Cyber Security in Securities Markets – An International Perspective

Report on IOSCO's cyber risk coordination efforts

THE BOARD OF THE
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

FR02/2016	**APRIL 2016**

Copies of publications are available from:
The International Organization of Securities Commissions website www.iosco.org

Executive Summary

At its February 2014 meeting in Kuala Lumpur, the Board (IOSCO Board) of the International Organization of Securities Commissions (IOSCO) decided to investigate how IOSCO can further support its members and market participants in enhancing cyber security in securities markets. The IOSCO Board recognized that cyber risk constitutes a growing and significant threat to the integrity, efficiency and soundness of financial markets worldwide. In view of the fact that this threat impacts many different components of securities markets, and to ensure a coherent and efficient use of IOSCO's resources, a board-level coordinator was consequently nominated (namely the Quebec AMF with the assistance of the China Securities Regulatory Commission and the Monetary Authority of Singapore) to coordinate and guide the work otherwise conducted by various IOSCO Policy committees and other stakeholders on cyber security issues.

This report is the result of that coordination effort. It brings together the contribution of relevant IOSCO Policy committees, under the aegis of the IOSCO Board, and related stakeholders to cover the main regulatory issues and challenges related to cyber security for relevant segments of securities markets. The report is targeted at IOSCO members as well as market participants in securities markets.

For IOSCO member organizations, the report provides an overview of some of the different regulatory approaches related to cyber security that IOSCO members have implemented thus far. As the examples in the report demonstrate, regulators are generally still in the early stages of developing policy responses in the area of cyber security. This review of potential tools available to regulators can serve as a valuable point of reference to IOSCO members as they consider policy responses appropriate to the specific markets they regulate. For market participants, the report outlines various plans and measures participants have put in place to enhance cyber security in terms of identification, protection, detection, response and recovery. In doing so, the report describes some of the practices adopted by market participants and aims to encourage, where appropriate, the adoption of those or similar practices. Given that the cyber security landscape is constantly evolving, it is important to note that cyber security practices will undoubtedly change and evolve over time.

The report is organized around the relevant segments of the securities markets, namely: reporting issuers; trading venues; market intermediaries; asset managers; and financial market infrastructures. For these segments, the report discusses some of the main regulatory issues and challenges related to cyber security and highlights examples of approaches adopted by

market participants and regulators.[1] The report also discusses issues related to cooperation and the sharing of information among market participants and regulators.

Cyber risk: Definitions and the need for a focused, collaborative approach

While there is still a certain level of ambiguity concerning the various terminologies associated with cyber risk, agreement on some definitions is beginning to solidify. In essence, cyber risk refers to the potential negative outcomes associated with cyber attacks. In turn, cyber attacks can be defined as attempts to compromise the confidentiality, integrity and availability of computer data or systems.[2] And for the purpose of this report, cyber security is understood as a very broad concept, which encompasses all of the important activities associated with mitigating cyber risk, namely to identify, protect, detect, respond, and recover from cyber attacks.

Data on cyber attacks are often partial and of varying quality, particularly at a global level. Nonetheless, all available evidence makes clear that cyber attacks are becoming more frequent and more costly for organizations and societies more broadly. And the financial sector is one of the prime targets of cyber attacks.[3] It is easy to understand why: the sector is "where the money is" and it can represent a nation or be a symbol of capitalism for some politically motivated activists.

In many respects, cyber risk is not "just another risk." Cyber risk is a highly complex and rapidly evolving phenomenon. And the human element of cyber risk, combined with rapidly evolving technologies, gives it some unique characteristics: as organizations upgrade their defenses, criminals continuously develop new and more complex approaches. Ultimately, in a highly interconnected and interdependent financial ecosystem, cyber attacks may have systemic implications for the entire financial system, and also affect over time the trust on which financial markets are built. For these and other reasons, regulators, market participants, and other stakeholders must work together to enhance cyber security in securities markets.

---

1 Note that a separate joint CPMI-IOSCO initiative was put in place to specifically address issues relating to financial market infrastructures and cyber resilience. The chapter of this report that relates to financial market infrastructures provides an overview of a draft guidance that was produced as part of this initiative.

2 See, for instance: Joint Staff Working Paper of the IOSCO Research Department and World Federation of Exchanges, *Cyber-crime, Securities Markets and Systemic Risks*, 16 July 2013, which defines cyber-crime as "an attack on the confidentiality, integrity and accessibility of an entity's online/computer presence or networks – and information contained within."

3 Among other similar reports, the Verizon's Data Breach Investigations Report consistently ranks the financial sector among the top three industries affected by security incidents.

What securities regulators can do

Across the world, governments and financial authorities are taking important steps to mitigate cyber risks in financial markets. Reflecting the growing importance of cyber risk, cyber security is now governed in many countries by securities regulations and technical requirements that regulated entities are expected to comply with. The scope and depth of the regulatory responses do vary importantly among countries, reflecting the varying nature of financial markets, existing legislation and regulatory remit; some have put in place few or no such regulations or requirements. Overall, regulatory approaches tend to be high-level and allow for flexibility, recognizing that there is no "one size fits all" approach that market participants should adopt.

In many instances, regulated entities are expected to have appropriate risk management systems in place to minimize their exposure to cyber risks, by, for instance, implementing adequate physical and electronic security arrangements, ensuring compliance with financial stability standards, notifying appropriate authorities of incidents, and having appropriate protections for electronic trading.

However, the approaches used to achieve these regulatory objectives do differ among jurisdictions. Some jurisdictions have specific regulatory requirements regarding cyber security, while others have non-regulatory requirements relating to cyber security that are for instance part of self-regulatory governance rules, risk control systems procedures or guidelines regarding information and cyber security. Where regulatory requirements do exist, they vary across jurisdictions and financial authorities.

Regulators do indeed play a variety of roles and have adopted various tools in order to help enhance the cyber security frameworks of market participants. Amongst other tools, regulators have chosen to raise awareness levels regarding cyber security through the use of examination sweeps and the issuance of guidance, guidelines or frameworks. Furthermore, regulators have initiated and coordinated drills simulating cyber events and breaches involving all stakeholders including SROs, trading venues, financial market infrastructures, and various market participants.

While it is understood that each regulator operates in different institutional and market environments, the review of regulatory initiatives contained in this report highlights a number of avenues that could be considered for adoption by other IOSCO members.

Disclosure by reporting issuers

The report highlights the need for reporting issuers to rely appropriately on the existing disclosure framework to ensure that investors receive material information, including as it relates to cyber risk. Based notably on a review of issuer disclosure practices, the following have been identified among the factors that issuers might consider when preparing their disclosure, if they have determined that cyber risk is a material risk, and which IOSCO members may take into account when considering issuer disclosure in their jurisdictions:

- the reasons why the issuer is subject to cyber risk;
- the source and nature of the cyber risk, and how the risk may materialize;
- the possible outcomes of a cyber incident, for example:
  - effects on the issuer's reputation and customer confidence;
  - effects on stakeholders and other third-parties;
  - costs of remediation after a breach;
  - litigation, whether brought by parties seeking damages against the issuer or by the issuer against third parties;
  - effects on the issuer's internal and disclosure controls;
- the adequacy of preventative measures and management's strategy for mitigating cyber risk; and
- whether a material breach has occurred previously and how this affects the issuer's overall cyber risk. (A previous material breach might need to have been disclosed in accordance with disclosure requirements in a member jurisdiction.)

Disclosure of material risks should be tailored to the circumstances of the individual issuer. Although issuers should provide sufficient detail to describe the nature and potential consequences of a particular risk, or of a previous cyber attack, they should achieve the appropriate information balance without disclosing information that would compromise their cyber security.

Market participant practices to enhance cyber security

The report also provides descriptions of some current cyber security practices adopted by securities market participants as well as of emerging trends and approaches in cyber security.[4] Among other sources, the information is derived from answers received in a survey by IOSCO's Affiliate Members Consultative Committee (AMCC) and from the input of various IOSCO and AMCC working groups that were put in place specifically for this

[4] The term "securities market participants" solely as used in this report refers to a broad range of participants, entities, and securities and derivatives markets that include trading venues, market intermediaries such as broker-dealers, and asset managers.

initiative. Regulated entities and other market participants should consider to what extent such practices might be appropriate given their own cyber security objectives and risk tolerance. As both cyber security practices and threats are continuously evolving, the list of elements to consider by market participants will also likely evolve over time.

