Cybersecurity – WFE Statement

How Market Infrastructure is delivering Safe and Efficient Trading Venues during a Global Pandemic

Introduction

During this time of increased market volatility, cyber threats have not gone away and, without care and attention relating to exceptional working procedures, there is the concern that adversaries may identify and exploit new routes into the system to either compromise operations or information systems.

In the face of these challenging, unrelenting and unparalleled considerations in the operation of critical market infrastructure, many exchanges and CCPs have purposefully triggered continuity plans (involving, for example, remote working) to ensure their operational resilience and ability to serve their markets, when needed most, against the backdrop of social-distancing policies that governments around the world are adopting. Through the WFE, they are actively collaborating and sharing best practice on these and other measures taken to keep markets open and resilient. The World Federation of Exchanges (WFE) has also launched a repository of COVID-19-related public communications from exchanges and CCPs on its website, as a resource for the financial community and our stakeholders.

Role of Market Infrastructure

Market infrastructures, i.e. exchanges and central counterparties (CCPs), are amongst the critical elements of the financial system which must remain open – supplying finance to the real economy and a platform for investors at a vital time. For this reason, they have well-developed business continuity plans, which have now been executed according to plan. Accordingly, market infrastructures are now operating their business as robustly as usual, with record volumes of trading. This is no easy feat in effectively enabling safe and efficient markets to function and oversee global trading – not in their established venues but often from employees' homes.

Action by the WFE and Global Market Infrastructures

Cybersecurity is an integral – and integrat*ed* – part of those contingency arrangements. Cybersecurity consistently remains in the top quartile of WFE regular surveys of membership priorities and focus. Across the membership, market infrastructure has consequently dedicated time and resources to the preparation of contingency planning and the associated cybersecurity requirements. These efforts are typically subject to regulatory and supervisory scrutiny, as well as in-house or external auditor stress testing. In current circumstances, this planning is proving its value in real time as never before, with market infrastructure arrangements focused on the outcome of safe and efficient markets.

Across businesses employees working remotely from home now rely on home Wi-Fi routers, commercial network providers, and a combination of corporate and personal endpoint devices that may not all have been configured to withstand a targeted cyber-attack. This environment can increase the risk of system misconfiguration and the potential unauthorised disclosure or theft of sensitive company information. Cyber adversaries are also increasing reconnaissance techniques to identify and exploit system security vulnerabilities, execute targeted COVID-19-related phishing campaigns, and attempting to compromise personal and corporate-owned mobile devices. The current conditions, as a result, shift information security focus from enterprise infrastructure located mainly within corporate-owned data centres to public/private cloud and virtualised architecture. To address these

risks companies have used their secure remote connectivity options such as Virtual Private Networks (VPN) and establishing access to corporate environments through Virtual Desktop Infrastructure (VDI).

With the backing of the WFE's GLEX (global exchange cybersecurity) working group, and in co-operation with their regulators, many exchanges and CCPs have developed their resiliency plans and 'stood up' a number of further cybersecurity measures to support safeguarding their operations and the economies they serve. The scaling up of these reserve measures is successfully managing the unprecedented features of markets experiencing the consequences of the pandemic, as well as those who seek to take advantage of the disruption to infiltrate crucial systems for their own gain.

However, members are not complacent about handling the ever-evolving threats they face and are ever vigilant – continuously investing resources and technology to enhance their capabilities. These activities and actions are taken under the philosophy that it is not a question of 'if' they experience a cyber incident but when. In operating the core critical infrastructure vital to the successful functioning of economies, adherence to this principle requires market infrastructure operators to be in a constant heightened state of awareness and vigilance, so that they can respond and recover operationality, should any cyber-attack take place.

Among the measures operated by members which facilitate continued safe and efficient trading are (but not exhaustively):

Mass/Remote working

- Ensuring licences and infrastructure is expanded to enable all staff to work remotely. In a number of organisations all staff already had the ability to work remotely, using desktop replication systems or a VPN with multifactor authentication.
- Ensure remote access systems are fully patched and have secure configuration.
- Recirculated and updated guidance for employees to protect the home network, such as change the default passwords for routers, keeping equipment updated, and create distinct work and guest networks.
- 'Awareness notes'/notifications regularly circulated to staff tailored around COVID-19 based phishing attacks and fraudulent communications. These stress the requirement for diligence and how to handle (sensitive) information and access to documents from home, and the management of printed materials.
- Clear communication of technical channels and support procedures to prevent social engineering attacks.
- Special notices (which have also gone to market participants), regarding the increased threats related to COVID-19 scams.
- Security operations centre (SOC) teams continually reviewing perimeter issues and device telemetry for spikes/abnormality.
- Security tests (Red Teams) focused on new threats and use cases, identifying technical vulnerabilities and behaviour improvements.
- Regular communications from senior and risk management teams to ensure appropriate regulatory measures, protocols and safeguarding is followed by staff.
- Regular liaison with regulators/supervisors and cybersecurity working groups, to share information and, if relevant, refresh best practices and requirements.
- Expenses/allowances for staff to enable the use of equipment for home working which is of sufficient high-standard and incorporates the high-standards cyber defences required.

- Embedded cyber incident response plans and employee support teams, as well as dedicated COVID19 management teams (alongside existing crisis management teams and incident response teams).
- Highlighting processes for responding to a security incident across an unfamiliar and distributed operating environment when you a have a dispersed cybersecurity workforce or not all critical personnel are available.
- Raising contingency out-of-band communications channels when the corporate network or other traditional communications channels have been compromised by the attackers.

Remote collaboration tools (video and audio-conferencing applications)

- Use of advanced end-point security solutions are being used with in-house working groups to review and approve the use of such tools, to enable communications to happen more safely.
- Proactively prohibiting the use of any platforms which do not comply with corporate security requirements, as well as providing clear guidance on approved mechanisms and tools.

Third-Party risk

- Continued structured and frequent engagement with critical service providers (e.g. cloud service providers) and critical vendors, including collaboration to support remote connectivity and cyber resilience strategies.

These efforts are alongside previously published practices and more detail on best practice cyber security guidelines[1] can be found here.

The WFE is tracking the information-sharing that market infrastructures globally are making to their stakeholders, and has taken a lead in addressing stakeholders in response to recent market volatility and COVID-19. To this end, we have created a comprehensive, rolling repository of exchange and CCP efforts. This can be found on our website and we encourage you to sign-up for regular updates.

When the current world-wide pandemic situation, hopefully, lessens and countries and companies implement measured return to work procedures, WFE members recognise there will be a "new normal" operating environment for all in which such measures must continually be monitored, reviewed and implemented to protect against future threats.

Market infrastructures around the world recognise their responsibility not only to issuers and market participants, but to the economies they serve and society at large. We believe that with continuing appropriate action, information-sharing and vigilance, along with a fundamental focus on market integrity, markets will be able to help their economies come through the current crisis.

[1] WFE 2018, The World Federation of Exchanges publishes best practice guidelines for cybersecurity compliance, https://www.world-exchanges.org/news/articles/the-world-federation-of-exchanges-publishes-best-practice-guidelines-for-cyber-security-compliance