WORLD FEDERATION OF EXCHANGES

April 2017

World Federation of Exchanges: Exchange and CCP Cyber Resilience

Visit us at:
www.world-exchanges.org

Preamble

The World Federation of Exchanges (WFE) and its members who operate exchanges and CCPs (collectively "WFE members") are highly incentivised to ensuring the trading and clearing environments they operate are secure, stable and resilient. This is fundamental to their business.

In light of the work CPMI and IOSCO[1] have undertaken in 2016 relating to Financial Market Infrastructure (FMI), and the recent G7 publication[2] relating to the wider Financial Sector, the WFE hereafter reiterates the views of the exchange and CCP industry on cyber-related matters.

This is in the dual interests of:

- Assuring regulators the industry is fully on top of and committed to cyber resilience; and

- Providing a common industry standard to be used by new /developing markets in order to benchmark their cyber security arrangements against.

Introduction

WFE members continue to prioritise cyber resilience to ensure the strength of their markets, particularly given the level of interconnectedness amongst other financial market participants. They are highly motivated to ensure their systems – and the wider financial system in which they operate - are robust, resilient, stable and regularly tested. However, not all are at the same stage of development.

Risk tolerance, threat landscape and systemic nature vary from market to market; each operates in different legal and regulatory environments, are at different stages of maturity, and apportion differing cyber budgets.

As such, being overly prescriptive or trying to offer a "one-size-fits-all" approach will not likely succeed.

Therefore, whilst acknowledging the need for flexibility, below we provide guidelines for WFE members to serve as the building blocks on which their individual approach should be based

[1] CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructure

[2] G7: Fundamental Elements of Cyber Security for the Financial Sector

Standard

In general, exchanges should align their processes and procedures with key relevant elements of existing global standards[3] with a particular focus on availability and avoiding tamper or disruption.

- **Strategy and Framework**: WFE members should have effective cyber framework arrangements in place to establish, implement and review their approach to managing cyber risk. To enable this, they should develop and document a high-level strategy, with clearly documented policies and procedures established (and maintained) to execute that strategy.

- **Governance**: WFE members should have appropriate lines of accountability, responsibility and cultural buy-in throughout all levels of the organisation regarding cyber resilience.

- **Risk Identification**: WFE members should regularly identify, update and review processes and business functions to ensure they are aware of, and proactively mitigating, any new risks - in addition to monitoring for existing ones.

- **Protection / Controls**: WFE members should continuously evolve their protection measures, such as security controls and systems and processes - including behavioural monitoring - to ensure they keep pace with market developments.

- **Monitoring and Detection**: WFE members should ensure strong detection controls and standards that are proportionate to each member's relative size, systemic importance, risk tolerance and threat landscape.

- **Response and Recovery**: WFE members' response and recovery strategies should aim to ensure that critical systems can be restored to full operation as soon as practicable without further compromising the orderliness of the market, acknowledging that conditions will vary from incident to incident, and member to member.

- **Information Sharing**: WFE members should seek to proactively share experiences, knowledge and expertise, and to cooperate and collaborate through industry groups such as WFE's Global Exchange (GLEX) cyber security working group.

- **Testing, Situational Awareness and Learning & Evolving**: As per the overarching cyber strategy and framework, WFE members should have effective arrangements to review and refine all elements of their approach to ensure their arrangements remain commensurate with the evolving threat landscape.

[3] for example, CPMI-IOSCO, NIST