Identification. Appropriate governance is at the heart of any effective cyber security framework. The governance structure established by market participants to deal with cyber security issues, including the involvement of senior management and company boards, is paramount for the effectiveness of the overall information security framework. It helps organizations focus attention, determine their risk appetite and priorities and allocate resources to cyber security. Cyber security should be an integral part of a regulated entity's risk management program. A key component of the risk management program is the identification of critical assets, information and systems, including order routing systems, risk management systems, execution systems, data dissemination systems, and surveillance systems. Practices supporting the identification function include the establishment and maintenance of an inventory of all hardware and software. This risk management program should also typically include third-party and technology providers' security assessments. Finally, accessing information about the evolving threat landscape is important in identifying the changing nature of cyber risk.

Protection. There are numerous controls and protection measures that regulated entities may wish to consider in enhancing their cyber security. Such measures can be organizational (like the establishment of security operations centers) or technical (like anti-virus and intrusion prevention systems). Risk assessments help determine the minimum level of controls to be implemented within a project, an application or a database. In addition, employee training and awareness initiatives are critical parts of any cyber security program, including induction programs for newcomers, general training, as well as more specific training (for instance, social engineering awareness). Proficiency tests could be conducted to demonstrate staff understanding and third party training could also be organized. Other initiatives which contribute to raising employees' awareness of cyber security threats include monthly security bulletins emailed to all employees, regular communications regarding new issues and discovered vulnerabilities, use of posters and screen savers, and regular reminders sent to employees. Mock tests can also be conducted to assess employees' preparedness. Employees are also often encouraged to report possible attacks.

Detection. External and internal monitoring of traffic and logs generally should be used to detect abnormal patterns of access (e.g. abnormal user activity, odd connection durations, and unexpected connection sources) and other anomalies. Such detection is crucial as attackers can use the period of presence in the target's systems to expand their footprint and their

access gaining elevated privileges and control over critical systems. Many regulated entities have dedicated cyber threat teams and engage in file servers integrity and database activity monitoring to prevent unauthorized modification of critical servers within their organization's enterprise network. Different alarm categories and severity may be defined. In terms of monitoring, the latest trend is to combine organizational Security Information and Event Management (SIEM) tools (covering the organization's own security events) with relevant (sector-specific) threat intelligence services. Such a combination is aimed at ensuring greater proactivity in the identification of and response to changing cyber threats.

Response. Regulated entities generally should consider developing response plans for those types of incidents to which the organization is most likely to be subject. Elements associated with response plans may include: preparing communication/notification plans to inform relevant stakeholders; conducting forensic analysis to understand the anatomy of a breach or an attack; maintaining a database recording cyber attacks; and conducting cyber drills, firm-specific simulation exercises as well as industry-wide scenario exercises.

Recovery. Following a cyber security event, it is important for regulated entities to have plans in place to restore any capabilities or services that were impaired. Regulated entities generally should consider defining recovery time and recovery point objectives. Such objectives may vary depending on the particulars of a firm or the industry in which it operates. For instance, the recent CPMI-IOSCO draft Guidance for Financial Market Infrastructures (FMIs) proposes that FMIs should design and test their systems and processes to enable the safe resumption of critical operations within two hours of a cyber disruption.[5] Such a prompt objective may not necessarily be needed for other types of market participants. As with response planning, conducting regular drills is important to assess the effectiveness of the recovery planning, and to make necessary improvements. Finally, the recovery function should include a communication component with internal and external stakeholders (for instance, for public relations).

Information sharing among regulators and market participants

Finally, the report considers issues surrounding the importance of sharing information related to cyber security among market participants and regulators. Information sharing provides numerous benefits by notably allowing organizations to tap into a broader community's intelligence, capabilities, knowledge and experience related to cyber security.

[5] See CPMI-IOSCO, Consultation Report on *Guidance on cyber resilience for financial market infrastructures*, at https://www.iosco.org/library/pubdocs/pdf/IOSCOPD513.pdf. Proposed guidance has been published for consultation in November 2015, with a potential final report slated for 2016. As such, the content of the Guidance is still subject to changes before final publication. For more details on the proposed guidance, please refer to Chapter 6.

Securities regulators can also benefit from information sharing. Such information can provide regulators with more information on the types of threats faced by market participants, on their cyber security practices, and on their general level of preparedness. Ultimately, this information can potentially be helpful in ensuring that rules, regulations, and supervisory activities are effective and appropriate.

As part of their regulatory framework, securities regulators may want to require or encourage some or all market participants to participate in information sharing networks or initiatives, taking into consideration the participants' capacity or technological sophistication to process and act on the information received. And legal issues regarding information sharing, ranging from data and privacy protection issues, liability protection matters to potential antitrust concerns, remain a challenge in many countries.

Given the international nature of cyber risk, there is a widespread recognition that information sharing at the international level is also essential. Some privately led initiatives are starting to cross national borders, but important challenges remain due notably to the fact that hurdles – legal, operational, or otherwise – are particularly acute at the international level.

Information exchange among regulators is also considered by many to be necessary at the international level. Under IOSCO's Multilateral Memorandum of Understanding (MMoU), regulators can exchange information concerning a securities related offence involving a cyber attack. The MMoU is sufficiently flexible in allowing assistance to be sought when investigating breaches of securities laws, which involve cyber crime. This assertion is supported by the Objectives of securities regulation and by the IOSCO Principles relating to cooperation, which stress the importance of cooperation channels in cross-border enforcement cases and for other regulatory purposes.

Over and beyond information related more narrowly to enforcement actions, the exchange of information among regulators on cyber risk more broadly would be beneficial given their responsibilities to ensure that markets are fair, efficient and transparent and to reduce systemic risk. To the extent that some regulators require disclosure of cyber attacks from regulated entities, and that they might otherwise gather information on cyber risk in the conduct of their regulatory and supervisory responsibilities, regulators might benefit from greater cross-jurisdiction information sharing.

Contents

Chapter 1 – Introduction

The increasing and pervasive use of technologies within modern economies brings both risks and rewards. The benefits are manifold and obvious to most: products and services that can be delivered at lower costs and that exhibit many of the attributes desired by consumers such as convenience, speed and reliability, to name just a few. Securities markets, by their very nature, are at the forefront of technology developments. For instance, the trading of securities occurs essentially through purely electronic systems, and at speeds unparalleled to those involving human interactions.

Technologies, of course, are also associated with risks. The failure of an important electronic system can generate ripple effects affecting participants beyond those directly involved, threatening in some instances the stability of entire financial systems or economies. These risks have long been recognized and various safeguards have been put in place over the years, including various regulatory frameworks. These safeguards have traditionally been focused on ensuring the resilience of systems from the occurrence of various technological glitches. There has historically been less focus, however, on failures or incidents that might originate from malicious intent, generally referred to as cyber attacks. The risks associated with these types of attacks in securities markets are the subject of this report.

The impetus for this report is the explicit recognition by the IOSCO Board that cyber risk constitutes a growing and significant threat to the integrity, efficiency and soundness of financial markets worldwide. At its February 2014 meeting in Kuala Lumpur, the IOSCO Board decided to investigate further how IOSCO can support its members and market participants in enhancing cyber security in securities markets. Cyber risk is a highly complex and rapidly evolving phenomenon for which standard risk management techniques may be considered insufficient. And the potentially systemic nature of this risk militates in favor of a targeted regulatory response.

In that context, this report aims to cover the main regulatory issues and challenges related to cyber security for all the relevant segments of securities markets. To achieve that goal, the report brings together the contribution of the various IOSCO Policy committees and related stakeholders – notably the Committee on Payments and Market Infrastructures (CPMI) and the AMCC, – each covering a different but related aspect of cyber security and of securities markets. More specifically, the following IOSCO Policy committees, under the aegis of the IOSCO Board, contributed to this report:

- Committee 1: Issuer Accounting, Auditing and Disclosure;
- Committee 2: Regulation of Secondary Markets;
- Committee 3: Regulation of Market Intermediaries;
- Committee 4: Enforcement and the Exchange of Information and the Multilateral Memorandum of Understanding Screening Group; and
- Committee 5: Investment Management.

The report also leverages other projects (including, but not limited to, IOSCO projects), notably surveys and other work related to the robustness of electronic trading systems and markets and to the business continuity and recovery for trading venues and intermediaries. The *Autorité des marchés financiers* (AMF) Quebec, with the assistance of the China Securities Regulatory Commission (CSRC) and the Monetary Authority of Singapore (MAS), was responsible for the overall coordination effort for the report (henceforth, collectively referred to as IOSCO Cyber Risk Coordinators).

