WORLD FEDERATION OF EXCHANGES

WFE Response to the Financial Stability Board's Consultation Document – 'Effective Practices for Cyber Incident Response and Recovery'

www.world-exchanges.org

Background

Background

The World Federation of Exchanges (WFE) is the global trade association for regulated exchanges and clearing houses. We represent over 200 market-infrastructures, spread across the Asia-Pacific region (~37%), EMEA (~43%) and the Americas (~20%). with everything from local entities in emerging markets to groups based in major financial centres. Collectively, member exchanges trade some $95 trillion a year; while the 50 distinct CCP clearing services (both vertically integrated and stand-alone) collectively ensure that traders put up $1 trillion of resources to back their risk positions.

With extensive experience of developing and enforcing high standards of conduct, WFE members support an orderly, secure, fair and transparent environment for investors; for companies that raise capital; and for all who deal with financial risk. We seek outcomes that maximise financial stability, consumer confidence and economic growth. And we engage with policy makers and regulators in an open, collaborative way, reflecting the central, public role that exchanges and CCPs play in an internationally integrated financial system. The WFE coordinates its activities via working groups, which includes a dedicated enterprise risk group consisting of chief risk officers and risk experts, as well as a cybersecurity group (GLEX) with cybersecurity teams from around the globe.

If you have any further questions, or wish to follow-up on our contribution, the WFE remains at your disposal. Please contact:

Jonathan Pallant, Regulatory Affairs Manager: jpallant@world-exchanges.org
Richard Metcalfe, Head of Regulatory Affairs: rmetcalfe@world-exchanges.org

Overview

The World Federation of Exchanges (WFE) welcomes the opportunity to respond to the Financial Stability Board (FSB) consultation document, ***Effective Practices for Cyber Incident Response and Recovery (CIRR)***. We commend the work of the FSB in seeking to promote effective practices for cyber incident response and recovery across financial services and providing practices that will help other market segments 'level up' their standards in this area. Many of the practices detailed in the document are supported and embedded by WFE members, especially given their position as critical national infrastructure. As all sectors benefit from interaction with each other, the same standards should apply (mutatis mutandis), to ensure the best outcomes for the real economy. This includes the ability of financial institutions to respond and recover from cyber incidents.

Incident response and recovery capabilities are a key function of operational resilience. In order to promote the ability to manage dynamic, extreme threats, of possibly unknown duration, resilience capabilities are an essential requirement for all financial institutions and the financial services sector. Raising the resilience of firms, in keeping with the services they deliver, will ensure a more resilient ecosystem. The COVID-19 pandemic demonstrated evidence of financial institutions' ability to sustain operations in the face of a severe operational challenge. When looking at the pandemic through a cyber lens, financial institutions were faced with significant challenges. The pandemic proved that even when strong resilience measures are embedded by key market infrastructure[1], if the market participants are not required to meet certain controls, in accordance with the functions or services they deliver or support the delivery of, then that industry-wide resilience could be adversely impacted.

The WFE believes that the consultation document is beneficial and comprehensive, covering the key areas of cyber incident response and recovery that financial institutions need to consider. It also aims to be compatible with national approaches and standards which are, notably, ever-growing in their specificity[2].

With that in mind, the WFE would recommend greater use of the FSB Cyber Lexicon[3] in delivering commonality in terminology and thereby reducing the variance of differing meanings and definitions. The WFE would ask the FSB to consider including a glossary of terms and definitions for those terms not included in the Cyber Lexicon (e.g. unity of command) and ensuring clarity of use of those terms throughout. This in turn would reduce possible international market fragmentation related hazards.

It is noted that the FSB CIRR used the following nomenclature to structure this toolkit: '*Governance*', '*Preparation*', '*Analysis*', '*Mitigation*', '*Restoration*', '*Improvement*', 'and '*Coordination and Communication*'. It is important that the practices and terminology used are compatible with cybersecurity frameworks used across the world, such as ISO or NIST. Firms may be better facilitated by being able to easily map the practices referenced in the document to their cybersecurity frameworks, to ensure a harmonised approach. The FSB should consider indexing this toolkit to more closely align on this basis.

