WORLD FEDERATION OF EXCHANGES

PRINCIPLES TO CONSIDER WHEN DESIGNING AND IMPLEMENTING CYBER STANDARDS FOR FINANCIAL MARKET INFRASTRUCTURES

INTRODUCTION

The World Federation of Exchanges (WFE) is the global trade association that represents more than 200 Financial Market Infrastructures (FMIs), of which more than 100 are Central Counterparties (CCPs) and Central Securities Depositories (CSDs). 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, across all asset classes, 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 organisations to support and promote the development of fair, transparent, stable and efficient markets around the world.

SUMMARY

Cyber security matters have been - and continue to be - a topic of great priority for FMIs, and one in which significant time, effort and money has been invested. FMIs are naturally incentivised – for business and reputational purposes – to ensure their markets and ecosystems are safe and resilient.

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 we applaud the work of international bodies – and in particular CPMI and IOSCO - on this important issue.

Alongside this support, the FMI community also advocates the importance of industry-led initiatives and solutions. Global practitioner groups such as the WFE's GLEX[3] group have already proactively sought to collaborate in knowledge-sharing regarding risks and issues which are specific to FMIs, thus ensuring a continuous and real-time dialogue. Regulators and FMIs therefore need to work hand-in-hand in implementing sensible and practical arrangements.

As such, the principles presented here seek to capture practical and operational considerations that we encourage national and regional regulatory agencies to build into their thinking when designing, implementing and/or monitoring for compliance with rules, regulations or laws that affect the operational resilience of market infrastructure providers at the local level. These are not designed to be exhaustive and are intended as a prompt for

[1] The WFE membership list can be found here

[2] As at end 2015

[3] Global Exchange Cyber Security Working Group

further regulatory and industry discussion to ensure appropriate standards and expectations that fit the nuances of global markets operating in local jurisdictions.

THE CONTEXT

CPMI-IOSCO's Principles for Financial Market Infrastructures (the PFMIs) offer a sound framework under which FMIs should consider operational resilience matters. The supplementary guidance within the CPMI-IOSCO '*Guidance on Cyber Resilience for Financial Market Infrastructure*'[4] elaborates further on the five main areas of the PFMIs that are relevant for cyber security. The WFE applauds CPMI and IOSCO on the pragmatic approach it has taken to the design to date and the engagement it has had with the industry in doing so.

Further to the CPMI-IOSCO guidance, WFE offers its perspectives on areas it considers important for national and/or regional legislators and regulators (collectively: "authorities") to consider in their implementation, and/or the design of alternative or additional standards – and the monitoring of compliance thereafter, to ensure that markets are not only resilient, stable, effective and robust, but also are able to operate on a fair, level and safe playing field.

GOVERNANCE

There is great importance in having effective arrangements to establish, implement and review the approach to managing cyber risk. Also 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. Further, it is important to connect the dots and share knowledge and best practice within the community.

However, the different scales, business focuses and cultures within each FMI needs to be recognised, and flexibility afforded to allow individual institutions to meet desired outcomes via different methods.

As such it will be important for national and regional authorities to ensure flexibility when designing, implementing and monitoring for compliance with standards relating to cyber strategy, governance and procedures, taking into account the differing businesses and stages of maturity.

IDENTIFICATION

Identification is a key component of cyber preparedness, resilience and recovery. However, FMIs are different in nature to other parts of the financial system, tending to be forward looking and proactive, with a particular focus on systems availability and avoiding tamper or disruption.

As such, when designing and implementing standards – and monitoring for compliance thereafter - it will be important that national and regional initiatives do not to stifle FMIs' efforts on identifying threat actors and categories, tools, and methods so that FMI defences may still be properly positioned and tested.

The system is only as strong as its weakest link; WFE members support an approach that considers the risks presented by the wider ecosystem. However, that ecosystem is filled with multiple FMI and non-FMI actors, and therefore there is a finite amount any single organisation can achieve outside its own system.

It will be important that the design and implementation of national and regional standards and principles fosters cooperation and supports coordination by ensuring

[4] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf

there is consistency across different parts of the system. Whilst in their interests to ensure and encourage third party providers to have resilient cyber defences, FMIs themselves should not be penalised for risks identified and mitigated by FMIs but generated by third parties.

PROTECTION

Cyber controls should be strong and robust, yet 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 have systemic significance and invest time, resource and management attention on protection measures including security controls and systems and processes. However, not all FMIs are at the same stage of development. Level of systemic importance varies from market to market, and so too can the risk tolerance and threat landscape.

As such, in designing and implementing standards it will be important to remain sensitive to the fact that being overly prescriptive, or offering a one size fits all approach, will not likely be successful.

Similar to Identification standards, interconnectedness risks need to be considered and frameworks designed to build in protections from external third party risks. However:

It should be recognised that whilst an individual FMI has the responsibility for all services – including those provided by third parties – it may not always be possible to ensure such providers meet the same level of cyber resilience as the FMI itself.

DETECTION

In designing and implementing local and regional standards, and monitoring for compliance thereafter, it will be important that controls and standards are proportionate and consistent to the FMI's relative size, systemic importance, risk tolerance and specific needs.

RESPONSE AND RECOVERY

FMIs play a key role in supporting financial stability, including ensuring obligations are settled when they are due. The focus of FMIs' response and recovery strategies is to ensure that critical systems resume full operation as soon as possible and without further compromising the orderliness of the market. Whilst working towards a swift resumption, conditions will vary from incident to incident and from FMI to FMI. It is important to have a clear and timely plan to deal with, and communicate, crises.