The report is targeted at IOSCO members as well as market participants in securities markets. For IOSCO member organizations, the report provides an overview of some of the different regulatory approaches related to cyber security that IOSCO members have implemented thus far. As the examples in the report demonstrate, regulators are generally still in the early stages of developing policy responses in the area of cyber security. This review of potential tools available to regulators can serve as a valuable point of reference to IOSCO members as they consider policy responses appropriate to the specific markets they regulate.

For market participants, the report outlines various plans and measures participants have put in place to enhance cyber security in terms of identification, protection, detection, response and recovery. In doing so, the report describes some of the practices adopted by market participants and aims to encourage, where appropriate, the adoption of those or similar practices.

The report is structured as follows. Chapter 2 provides an analysis of issues related to the disclosure of cyber security risks and incidents by reporting issuers. Chapter 3 depicts current cyber security practices at trading venues and associated regulatory approaches. Chapter 4 discusses cyber security in the context of market intermediaries, while Chapter 5 focusses on asset managers. Chapter 6 discusses the work of the joint CPMI-IOSCO Working Group on Cyber Resilience (WGCR) that was established to address issues cyber risk may pose to the well functioning of Financial Market Infrastructures and to financial stability. Chapter 7 provides a discussion of information sharing related to cyber security and the role of securities regulators. Chapter 8 concludes.

1.1 What is cyber risk?

While there is still a certain level of ambiguity concerning the various terminologies associated with cyber risk, some definitions are beginning to solidify among the public and private sectors. In essence, cyber risk refers to the potential negative outcomes associated with cyber attacks. Cyber attacks can be defined as attempts to compromise the confidentiality, integrity and availability of computer data or systems.[6] In the more specific context of securities markets:[7]

- *Confidentiality*: An attack on confidentiality typically involves the unauthorized access to sensitive information such as customers' access credentials for trading accounts or corporate deal-making information. This information is then used to commit fraud or identity theft, by creating unauthorized buy and sell orders or to gain

[6] Source: CIA Triad

[7] Source: Mark G. Clancy (DTCC), Speech, House Committee on Financial Services, Subcommittee on Capital Markets and Government Sponsored Enterprises, Hearing on "Cyber Threats to Capital Markets and Corporate Accounts," June 1, 2012

an advantage in competitive negotiations. Other intellectual property assets such as proprietary algorithms may also be targeted.

- *Integrity*: An attack on integrity would involve affecting the accuracy or consistency of data or systems related to financial assets or personal information – which exist overwhelmingly only in digital form – by for instance changing the ownership information of a security or by simply destroying that information.
- *Availability:* An attack on availability would result in the disruption or delay of the orderly and efficient operation of capital markets by making related systems, such as those that facilitate the execution of trades, unavailable when needed, many of which normally operate on a real-time basis.

The National Institute of Standards and Technology (NIST)'s Glossary of Key Information Security Terms provides the following definition for a cyber attack, which overlaps the concepts mentioned above:[8]

> "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information. Source: CNSSI-4009" [9]

Cyber attacks can be performed by a number of different actors, presenting different types of motivations and levels of capabilities. There are essentially four types of so-called "threat actors:"[10]

- *Criminals*: The motivation of this group is financial gains generated by the stealing of money or information that can be sold. This group is very disparate in terms of capabilities, with large numbers of actors present in numerous countries, including some that have very high levels of sophistication and access to sophisticated cyber crime markets.
- *Hacktivists*: This group's motivation is to promote political or ideological points of view through targeted attacks that can cause reputational or financial damage to firms or entities. In general, most have capabilities that tend to be more limited in terms of skill-sets.
- *Nation-states and terrorist organizations*: Nation-states can typically aim to gain an economic and competitive advantage by stealing intellectual property. They, along with terrorist groups, can also aim to destroy the cyber capabilities of other governments or corporations in the context of a conflict or a war. There are relatively few actors in this space, but they tend to have very sophisticated skills and access to large amounts of resources.

---

8 The National Institute of Standards and Technology is a non-regulatory agency of the United States Department of Commerce.

9 http://www.nist.gov/customcf/get_pdf.cfm?pub_id=913810

10 Source : The Securities Industry and Financial Markets Association, *SIFMA's Guidance for Small Firms: How Small Firms Can Protect Their Business*, July 2014

- *Insiders*: This group includes current or former employees, as well as outside parties colluding or misusing their access privileges. Those trusted insiders may have financial or other (e.g., revenge) motivations.

1.1.1 Cyber security: mitigating cyber risk

Relatedly, cyber security refers in general terms to the ability to protect against cyber attacks and to recover from them. In one of its reports, CPMI describes in more detail that cyber security includes "strategies, policies and standards encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resilience, and recovery activities and policies".[11]

In the more specific context of the securities industry, the Financial Industry Regulatory Authority (FINRA), a self-regulatory organization under the US securities laws, provides the following definition for cyber security:

> "FINRA takes a broad view and defines cyber security as the protection of investor and firm information from compromise through the use—in whole or in part—of electronic digital media (e.g., computers, mobile devices or Internet protocol-based telephony systems). "Compromise" refers to a loss of data confidentiality, integrity or availability."[12]

For the purpose of this report, cyber security is understood as a very broad concept, which encompasses all of the important activities associated with mitigating cyber risk, namely to identify, protect, detect, respond, and recover from cyber attacks.[13] As such, this definition does not only cover protective measures, but also those aimed at promoting resilience in the event of a successful cyber attack.

In short, cyber security aims at mitigating the occurrence and the impact of cyber risk. In some instance, the term "cyber resilience" is used somewhat interchangeably, although this term does put more emphasis on the ability to recover from a cyber attack. For instance, the CPMI-IOSCO draft Guidance defines cyber resilience as the "ability to anticipate, absorb, adapt to, rapidly respond to and recover from disruption caused by a cyber attack."[14]

Like any risk, cyber risk can be understood as the combination of certain vulnerabilities – in this case susceptibility or insufficient defenses related to information systems – and of a trigger event – in this case a cyber attack. Organizations often have little control over the occurrence of a cyber attack. But they do have a more direct influence on their vulnerabilities.

---

[11] Committee on Payments and Market Infrastructures, *Cyber resilience in financial market infrastructures*, November 2014, page 14

[12] The Financial Industry Regulatory Authority, *Report on Cybersecurity Practices*, February 2015, Page 3. FINRA is a private corporation that acts as a self-regulatory organization (SRO) in the United States.

[13] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, 12 February 2014

[14] Committee on Payments and Market Infrastructures and the Board of the International Organization of Securities Commissions, Consultative Report on proposed draft *Guidance on Cyber Resilience for Financial Market Infrastructure*, November 2015.

Vulnerabilities associated with cyber risks are often technological in nature, for instance those related to legacy software that lack sufficient security support. But these vulnerabilities also frequently relate to people and processes. People are often the "weakest link" when there is not an appropriate level of awareness of cyber risks within an organization. Further, deficiencies in decision-making processes within organizations can also be a source of vulnerability that can be exploited by cyber criminals, for instance lack of clear accountability processes. As a consequence, effective cyber security includes measures that typically address not only technology issues, but also those related to both people and processes.

1.2 Why this report?

1.2.1 Cyber risk: a growing threat

Data on cyber attacks are often partial and of varying quality, particularly at a global level, due notably to the fact that many organizations are reluctant to disclose cyber attacks for reputational concerns, while others may be unaware that an attack even took place. Hence, available statistics may underestimate the extent of cyber attacks. Nonetheless, all available evidence makes clear of the following trend: cyber attacks are becoming more frequent and more costly for organizations and societies more broadly.

According to PwC's Global State of Information Security Survey 2016, – which collected responses from more than 10,000 executives from 127 countries – the total number of security incidents detected by respondents in 2015 was up 38% compared to 2014. According to previous Global State of Information Security Surveys, security incidents have increased 66% on average from year to year from 2009 to 2014. For 2015, around 10% of respondents estimated total financial losses associated with all their security incidents to represent USD$10 million dollars or more.