The FSB may also want to further consider how the effective practices are implemented by firms to ensure that they raise the level of cyber incident response and recovery programmes across financial institutions. It is also important that any regulatory approach, which may emerge, derived from the consultation document, is principles-based and outcomes-focused as opposed to a prescriptive list of practices that does not evolve in line with technology and changing types of cyber threats. Subsequently, such an outcomes-based approach would also recognise that different types of entities play different roles within the ecosystem (for example, brokers and exchanges), requiring

---

[1] The World Federation of Exchanges publishes update on industry cyber efforts during the pandemic, WFE, May 2020

[2] Cybersecurity a challenge for the public sector and the financial industry, BaFin, July 2020, Pg.45

[3] Cyber Lexicon, Financial Stability Board, November 2018

resilience measures that are adapted to their respective roles, yet simultaneously support the cyber and wider operational resilience required for the system as a whole.

The WFE would welcome a continually evolving and updated set of cyber incident response and recovery practices with the aim of constantly promoting them across industry. Cyber incident response and recovery is, of course, only one element of the cyber resilience, and operational resilience more broadly, needed by financial sector firms and the WFE stands ready to work with international regulators in all these efforts.

Specific Commentary

The WFE would also make the following additional specific comments:

GOVERNANCE

Board vs Senior Management Responsibilities

Under the *Organisation-wide Governance Framework* (Practice #1), greater delineation could be made between the roles and responsibilities of the board and that of senior management. In particular, clarification that the day-to-day management of CIRR activities lies with senior management while the oversight responsibilities of the board should include having access to the expertise needed to challenge the financial institution's CIRR strategy, ensuring that the CIRR is comprehensive and covers all of the organisation's functional areas, and that the appropriate expertise is also available to perform the CIRR responsibilities.

Roles and Responsibilities

Material incidents often involve bespoke crisis or incident management teams consisting of a broad cross-section of organisational roles. Given that each individual / business area represented in these groups has a specific purpose, this practice (Practice #3) may be more effective if no specific role is identified and defined. The category and nature of the incident (i.e., Practice #19, *Cyber Incident Taxonomy*) would also influence the procedures and staff involved in managing the incident.

PREPARATION

Terms and Definitions

The consultation document would benefit from aligning the terminology with those terms defined in the 2018 FSB Cybersecurity Lexicon[4]. There are also terms contained in the document where the definition may be unclear or unknown. As an example, Practice #10: *Plans and Playbooks*, uses *cyber resilience* in a manner that appears to be equal or synonymous with *cyber incident response and recovery*. This may also be the case with the use of the terms '*plans*' and '*playbooks*' where these terms may not be synonymous across the financial services sector. Detailed description of the tools and practices involved might benefit the user. More broadly, ensuring appropriate mapping and indexing of the practices and references to international cybersecurity frameworks and/or regulations (as appropriate) would also aid the implementation of the practices.

[4] Cyber Lexicon, Financial Stability Board, November 2018

Expansion of Concepts

There are certain practices where the expansion of the provided concept is needed for clarity. For example, Practice #15: *Forensic Capabilities* reads, "*The types of logs to be collected and retention period of logs are predetermined.*" For financial institutions where the availability of expertise may be limited, it could be beneficial to provide examples of the criteria used to determine the types of logs and retention periods (e.g. legal or regulatory requirements, criticality of business data on the system, criticality of the business data that passes through the device).

Scenario Planning and Stress Testing

While not advocating for the removal of planning and testing for identified scenarios, the WFE would caution against emphasis on scenario-based testing (especially by regulators). Planning for set scenarios (Practice #12), as advocated in a number of jurisdictions under the '*severe or extreme but plausible'* approach, can have drawbacks. Unforeseen, or new scenarios can always emerge, the preparation for which, if there has been any, may greatly alter between organisations. This may result in one or more organisations having greater preparation for that particular scenario becoming reality without consideration for the wider ecosystem. As a result, other market participants' organisations could be less or even unprepared for such an event.

From a practical perspective, failures are more straightforward to plan for and recover from (e.g., using contingency network equipment, parallel utilities services, secondary data centres). The real challenge for incident management is, arguably, partial failure or service degradation where teams are dealing with novel (or previously unknown) issues with only partial or emerging information. It is in these situations that an organisation's incident response capability proves itself. Rather than dealing only with that which is known, the incident teams need the ability to triage and address unknowns – in effect, the ability to rapidly, and as efficiently as possible, manage any such scenario. This is crucial from a business resilience perspective and potentially more so than the more obvious 'failover' scenarios. Greater emphasis could, instead, be focused on understanding how firms are setup to respond (as with other effective practices listed) and how entities consider and determine their approach to novel risk management to achieve the end outcome of cyber and, ultimately, operational resilience.

