consider that different businesses falling under CPMI-IOSCO guidance will have different realistic 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 tenable path is to establish a point of reliability loss, invalidate transactions submitted after that point, and return to a previous checkpoint to resume processing. Therefore we believe that a certain degree of **flexibility needs to be afforded to FMIs to determine what is appropriate not only for their business but for the specific scenario and impacts they are processing.**

Further, in many cases participants in FMIs are the only entities properly positioned to conduct reconciliation activity, and in many circumstances this is a real and regular part of daily processing to safeguard against non-cyber operational error. **Tasking FMIs themselves with 'independent reconciliation' is in our view prescriptive and dangerous.** Allowing participants to drive and inform reconciliation requirements directly is self-policing and successful already.

2.6.4 Interconnections (6.4)

In addition to the suggested and acceptable ecosystem requirements, international and inter-connected stress tests for an FMI ecosystem need to test the resilience and preparedness of an FMI and key market participants on a regular basis.

A joint situational awareness within the FMI's ecosystem could complement local FMI controls. This also applies to the Testing section (7)

2.7 Testing (Section 7 in the guidelines)

2.7.1 Comprehensive testing programme (7.2)

We largely agree with the components of the suggested testing programme components.

Incremental to the procedural testing of processes and communication links, systemic tests to verify internal controls capabilities (e.g. methodical implementation of minimum security controls relative the identified risk exposure) in the area of the entire security controls lifecycle (specifically around the implementation of security controls, their testing and their introduction in production, including end-of-life and technology refresh scenarios)**.**

2.7.2 Coordination (7.3)

We believe that the emphasis in the Guidance on information sharing, collaboration, and exercise is correct. We would however **suggest an alternative wording to the current 'promote, design, organise and manage' and rather use 'participate',** in order 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.

- END -