Cost estimates can vary widely depending on methodologies and scope, but they all tend to show these costs to be on a growing trend. The Ponemon Institute's 2015 Cost of Data Breach Study: Global Analysis, sponsored by IBM, pegs the average cost of data breaches to a company at USD$3.79 million dollars, a 23 percent increase over the past two years. The Center for Strategic and International Studies estimated in 2014 that the likely annual cost to the global economy from cyber crime is more than USD$400 billion.[15]

Another trend is clear: the financial sector is one of the prime targets of cyber attacks. It's easy to understand why: the sector is "where the money is" and it can represent a nation or be a symbol of capitalism for some politically motivated activists. Among other similar reports, the Verizon's Data Breach Investigations Report consistently ranks the financial sector among the top three industries affected by security incidents.[16] According to many cyber security experts, the question for financial market participants is not if a cyber attack will occur, but rather when.

---

[15] Center for Strategic and International Studies (sponsored by McAfee , part of Intel Security), "*Net Losses : Estimating the Global Cost of Cybercrime*," June 2014

[16] See: http://www.verizonenterprise.com/DBIR/

Examples highlighting the varying nature of cyber threats in securities markets

Attacks on stock exchanges' websites: In 2011, the Hong Kong stock exchange was forced to halt trading in the shares of some companies after a cyber attack on its website deprived investors of important announcement from listed companies.[17] In 2012, a wave of distributed denial-of-service (DDoS) attacks, which flood websites with unwanted traffic, targeted a number of U.S. stock exchanges. The attacks caused accessibility issues, although trading systems were not affected. The Warsaw Stock Exchange's website was also temporarily paralyzed by a cyber attack in 2014, reportedly leading to login credentials for dozens of brokers being exposed.

CME Group attack: In July 2013, the CME Group was the victim of a cyber attack. The exchange indicated that certain customer information relating to the CME ClearPort platform had been compromised. The exchange also indicated in public documents that they had incurred expenses of USD$16 million related to their response to the event.[18]

Trading on hacked news releases: In August 2015, the U.S. Securities and Exchange Commission charged defendants in a scheme to trade on hacked news releases from three news wire services, with hackers and traders allegedly having reaped more than USD$100 million of illegal profits.[19]

Internal threats: In early 2015, Morgan Stanley fired one of its financial advisers after it accused him of stealing account data on about 350,000 clients and posting some of that information for sale online, although there was no evidence of economic loss.

"Pump-and-dump" scheme: According to a complaint filed by the SEC, it charged an individual with repeatedly hijacking online brokerage accounts and placing unauthorized trades. The SEC alleged that through these trades, the individual would "pump up" the price of thinly traded stocks, and subsequently would sell the same stocks at an artificially elevated price for its own benefit.[20]

SQL injection attack: According to FINRA, in one instance where it took enforcement action, FINRA alleged that a firm's database was hacked using a SQL injection attack,[21] giving access to confidential information of more than 200,000 customers, including names, account numbers, Social Security numbers, addresses and dates of birth.[22]

---

17 The Financial Times, *Hong Kong exchange hit by hackers*, 10 August 2011, http://www.ft.com/intl/cms/s/0/f448a9b6-c33a-11e0-9109-00144feabdc0.html#axzz3Xr9ioFXw

18 Chicago Mercantile Exchange, *CME Group Confirms Cyber Intrusion*, 15 November 2013, http://investor.cmegroup.com/investor-relations/releasedetail.cfm?ReleaseID=807750. See also CME, *Annual Report 2013*.

19 http://www.sec.gov/news/pressrelease/2015-163.html

20 U.S. Securities and Exchange Commission v Broco Investments, Inc. and Valery Maltsev, Civil Action no. 10-CIV-2217 (S.D.N.Y.)

21 A Structured Query Language (SQL) injection attack is a technique in which an SQL query is used to try and extract information from a database.

22 The Financial Industry Regulatory Authority, *Report on Cybersecurity Practices*, February 2015, Page 8

A survey of 46 securities exchanges conducted by IOSCO and the World Federation of Exchanges (WFE) Office found that more than half (53%) had experienced a cyber attack.[23] According to a U.S. Securities and Exchange Commission Office of Compliance Inspections and Examinations staff's Cybersecurity Examination Sweep Summary published in February 2015, a majority of broker-dealers (88%) and advisers (74%) stated that they have experienced cyber attacks directly or through one or more of their vendors.[24]

Factors that have underpinned the rise in cyber attacks in securities markets are multiple. And these factors are expected to persist, and in some instances gain in importance, suggesting that the growth in cyber attacks is a trend that will not abate any time soon, and that may even accelerate in the future.

Above all, the almost complete digitalization of data within the securities industry is well underway, and there is no reason to believe that this trend will not continue in the future. This creates potential opportunities for cyber criminals, and raises the need to ensure the integrity of financial data. There are other long-term trends within the financial industry, such as the increasing use of mobile devices, outsourcing and cloud computing, that introduce additional vulnerabilities to cyber attacks.

In short, available evidence suggests that cyber risk has become more prevalent and may become more so in the foreseeable future. For securities markets, this growth in cyber risk poses an increasing threat for market efficiency, investor protection, and ultimately confidence in financial markets. As the global standard setter for the securities sector, IOSCO is taking an active role in enhancing cyber security in securities markets and in promoting cooperation at the international level. This report adds to this effort.

1.2.2 Why is cyber risk "special"?

Some have argued that cyber risk, in spite of its growing importance, is "just another risk". There are however a number of arguments that militate in favor of adopting a specific approach to addressing this risk. First, as argued by CPMI in its report on cyber resilience, cyber risk is a relatively new, highly complex and rapidly evolving phenomenon. The human element of cyber risk, combined with rapidly evolving technologies, gives it some unique characteristics: as organizations upgrade their defenses, criminals continuously develop new and more complex approaches.[25]

The sophistication of some cyber-attacks, coupled with the varied motivations behind these attacks, create some unique challenges for market participants. The detection of an attack itself can be challenging, as well as the assessment of potential damages. And existing industry protocols and regulations may, in certain circumstances, be ineffective in addressing cyber risk. For instance, switching to a backup data center, as would be warranted in a physical attack, may not be effective if doing so would lead to further contamination of data.

---

23 http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf

24 http://www.sec.gov/about/offices/ocie/cyber security-examination-sweep-summary.pdf

25 See, for instance: Autonomous Research LLP, *Cyber risk – the stuff of nightmares*, 22 April 2015

As argued elsewhere, cyber risk can be systemic in nature.[26] A cyber attack could produce important ripple effects affecting entire financial systems and the broader economy.[27] Given the critical and interconnected nature of the financial system, the Depository Trust & Clearing Corporation (DTCC) has identified cyber risk as "arguably the top systemic threat facing not only the global financial markets and associated infrastructures, but also world governments and military establishments" in its 2013 Systemic Risk White Paper.[28] According to its analysis, cyber attacks could cause important market disruption by preventing business transactions or by deleting, modifying or corrupting books and records of the financial industry.

For instance, if a clearing and settlement organization were to fail to perform its essential functions as a consequence of a cyber attack, investors would be unable to know with certainty if trades will be or have actually been executed and therefore what securities they actually own, or how much capital they have; on a large scale, such uncertainty could quickly spread to large parts of the financial market. If the failure were to persist, liquidity and access to capital could be negatively affected. Cyber attacks could also cause market disruption by potentially leading to the disclosure of restricted and non-public confidential data.

Relatedly, the IOSCO and WFE survey on cyber risk found that a majority of exchanges (89%) view cyber crime in securities markets as a potential systemic risk, citing the possibility of massive financial and reputational impacts; loss of confidence; effects on market availability and integrity; the interconnectedness and dependencies in securities markets; and related knock-on effects on market participants from an attack.

IOSCO's Committee on Emerging Risks (CER), together with the IOSCO Secretariat's Research Department, have identified cyber risk as an important and potential systemic risk in its 2015-2016 Securities Markets Risk Outlook.

In short, if cyber attacks were to occur on a large scale, they could have immediate systemic implications for entire financial systems, and also affect over time the trust on which financial markets are built. In turn, a systemic risk typically invites some form of government or regulatory response. The reasoning is as follows: systemic risks, according to economic theory, typically involve externalities; meaning that an individual firm's actions can have impacts on others participants and the rest of the financial system. Hence, firms, individually and as a whole, may not necessarily put in place levels of cyber security that might otherwise be beneficial for the broader financial system.

