Cyber Security in the Securities Markets-An international perspective. May 2016.

At its February 2014 meeting, the IOSCO Board decided to support a range of initiatives being considered in the field of cyber security in the securities markets, recognizing the need to confront a threat to the integrity, efficiency and soundness of the world's financial markets. The Quebec AMF is coordinating a number of IOSCO Policy committees and other stakeholders on cyber security issues, with support from the China Securities Regulatory Commission (CSRC) and the Monetary Authority of Singapore (MAS). The work has been focused on the cyber security challenges faced by IOSCO members and other stakeholders in the securities market and it was summarised in a report. The five key issues identified at this first step toward a common security policy are risk identification, protection of technical facilities, organisation and staff awareness, detection by monitoring data traffic (combining SIEM software tools with company intelligence services), response, with business continuity plans (BCP) and measures to safeguard or recover data or system availability, and recovery, taking account of the specificities or the company or sector concerned.

In relation to the role of the regulators, a wide diversity of regulatory options and practices may be useful and successful. The report gives examples of regulation in different jurisdictions (Singapore, Australia, the UK and USA) whose common thread is the flexibility generally afforded to regulated institutions when dealing with this problem. It also gives examples of practices used by market stakeholders to identify, protect, detect, respond and recover from cyber-attacks. The report goes on to discuss the issue of information exchange, based on IOSCO's Principles and the multilateral memorandum of understanding (MMoU) on inter-authority cooperation in the investigation of breaches linked to cyber-crime.

The report contains an introduction to cyber security issues, seven chapters, general conclusions, in addition to bibliography and appendices.

Chapter 1 sets out the introduction and defines cyber risks, cyber-attacks, countermeasures available to supervisors and improvements in cyber security practice for market participants. New technologies bring advantages and disadvantages. Securities trading is electronic and therefore continuously at risk. Some organisations fail to report attacks due to concerns about their reputation. A survey by IOSCO and the World Federation of Exchanges (WFE) found that 53% of securities trades were affected and these threats are on the rise. Various initiatives have been taken to confront these threats. In Singapore guidelines have been issued. In the UK, action has focused on proposals for institutional management and the USA has emphasised the role on the registered investment firms.

Chapter 2 deals with disclosure of incidents, principles for regular disclosure and the disclosure frameworks in IOSCO member jurisdictions dependent on domestic law. It recommends applying existing IOSCO standards designed to prevent cyber-risks.

Chapter 3 focuses on trading venues and recommendations for electronic trading, periodic reviews, secure practices and scrutiny of current cyber-security frameworks. It gives examples of hackers, criminals and possible terrorist attacks and a list of potential cyber vulnerabilities. It also summarises the National Institute of Standards and Technology (NIST) framework. Trends that emerge in trading venue security practice include attract-and-trap systems, real-time threat information, SIEM tools, internal data protection, third party management, new cloud-based security focuses and collaboration with the trading venue community. It also describes the cyber security regulatory frameworks applying to trading venues. A preliminary conclusion on this issue is that regulators take different roles to ensure cyber security and have simulated a range of attacks including breaches involving computer systems, members of SROs – self-regulating organisations – and institutional clients.

Chapter 4 deals with market intermediaries. The relevant IOSCO committee has formed a working group to provide assistance in this area, including a list of basic requirements, essential reading and relevant reports

addressing the five functions listed above. It looks at the examples of Mexico and the USA. Steps taken by FINRA include governance and risk management for cyber security, risk assessment, incident response planning, staff training, cyber intelligence and information sharing. There seems to be no "one size fits all" approach to cyber security for all members.

Chapter 5 looks at asset managers, based on an 85-question survey of members designed to generate some reliable data for management use. Among the conclusions drawn were: i) ensure information security programmes are consistent; ii) use large complex passwords; iii) carry out a periodic inventory of computers, software and applications; and iv) have a detailed response plan. Regulators have taken a variety of steps in response to cyber security issues, some emphasising particular management arrangements, others a principle-based approach. Regulators have started to examine breaches and trade associations have launched initiatives including seminars, awareness raising, experience sharing and simulated attack drills.

Chapter 6 considers financial market infrastructures. The joint CPMI-IOSCO Working Group on Cyber Resilience (WGCR) has issued draft guidance for FMI's covering governance, identification, protection, detection, response and recovery issues. Once these criteria have been addressed it is essential to run tests, remain aware of the changing situation and learn and evolve. The guidance suggests taking an active role in serving stakeholders and presents a range of tools to improve cyber-resilience.

Chapter 7 discusses the need for information sharing and the role of securities regulators. Information sharing is a useful way to emulate technical measures taken by other operators and prevent cyber-attacks. There are two basic types of information: technical/operational information, which can pass from computer to computer, and strategic information, which includes contextual background about threats or vulnerabilities. In general, governments have responsibility for promoting, facilitating and sharing information with the industry through information networks. Participants in the Montreal round-table meeting concluded that the most successful information came from the private sector although it is not always suitable for all classes of organisation. Information should be shared among regulators, something that IOSCO has been suggesting, particularly across different jurisdictions. In fact, under the IOSCO's MMoU, regulators can swap information on security breaches related to cyber-attacks. Members of the C4 have proposed such information exchange in cases of misselling, misappropriation of assets, market abuse, system disruption or sabotage. The MMoU provides for mutual support based on cross-border cooperation principles on matters such as the methods used by criminals, vulnerabilities, attack prevention techniques and trends in cyber risks.

Chapter 8 sets out general conclusions: i) cyber security is one of the biggest challenges facing markets and regulators; ii) the report provides a broad overview of the challenges associated with cyber security in securities markets from an international perspective; iii) there are a multitude of threats, including those associated with the use of cloud computing and data storage; iv) market agents are encouraged to adopt the measures and plans described and associated tools, guidelines and frameworks; v) disclosure of serious incidents involving cyber risks and cyber-attacks must be appropriate to the circumstances of each issuer, giving sufficient detail but not so much as to further compromise security; vi) it is essential to integrate cyber security within corporate governance and involve executives and directors; vii) cyber security should be included in risk management programmes; viii) it is important to share information both internally (participants-regulators in each market) and, especially, internationally, given the cross-border nature of cyber risks; and ix) organisations like IOSCO may be well placed to establish or promote ways of enhancing the exchange of information.

Finally, the report concludes by saying that the IOSCO Board is aware of the importance of security in the use of technologies affecting securities markets and their participants and therefore agreed to follow up this issue with the creation of a working group to develop recommendations and best practices in this field.

Link: Cyber Security in the Securities Markets – An international perspective