RESTORATION

Recovery Time Objective

The *Governance* section, (Box 1) advocates for organisations to establish metrics to measure the impact of a cyber incident and to report to management the performance of CIRR activities. The WFE agrees that metrics are important to measure a financial institution's performance of cyber incident response and recovery activities. However, the examples detailed in 'Box 1', refer to "recovery point objectives (RPO) and recovery time objectives (RTO) [being] satisfied". The use of RTOs can result in counterproductive actions in the face of a cyber incident by pressurising support teams into the restoration of systems based on time constraints rather than ensuring that the threat has been neutralised and the systems are no longer compromised. Further, the consultation document then supports a 'validation' process as part of its effective practices in *Restoration* (Practice #30) but which appears at odds with the previous mention of the use of RTOs:

> **"Validation**. Organisations validate that restored assets are free of compromise, fully functional and meet the security requirements before returning the systems to normal business operations."

This is further confused by existing regulation which differs on the use of RTOs. For example, under EMIR[5] an RTO of under two hours is mandatory for inclusion in a CCP's business continuity plan. Clarity on the interaction with existing regulatory approaches that conflict or appear ambiguous, particularly on the use of RTOs, may resolve this.

IMPROVEMENT

Cross-Sectoral and Cross-Border Exercises

The WFE welcomes the practice (Practice #35) and advocates for cross-sectoral and cross-border exercises. All market participants ultimately have a shared incentive for a well-functioning and resilient market. Engagement across the financial service sector is the only way to achieve that common goal. The use of industry-wide resilience testing to exercise firms' response strategies to potential crisis situations, where the whole industry is impacted (e.g. the Quantum Dawn exercises in the US[6], the Raffles exercises[7] in Singapore) help to address this objective. Such exercises support a 'levelling up' of any parts of the ecosystem that may not be operating effective practices.

External Events and Sources and Industry-Wide Initiatives

In line with its membership guidance, the WFE has long supported the need for market infrastructure to be prepared and resilient. For this reason, the WFE has previously created working groups, consisting of exchange and CCPs' risk experts and CISOs from across the globe, focused on enterprise and operational risk and on cybersecurity (GLEX – Global Exchange Cybersecurity). These groups have the expressed aim of sharing information (i.e., Practices #37 and #38), developing best practice, benchmarking and have specific threat-intelligence sharing mechanisms in place. The WFE would welcome further broad engagement with international standard-setters to ensure the full potential of the groups is realised.

COVID-19 AND LESSONS FROM THE PANDEMIC

The WFE published a report, ***How Market Infrastructure Is Delivering Safe and Efficient Trading Venues During A Global Pandemic***[8], detailing measures the industry undertook to adapt and enhance existing cyber-resilience tools during the pandemic, as exchanges and CCPs across the world successfully moved to operate remotely. Prior cyber-resilience measures were integral in shielding market infrastructures in relation to pandemic related cyber threats. An observation, for instance, during the time of this pandemic was the increase of phishing emails using the pandemic as a means to trick individuals into accessing malicious links in order to compromise the user's systems. While phishing did not constitute a new threat vector, the pandemic did increase the value of the bait used to entice individuals to 'click on the link' and facilitate a cyber-attack. Significant measures had already been taken by financial institutions to limit the impacts of phishing and other threats that were encountered over the pandemic. These measures include security awareness of the threat and security training to inform individuals on the identification of the threat. These existing measures and investments in cyber resilience have proven to be effective in the face of this pandemic and serve as one example that financial institutions should not radically alter their approach to managing resilience.

---

[5] Article 17 (6) of RTS 153/2013

[6] Standing Together for Financial Industry Resilience, Quantum Dawn IV after-action report, June 2018, Deloitte

[7] Singapore's Financial Sector Wraps Up Two-day Exercise to Strengthen Business and Operational Resilience against Cyber Threats, Monetary Authority Singapore, November 2019

[8] This report can be found on the World Federation Of Exchanges site at: https://www.world-exchanges.org/storage/app/media/cyber-security-in-the-age-of-covid-19-board-003.pdf