---

[26] See for instance: IOSCO/WFE, *Cybercrime, Securities Markets and Systemic Risk*, Joint Staff Paper, July 2013

[27] According to the IMF/BIS/FSB, "Systemic risk is the risk of disruption to financial services that is (i) caused by an impairment of all or parts of the financial system and (ii) has the potential to have serious negative consequences for the real economy." Source: International Monetary Fund, the Bank for International Settlements, and the Financial Stability Board, *Guidance to Assess the Systemic Importance of Financial Institutions, Markets and Instruments: Initial Considerations*, October 2009

[28] *Beyond the Horizon White Paper Systemic Risk.ashx*

1.3 Overview of recent national initiatives by IOSCO members

Before exploring in greater detail the various components of securities markets, below is an overview of some recent initiatives implemented by IOSCO members that apply broadly to the securities markets they oversee. This is by no means an exhaustive review of the various initiatives put in place around the globe. It does however provide examples of approaches adopted in some jurisdictions and that other regulators may want to consider.

1.3.1 Steps taken in Australia

In March 2015, ASIC published Report 429 Cyber resilience: Health Check (REP 429) to assist its regulated population prepare, respond, adapt and recover from a cyber attack.[29]

Report 429 highlights the importance of cyber resilience to ASIC's regulated population, to support investor and financial consumer trust and confidence and ensure markets are fair, orderly and transparent.

This Report outlines some "health check prompts" to help businesses review their cyber resilience—including flagging relevant legal and compliance requirements, particularly on risk management and disclosure.

The health-check prompts cover:

- Governance;
- Identifying essential business information and assets;
- Potential exposure to cyber risks;
- Resilience of third party providers and clients;
- Current arrangements, policies and procedures;
- Testing existing information technology (IT) systems, processes and procedures for cyber resilience;
- Resources to deal with cyber risks, including properly trained staff (employees and contractors);
- Monitoring processes and procedures to detect a cyber attack;
- Response planning and reporting;
- Communications with customers;
- Recovery plans; and
- Legal and regulatory obligations.

ASIC is also encouraging businesses, particularly where their exposure to a cyber attack may have a significant impact on financial consumers and investors or market integrity, to consider using the United States' NIST Cybersecurity Framework to manage their cyber risks or stock-take their risk management practices.

ASIC is also incorporating cyber resilience in its surveillance programs, across its regulated population. In the markets area this means focusing on the cyber resilience of financial market infrastructure, investment banks and market participants.

[29] Available at: http://asic.gov.au/regulatory-resources/find-a-document/reports/rep-429-cyber-resilience-health-check/

1.3.2 Steps taken in Singapore

The Monetary Authority of Singapore (MAS) recognizes the need to address cyber security risks to safeguard the operations of its financial institutions. In this regard, MAS has issued a set of Technology Risk Management Notice and Guidelines. These regulations and guidelines seek to address the increased technology risks, including cyber security risks, which financial institutions face in the current operating environment.

In particular, the Technology Risk Management Notice requires financial institutions to implement IT controls to protect customer information from unauthorised access or disclosure as well as to establish a recovery time objective of not more than 4 hours for each critical system. Financial institutions are to further ensure that the downtime of critical systems, excluding scheduled maintenance periods, does not exceed a total of 4 hours within any 12-month period. In the event of any IT security incidents, financial institutions are required to report the incident to MAS within 1 hour upon discovery. Subsequently, they are to submit a root cause and impact analysis within 14 days of the incident.[30]

The Technology Risk Management Guidelines sets out more detailed sound practices to address the various technology risks that financial institutions may face. Amongst other areas, the security of financial institutions' IT infrastructure is an area addressed in the Technology Risk Management Guidelines. Some of the sound practices to address and contain cyber security threats to IT infrastructure include:

- The development of a comprehensive data loss strategy to protect sensitive or confidential information and prevent data loss through the use of encryption, encrypted channels and strong access controls;
- The establishment of a technology refresh plan to ensure that the IT infrastructure is up-to-date, thus reducing security risk arising from outdated and unsupported systems and software;
- Effective security management of IT systems and devices through the use of network security devices and anti-virus software to ensure appropriate levels of protection;
- The detection of security vulnerabilities in the IT environment through the conduct of vulnerability assessments;
- The establishment of proper security patch management procedures to ensure timely and effective implementation of security patches; and
- The establishment of appropriate security monitoring systems and processes to facilitate prompt detection of cyber attacks.[31]

---

[30] Full details of the TRM Notice can be viewed at the following links below:

http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/IID%20Notices/Notice%20CMGN02_2014.pdf

[31] Other sound practices addressing areas such as system reliability, availability and recovery are also set out in the TRM Guidelines and these can be viewed at:

http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf

1.3.3 Steps taken in the United Kingdom

The Financial Conduct Authority (FCA) is of the view that traditional risk management methodologies may be challenged by cyber threats. The management of cyber risks requires a broad understanding of these threats and their effects. The FCA, however, does not consider prescriptive regulation as a suitable response to cyber risk concerns because the constant evolution of the threats would render much of the detailed prescription obsolete in a very short period of time.

While some existing voluntary standards for cyber security are viewed as good technical control guides, the FCA places greater emphasis on the governance and leadership aspects of managing this risk. The FCA found that business continuity solutions are often insufficient for cyber risk challenges. The FCA's expectations regarding cyber resilience change with the scale, nature and complexity of a firm. Within the field of industry engagement, the presence of the FCA, as the regulator, is seen by many to inhibit the free flow of information and some firms have voiced competition concerns about the sharing of information related to cyber threats.

The FCA applies some measures in addressing cyber risks like internal cyber incident response procedures and notification to the regulator in the event of a cyber incident. UK organizations are also working together to put in place a program to improve and test resilience to cyber attacks. Additionally, the FCA (along with the Bank of England and Her Majesty's Treasury collectively known as the Authorities) has established a work plan, with the following steps:

- The Authorities are aligned and have implemented processes that will allow them to receive critical updates from UK government agencies in the event of a major incident. Following a major incident, information will be shared with the FCA where it will be analysed and reported to firms' supervisory teams for subsequent bilateral engagement;
- A comprehensive cyber-questionnaire has been sent to the 36 firms identified as "the core UK financial system." The outcomes of this questionnaire have resulted in specific action plans being issued to firms to strengthen their cyber defences;
- Two cyber resilience tests were conducted: one by launching the CBEST penetration testing framework alongside the Bank of England which replicates behaviours of threat actors to provide authentic, intelligence led penetration tests on financial firms and a second with the Waking Shark II exercise testing the cyber response arrangements of 21 high impact firms, the regulators and the government; and
- Information sharing has to be improved, in particular by providing firms with a platform where they will be sharing strategic information relating to current threats. The UK operates the CISP platform for the sharing of tactical and operational information.

1.3.4 Steps taken in the United States

On 26 March 2014, the Securities and Exchange Commission (SEC) hosted a roundtable at its Washington, D.C., headquarters to discuss cyber security and the issues and challenges it raises for market participants and public companies, and how they are addressing those concerns. The SEC's jurisdiction over cyber security is directly focused on the integrity of U.S. market systems, customer data protection, and disclosure of material information. As

noted by SEC Chair White at the roundtable, the SEC has been focused on cyber security-related issues for some time. For example, in connection with public company disclosures, in October 2011, staff in the SEC's Division of Corporation Finance issued guidance on issuers' disclosure obligations relating to cyber security risks and cyber incidents. That guidance makes clear that material information regarding cyber security risks and cyber incidents is required to be disclosed.

SEC staff continues to study the important and challenging issues that cyber security presents to public companies, market participants, and investors, including the intersection of U.S. investor-focused disclosure requirements and the types of information those with national security responsibility need in order to better protect critical infrastructure.

Cyber security for self-regulatory organizations (SROs) and large alternative trading systems also is a very important area of focus for SEC staff. Part of this focus involves the SEC's rule on Regulation Systems, Compliance and Integrity (Regulation SCI), approved on November 19, 2014, which requires an entity covered by the rule to have policies and procedures to test its automated systems for vulnerabilities, test its business continuity and disaster recovery plans, notify the SEC of cyber intrusions, and recover its clearing and trading operations within specified time frames.