As such, whilst it will be important to encourage robust post-mortem reviews, feeding back any lessons-learned via industry groups where possible and appropriate, rules and standards should remain flexible enough to allow each FMI to determine the critical services appropriate not only for their business but for the specific scenario and impacts they face - including with return to operation timelines and procedure.

TESTING, SITUATIONAL AWARENESS AND LEARNING & EVOLUTION

As above, regulatory standards and expectations should encourage robust testing, as well as post-mortem reviews and feeding back any lessons-learned via industry groups where possible and appropriate. Information sharing, collaboration, and exercise is rightly stressed.

WORLD FEDERATION OF EXCHANGES

TRANSPARENCY – DISCLOSURE OF RULES, KEY PROCEDURES, AND MARKET DATA

Transparency for transparency's sake is not always a desirable outcome and may not achieve wider public policy objectives to enhance safety and efficiency within the market infrastructure and - more broadly - to limit systemic risk and foster transparency and financial stability.

Any requirement to publicly disclose details on cyber resilience could be potentially detrimental to the objective, and it will be important therefore to consider carefully the approach to ensure disclosure of such information does not better equip potential attackers and increase cyber resilience-related risk.

PRINCIPLES TO CONSIDER WHEN DESIGNING AND IMPLEMENTING CYBER SECURITY STANDARDS FOR FINANCIAL MARKET INFRASTRUCTURES

Given the universality of the issue and its systemic significance, global organisations and authorities must continue to play a key role in developing, fostering and promoting consistent industry-wide standards for FMIs. Industry groups should also work together to ensure the common standards are the highest possible and consistently applied to ensure strength in the system. WFE encourages national and/or regional standard setters and implementing authorities to engage closely with the industry, and to use the following high level principles when setting and implementing requirements at the regional or local level, to ensure they are sufficiently flexible and workable in the global context:

1. In developing and implementing FMI standards, existing cyber security standards[5] should be utilised to ensure consistency of approach and operational convention, and it should be made clear against which international standards FMIs will be assessed. However, FMI standards should be flexible enough to accommodate differences in regional and national legal and regulatory frameworks;

2. In developing and implementing FMI standards, account should be taken of standards and approaches for non-FMI parts of the system, to ensure a consistently applied regulatory and operational approach;

3. Cyber resilience frameworks should be suitably robust yet balanced, and designed so they can easily be enhanced to incorporate new technologies and market models/services, without undue restriction;

4. FMIs - as market and operational experts – should continue to be consulted to ensure that FMI standards are developed and implemented which are workable, acknowledge the specificities of the particular FMI model, and do not give rise to unintended consequences;

5. Global principles should – insofar as national laws and regulations allow – be consistently implemented at national level without deviation or super-equivalence, to support the objective of ensuring a level playing field with no weak links;

6. Different markets have different models and different needs, and incidents are unpredictable in nature. Further, technology moves quickly. Standards and expectations should therefore have an element of flexibility so that FMIs can react quickly. In particular, flexibility should be applied in:

    i. The design and review of cyber strategies and governance;

[5] For example, National Institute of Standards and Technology - NIST - or ISO-IEC standards

ii. The application of more general operational resilience standards to cyber specific matters – which may not always be mutually applicable;
iii. Control standards (which should be proportionate and consistent to the FMI's relative size, systemic importance, risk tolerance and specific needs);
iv. The reasonableness of the length of time taken to resume operations following an incident; and
v. The extent to which details of cyber events, processes or controls are required to be made publicly available.

7. Further, national or regional regulatory standards should encourage, although not be restricted to, the following:

i. Identification efforts to focus on identifying threat actors and categories, tools, and methods[6] so defences may be properly positioned and tested;
ii. An emphasis on all phases of cyber kill-chain[7];
iii. Industry collaboration, and collaboration between the industry, the regulators, and other key parts of the system;
iv. Robust testing, post-mortems and sharing of information where possible and appropriate.

CONCLUSION

WFE and its members are committed to ensuring the trading and clearing environments they operate are secure, stable and designed to withstand cyber incidents. Investor confidence in public markets is crucial for the industry and, as markets evolve, FMIs continue to be proactive and vigilant in ensuring these risks are actively managed.

FMIs are highly incentivised and motivated to ensure their systems are robust, resilient, stable and regularly tested, and they invest significant amounts of time and money to ensure they are vigilant and can operate safe and orderly markets. Global practitioner groups have already proactively sought to work together to ensure there is a continuous and real-time dialogue and knowledge-sharing on risks and issues that are specific to FMIs.

As such, these principles are designed to capture considerations that we would encourage local and/or regional authorities to build into their thinking when designing, implementing and/or monitoring for compliance with rules, regulations or laws that affect the operational resilience of market infrastructure providers.

Given the global nature of the issue and its systemic significance, it is right and correct that authorities play a key role developing, fostering and promoting consistent industry-wide standards. Simultaneously industry groups should work together to ensure the common standards are the highest possible, and are consistently applied to ensure overall strength in the system.

Ultimately, we are working towards the shared objectives of achieving fair, robust and resilient markets in which investors can have confidence. As such, authorities and FMIs need to work hand-in-hand in implementing sensible and practical arrangements for the benefit of the wider system; WFE and its members therefore stand ready to work with regulatory agencies to ensure this.

[6] For example, targeted account hacking, a common method observed

[7] For example, see LockheedMartin Cyber Kill-Chain