Beginning in 2014, the SEC's Office of Compliance Inspections and Examinations (OCIE), as part of its "Cybersecurity Examination Initiative," conducted a series of examinations to identify cyber security risks and assess cyber security preparedness in the securities industry. These examinations were targeted at both registered investment advisers and broker-dealers. OCIE issued a Risk Alert in February 2015 summarizing observations and findings from an initial round of examinations.[32] OCIE issued a second Risk Alert in September 2015 identifying focus areas, such as testing of firms' systems and practices, for a subsequent round of examinations that remains ongoing.[33]

In addition, in April 2015, staff of the SEC's Division of Investment Management published guidance that emphasized the importance of cyber security to registered investment companies ("funds") and registered investment advisers ("advisers"). Investment Management staff noted that both funds and advisers increasingly use technology to conduct their business activities and need to protect confidential and sensitive information related to these activities from third parties, including information concerning fund investors and advisory clients. Investment Management staff listed a number of measures that funds and advisers may wish to consider in addressing cyber security risk, including the following:

- Conducting a periodic assessment of: (1) the nature, sensitivity and location of information that the firm collects, processes and/or stores, and the technology systems it uses; (2) internal and external cyber security threats to and vulnerabilities of the firm's information and technology systems; (3) security controls and processes currently in place; (4) the impact should the information or technology systems become compromised; and (5) the effectiveness of the governance structure for the management

[32] See *OCIE Cybersecurity Examination Sweep Summary*, February 3, 2015 at https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf

[33] See *OCIE's 2015 Cybersecurity Examination Initiative*, September 15, 2015 at https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

of cyber security risk. An effective assessment would assist in identifying potential cyber security threats and vulnerabilities so as to better prioritize and mitigate risk;

- Creating a strategy that is designed to prevent, detect and respond to cyber security threats. Such a strategy could include: (1) controlling access to various systems and data via management of user credentials, authentication and authorization methods, firewalls and/or perimeter defenses, tiered access to sensitive information and network resources, network segregation, and system hardening; (2) data encryption; (3) protecting against the loss or exfiltration of sensitive data by restricting the use of removable storage media and deploying software that monitors technology systems for unauthorized intrusions, the loss or exfiltration of sensitive data, or other unusual events; (4) data backup and retrieval; and (5) the development of an incident response plan. Routine testing of strategies could also enhance the effectiveness of any strategy; and

- Implementing the strategy through written policies and procedures and training that provide guidance to officers and employees concerning applicable threats and measures to prevent, detect and respond to such threats, and that monitor compliance with cyber security policies and procedures. Firms may also wish to educate investors and clients about how to reduce their exposure to cyber security threats concerning their accounts.

The Commodity Futures Trading Commission (CFTC) is of the view that cyber security is the most important single issue facing markets today in terms of market integrity and financial stability. Because of the interconnectedness of financial institutions and markets, an attack in one place can have serious repercussions throughout the system. In recognition of the importance of cyber security risks, the CFTC has responded in several ways. The CFTC has incorporated cyber security standards into its regulations, has required clearing houses and exchanges to maintain system safeguards and risk management programs, to notify the CFTC of incidents, and to have recovery procedures in place. The CFTC has made cybersecurity a priority in its examinations.

The CFTC recognizes that the responsibility for cyber security rests with private institutions and that as an agency it can set standards, engage in examinations, but it is up to the critical financial infrastructures to do the daily comprehensive work required. To that end, the CFTC's focus to date has been on systems testing and what constitutes effective and adequate risk analysis in testing by exchanges and clearing houses.[34]

[34] CFTC Staff Roundtable on Cybersecurity and System Safeguards Testing, Transcript, Mar. 18, 2015, available at http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/transcript031815.pdf.

Chapter 2 – Reporting issuer disclosure

To support IOSCO Cyber Risk Coordinators, IOSCO's Committee on Issuer Accounting, Audit and Disclosure (C1) performed a fact-finding exercise related to the disclosure of cyber security risks by reporting issuers. The work of C1 included an examination of IOSCO's issuer disclosure guidance and IOSCO member jurisdictions' disclosure frameworks in the context of cyber risks, as well as reporting issuers' current practices in disclosing cyber risks. Based on its work, C1 derived important observations relating to the principles and practices of issuer disclosure in the context of cyber risk.

2.1 Introduction

As digital technology plays an expanding role in the way that many issuers conduct their operations, the associated cyber risks that those issuers face also have increased. The impact of cyber risks on the operations of an issuer affects whether and how the issuer communicates them to investors. As issuers of public securities increasingly consider the effects of digital technology and cyber risk on their operations, they must consequently also consider what information concerning those effects they must disclose to investors in order to comply fully with applicable securities laws.

Issuers that conduct public offerings of their securities, or that issue securities that are publicly traded, are generally subject to disclosure requirements by securities regulators. Those disclosure requirements are established to protect investors by addressing the asymmetry of information about the issuer that exists between management and the investors. By having access to information about an issuer that is material, timely and not misleading, investors are better able to make informed decisions on whether to buy, sell or hold that issuer's securities. Information that is typically required to be disclosed under securities regulations includes a description of an issuer's business, financial condition, management, material risks, major shareholders, significant contracts, as well as other information that is material to investors' investment decisions.

2.2 IOSCO Issuer Disclosure Guidance

IOSCO has established over-arching principles of securities regulation related to an issuer's disclosure of information to investors who purchase its securities in the public capital markets.[35] These principles are primarily in support of IOSCO's objective of securities regulation related to investor protection. Principle 16, which pertains to issuer disclosure, stipulates that there should be "full, accurate and timely disclosure of financial results, risk and other information which is material to investors' decisions."

To assist securities regulators in implementing these over-arching principles, IOSCO has also developed standards and principles specific to the content of issuer disclosure relating to securities that are sold in the public capital markets. The IOSCO disclosure standards and principles, which are described below, provide guidance for use by securities regulators in establishing their national disclosure requirements for issuers with securities that are publicly offered and/or listed. IOSCO principles and standards are not self-executing; rather, they are prepared in order to assist domestic securities regulators in establishing disclosure

[35] See *International Organization of Securities Commissions Objectives and Principles of Securities Regulation*, June 2010, available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD323.pdf.

requirements in the context of their jurisdiction's regulatory framework. A key element for disclosure under the IOSCO principles relates to risk factors.

IOSCO has developed two sets of issuer disclosure standards and principles for prospectuses used in cross-border offerings and listings of securities in the public capital markets; namely, the *International Debt Disclosure Principles*[36] (debt principles) and the *International Equity Disclosure Standards*[37] (equity standards). The principles-based approach of the *International Debt Disclosure Principles* allows jurisdictions to implement them, as they deem appropriate in the context of their national regulatory frameworks. Therefore, the debt principles may be viewed as a starting point for consideration by national securities regulators. The *International Equity Disclosure Standards*, however, are broadly accepted as a disclosure benchmark, and IOSCO member jurisdictions may base their domestic disclosure regimes more directly on them.

To complement its debt principles and its equity standards, which apply to initial offerings and listings, IOSCO has also developed the *Ongoing Disclosure Principles*[38] (ongoing disclosure principles) and the *Periodic Disclosure Principles*[39] (periodic disclosure principles). Both the ongoing and the periodic principles address the issuer disclosure directed toward investors who participate in the secondary markets for public securities, *i.e.* trading that occurs in the market after the issuer's initial offering and/or listing of its securities. Periodic disclosure reports provide information covering a certain period of time, such as an annual report that covers the issuer's fiscal year. Ongoing disclosure is a more general term that also includes event-based or current reports, through which the issuer keeps the market informed of specific events. In developing its principles for ongoing and periodic disclosure, IOSCO has not distinguished between equity and debt securities, as it has done for disclosure applicable to initial offerings and listings of public securities. The principles-based format of most IOSCO disclosure guidance allows for a wide range of application and adaptation by domestic securities regulators.

IOSCO's equity standards and debt principles provide for disclosure of material information covering a wide range of topics about an issuer, including its business, financial position, operating and financial review and prospects, directors and officers, management's compensation, related party transactions, major shareholders, and many other areas.

Significantly, IOSCO's equity standards and debt principles both call for disclosure of risk factors that are material to an issuer's operations. Under these provisions, issuers should

---

[36] See International Disclosure Principles for Cross-Border Offerings and Listings of Debt Securities by Foreign Issuers - Final Report, Report of the Technical Committee of IOSCO, March 2007, available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD242.pdf.

[37] See *International Disclosure Standards for Cross-Border Offerings and Initial Listings by Foreign Issuers, Report of IOSCO,* September 1998, available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD81.pdf.

[38] See *Principles for Ongoing Disclosure and Material Development Reporting by Listed Entities,* A Statement of the Technical Committee of the International Organization of Securities Commissions, October 2002, available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD132.pdf.

[39] See *Principles for Periodic Disclosure by Listed Entities - Final Report,* Report of the Technical Committee of IOSCO, February 2010, available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD317.pdf.

prominently disclose risk factors that are specific to the issuer, as a summary of more detailed discussion elsewhere in the disclosure document. The IOSCO guidance does not address which specific risks an issuer should describe. Because materiality is determined by an issuer's circumstances, a risk that is material to one issuer may not be material to another. Therefore, IOSCO disclosure guidance does not specifically address cyber risks. In the equity standards and debt principles, both of which pertain to the cross-border offering and initial listings of securities, disclosure of such risks is captured under the general risk factor provisions.[40] Under IOSCO's ongoing disclosure principles and periodic disclosure principles, disclosure related to cyber risk would be captured under the general criterion, contained in both documents, that disclosure should not be misleading or contain any material omission of information.

2.3 Framework for cyber risk disclosure in IOSCO member jurisdictions

Analogous to the approach of the IOSCO disclosure standards and principles, under which disclosure of material cyber risks would be provided in response to general provisions for disclosure of known material risks to an issuer's operations, jurisdictions that are members of IOSCO's C1 do not have requirements that identify cyber risk disclosure specifically. Rather, information about cyber risks would be provided in response to general requirements that an issuer disclose information about material risks to its operations. Applying materiality, information called for by any specific disclosure items may need to be expanded upon where supplemental information is material to investors and necessary to keep the referenced disclosure from being misleading.

Disclosure of cyber risk in member jurisdictions remains subject to a materiality analysis under domestic securities laws, and is dependent on an issuer's specific facts and circumstances. The cyber risks may have a greater, or different, impact on some issuers compared to others. The impact of cyber risks may also vary across industries. It remains the issuer's responsibility to determine the materiality of cyber risk or a cyber incident to its operations, and how to disclose them in compliance with regulatory requirements.

Securities regulators in two C1 member jurisdictions, Canada[41] and the United States,[42] have issued staff guidance concerning issuer disclosure related to cyber security. The staff guidance issued by the Canadian Securities Administrators (CSA) highlights the importance of strong and tailored cyber security measures, and urges issuers to "consider whether the cyber crime risks to them, any cyber crime incidents they may experience, and any controls they have in place to address these risks, are matters they need to disclose in a prospectus or a continuous disclosure filing."

The guidance issued by the staff of the United States Securities and Exchange Commission seeks to assist issuers in assessing what, if any, disclosures about cyber security matters are appropriate in light of their specific facts and circumstances. While providing an overview of specific disclosure obligations (including risk factors, results of operations, business description, legal proceedings, and financial obligations) that may require a discussion of cyber risks and cyber incidents, the guidance notes that the United States federal securities

---

40 See the Appendix to this note for the text of those provisions.

41 See CSA Staff Notice 11-326 "Cybersecurity," (September 26, 2013).

42 See Division of Corporation Finance, Securities and Exchange Commission, "CF Disclosure Guidance: Topic No. 2 – Cybersecurity," (October 13, 2011).

laws do not require detailed disclosure that could compromise cyber security efforts by providing a "roadmap" to those seeking to infiltrate an issuer's security network.

2.4 Practices related to cyber risk disclosure

In conducting its work to better understand current issuer practices related to cyber risk disclosure, C1 held discussions with a limited sample of issuer management from large financial institutions and consultants responsible for advising issuers on how to manage and respond to threats to their cyber security. C1 also conducted its own informal review of a sample of issuer disclosure documents from among its member jurisdictions, in order to draw some observations about issuers' disclosure practices. C1 selected issuers from industries that either had been, or that might likely be, exposed to a cyber security breach.

2.4.1 Main takeaways from discussions

Among the main takeaways from discussions held by C1 is that any issuer may be exposed to cyber risk or subject to a cyber attack. Discussions highlighted the fact that there are essentially three main types of information related to cyber risk that are disclosed.

The first of these is the description of the cyber risk, which may include, for example, an increased reliance on technology, possible disruptions on the issuer's infrastructure or operating systems, possible security breaches that affect services to clients, and the difficulty in defending against all cyber risks.

The second type of information relates to the likely outcome of a cyber incident or attack, which may include financial losses, lost business, disrupted operations, reputational harm, litigation, regulatory penalties, and the unauthorized release of confidential or personal information.

The third type of information describes how the issuer is managing cyber risk, including monitoring, investing in tools to respond to threats, insurance coverage, and reliance on third-party risk management providers. In describing how risks are managed, issuers typically do not go into great detail in order to avoid divulging critical information that may compromise their security.

Some inherent limitations to disclosure were also highlighted. For example, the impact of cyber risks can be difficult to assess because it may not be quantifiable. For that reason, it may be difficult for issuers to provide meaningful disclosure. Also, in some cases, issuers may be reluctant to provide disclosure due to concerns about potential negative consequences, for instance those associated with reputational risks. Also mentioned were the impossibility for an issuer to have knowledge in advance of all cyber risks to which it may be exposed, the difficulty of detecting a cyber incident at the time it occurs, and issuers' reliance on third parties to monitor and detect cyber incidents.

2.4.2 Observations from disclosure samples

Risk Factor Disclosure

In its informal review of sample issuer disclosure among its member jurisdictions, C1 has observed that issuers often provide risk factor disclosure about a range of concerns relating to cyber risk, including:

- brand and reputational harm or harm to the business and results of operations as a result of a data breach;
- the costs of maintaining security and effective information technology systems, which could negatively affect results of operations;
- the potential adverse impact of changing laws and regulations related to cyber security; and
- general information about steps the issuer had taken to mitigate cyber risk.

C1 has observed variation in disclosure practices due to varying circumstances of issuers, including industry, size, geographic market, their use of technology, or other factors. C1 has also observed that issuers within a single industry tend to provide similar disclosure.

Disclosure of Cyber security Incidents

Some issuers have provided risk-factor disclosure indicating that they have been subject to cyber attacks in the past and are likely to be targeted again in the future. Issuers that have experienced a material data breach have, in some cases, included risk factor disclosure regarding government inquiries and their exposure to private litigation. In its informal review of disclosure documents, C1 noted that disclosure related to cyber risk was generally qualitative rather than quantitative, and that, according to management, a material cyber incident may not necessarily have a material impact on the financial statements.

C1 has also observed differences in disclosure by issuers that have been subject to a material cyber attack compared to those that have not, as well as differences in disclosure by the same issuer both before and after an attack. As a general observation, disclosure by issuers that have been subject to a material cyber attack tends to be more detailed than either disclosure from the same issuer before the attack, or disclosure from issuers that have not reported a material attack.

C1 has also observed some variation in practices related to the timing of disclosure of a cyber attack. Some issuers disclose the event of a breach shortly after its detection; other issuers take more time to assess the impact of a cyber attack before disclosing it to the market. At times, issuers disclose a cyber incident for reasons that appear to be unrelated to compliance with securities regulations.

2.5 General conclusions regarding reporting issuer disclosure

C1 has reached two general conclusions based on its work:

- First, the general materiality approach contained in existing IOSCO disclosure standards and principles is well designed to cover cyber risk. As such, revisions to the existing IOSCO disclosure standards and principles do not appear to be warranted. It is essential that issuers rely properly on the existing disclosure framework to ensure that investors receive material information, including as relates to cyber risk.
- Second, C1 has identified factors that issuers should bear in mind when preparing their disclosure. IOSCO members may take these factors into account when considering issuer disclosure in their jurisdictions.

2.5.1 Conclusions regarding IOSCO disclosure standards and principles

Both IOSCO guidance for issuer disclosure and national securities regulations describe items to be disclosed in general terms, without explicitly addressing cyber risk or other specific types of risks faced by an issuer. Rather, they encompass all risks and require the issuer to apply a materiality threshold in producing disclosure, rather than giving the issuer a "list" of items that forms the "minimum" disclosure. This regulatory framework is designed to achieve a necessary and appropriate balance, as it is designed to elicit full and accurate disclosure that is important to an investment decision, while leaving to the issuer the responsibility to consider what information should be disclosed in order to make required disclosures not misleading, given the specific circumstances of that issuer. Appropriate disclosure is heavily dependent upon an issuer's facts and circumstances, especially once there has been a breach. For these reasons, from a compliance and enforcement perspective this area is not conducive to eliciting disclosure via universally applicable, specific guidance, as compared to relying on a combination of the existing disclosure framework (e.g., risk factors, operating prospects, and so forth) augmented by the overriding principle of materiality.

In the view of C1, it is essential that issuers rely properly on the existing disclosure framework to ensure that investors receive material information, including as it relates to cyber risk. In this regard, C1 believes that it has an important role to play in continuing the dialogue among its member jurisdictions to be aware of issuer practices and regulatory developments related to cyber risk disclosure, particularly as cyber risks and related disclosure practices continue to evolve.

2.5.2 Conclusions regarding issuer disclosure practices

As noted earlier, the purpose of disclosure under securities regulation is to protect investors by providing them with material information so that they can make an informed decision to buy, hold or sell an issuer's securities. Based on the observations of C1, the following are among the factors that issuers might consider when preparing their disclosure, once they have determined that cyber risk is a material risk, and which IOSCO members may take into account when considering issuer disclosure in their jurisdictions:

- the reasons why the issuer is subject to cyber risk;
- the source and nature of the cyber risk, and how the risk may materialize;
- the possible outcomes of a cyber incident, for example:
    - effects on the issuer's reputation and customer confidence;
    - effects on stakeholders and other third-parties;
    - costs of remediation after a breach;
    - litigation, whether brought by parties seeking damages against the issuer or by the issuer against third parties;
    - effects on the issuer's internal and disclosure controls;
- the adequacy of preventative measures and management's strategy for mitigating cyber risk; and

- whether a material breach has occurred previously and how this affects the issuer's overall cyber risk. (A previous material breach might need to have been disclosed in accordance with disclosure requirements in a member jurisdiction.)

Disclosure of material risks should be tailored to the circumstances of the individual issuer. Although issuers should provide sufficient detail to describe the nature and potential consequences of a particular risk, or of a previous cyber attack, they should achieve the appropriate information balance without disclosing information that would compromise their cyber security.

Chapter 3 – Trading venues

Worldwide, the main concerns with respect to cyber attacks targeting trading venues relate to their increasing occurrences and the harmful impacts they may have.[43] In order to address cyber security issues, regulators are working to foster a safer electronic trading environment that aims to protect investor privacy, confidential information and other important trading aspects by strengthening trading systems' infrastructure.

As technology develops and the means available to cyber attackers evolve, trading venues' cyber security policies and procedures will need to be periodically reviewed and updated in order to keep up with new risks and emerging trends. In that context, IOSCO's Committee on Secondary Markets (C2) finalized the reports that touch on the issue of cyber security,[44] provided relevant updates on regulatory initiatives in their jurisdiction, and considered the AMCC Task Force Report (2014) (the "AMCC Task Force Report").

The first part of this chapter depicts current cyber security practices at trading venues and emerging trends and approaches in cyber security. The information is derived from answers received from a preliminary fact-finding survey completed as part of the AMCC Task Force Report and from the input of a working group composed of several trading venues that the AMCC put in place specifically for this initiative.[45]

Although this chapter provides insightful and meaningful information, readers should take note that it cannot cover all of the efforts currently being deployed in matters of cyber security due to the high number of trading venues around the world and the multitude of approaches that can be taken to address such an ever-changing and evolving risk. It is also not intended to provide specific recommendations.

The second part of this chapter describes some current regulatory frameworks related to cyber security applicable to trading venues. Answers come from responses from relevant questions to an IOSCO survey related to C2's Electronic Trading mandate. This section does not, by any means, represent an exhaustive account of all efforts put in place by C2 members.

---

[43] For the purpose of this paper, the term "Trading Venue" is generally defined as exchanges or other multi-lateral trading facilities, including, for example, alternative trading systems (ATSs) and multi-lateral trading facilities (MTFs). It also refers to the operator of a particular exchange or trading facility. IOSCO recognizes, however, that the concept of a "Trading Venue" is evolving in a number of IOSCO member jurisdictions. For example, the concept may, at the discretion of individual members for their jurisdictions only, also include swap execution facilities (SEFs) or the proposed European "organized trading facilities" (OTFs). A "Trading Venue" does not, however, include a single dealer system or a broker crossing facility.

[44] C2 had already undertaken two projects with implications for cyber risk issues. The first is entitled Robustness of electronic trading systems and markets (the Electronic Trading mandate); the second is entitled Business continuity and recovery for trading venues (the BCP mandate). The two projects resulted in the report entitled *Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity published* in December 2015. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD522.pdf

[45] This chapter benefited from the contribution of AMCC to C2's efforts, leveraging on the AMCC Task Force Report, with a focus on the specific threats and existing cyber security practices at the level of exchanges and other trading venues. This chapter also benefited from the input of a specific Working Group (WG) established by the AMCC in 2015, chaired by BSE Ltd. and composed of exchanges' Chief Information Security Officers, with the collaboration of the World Federation of Exchanges.

Note that Chapter 6 on financial market infrastructures, which describes the CPMI-IOSCO draft Guidance, may also be of relevance to trading venues.

3.1 Examples of potential cyber attacks targeting trading venues

Trading venues are important potential targets for attackers who, for instance, want to cause damage to the financial industry and, more broadly, disrupt markets. A number of attacks have been reported, which have led in some instances to trading suspension. Below are some examples of attacks, as well as other threats with a possible impact on the functioning of markets:

- **Hacktivists:** Hacktivists seek to draw support for a cause, or draw negative attention to a target. In 2011, the Hong Kong Exchange was forced to halt trading in shares of several blue-chip companies following a cyber attack of the exchange's news Web site, which disrupted investors' access to important corporate announcements. In 2012, a wave of Distributed Denial-of-Service (DDoS) attacks from an activist group targeted US exchanges including the NYSE, the NASDAQ and BATS, although the trading systems were not affected.[46] In 2012, regional political activists targeted Middle Eastern exchanges.[47] This was reported to have occurred again, in July 2014, at the Saudi Stock Exchange. The Warsaw Stock Exchange was also apparently hacked, in the fall of 2014, by an individual who posted login credentials of brokers and other internal data from the exchange's computer network.
- **Cyber criminals:** In 2011, breaches in the EU's carbon trading market led to the theft of EUR 50 million of emission allowances and the suspension of trading for a week.[48] Outside the regulated space, hackers also attempted to cause a selloff in the virtual currency Bitcoin in the spring of 2013 by attacking Bitcoin exchange Mt. Gox.
- **Other breaches reported:** Also in 2011, the NASDAQ OMX Group's confidential document-sharing service (the "Directors Desk") was infiltrated, an attack which targeted documents used by boards of directors.[49] In November 2013, the Chicago Mercantile Exchange (CME) revealed an intrusion on its ClearPort clearing system. According to the CME, the breach resulted in US$16.0 million of expenses related to the response to the event.[50] Trading venues also face insider threats that target intellectual property. By way of example, in 2012, a former employee of the CME Group pleaded guilty to theft of trade secrets.[51] Like other institutions, trading venues may also be targets for corporate or nation-state espionage, reputation damage or attempts at disrupting operations.

---

46 http://www.reuters.com/article/2012/02/14/us-nasdaq-attack-idUSTRE81D21720120214; see also Prolexic, DDoS attacks against Global Markets, Feb. 2014: http://www.prolexic.com/kcresources/white-paper/global-market/DDoS_attacks-against_Global_Markets_whitepaper_US_020314.pdf

47 Financial Times, *Hacker targets Tel Aviv bourse and El Al*, 16 January 2012; *Hackers attack Arab stock markets*, 17 January 2012.

48 The Financial Times, *Carbon trading: into thin air*, 14 February 2011, http://www.ft.com/intl/cms/s/0/368f8482-387d-11e0-959c-00144feabdc0.html#axzz3Y2wLpNj4

49 http://www.foxbusiness.com/industries/2011/03/30/report-national-security-agency-joins-nasdaq-cyber-breach-probe/

50 Chicago Mercantile Exchange, *CME Group Confirms Cyber Intrusion*, 15 November 2013, http://investor.cmegroup.com/investor-relations/releasedetail.cfm?ReleaseID=807750. See also CME, *Annual Report 2013*.

51 Reuters, Ex-CME programmer pleads guilty to trade secret theft, 19 September 2012, http://www.reuters.com/article/us-cme-theft-plea-idUSBRE88J02U20120920

- **New threats:** Although not directly targeted at trading venues, various reports noted the increasing likelihood of attacks targeting market-moving information about deals, such as those attributed to the FIN4 group.[52] Such attacks employ, amongst other techniques, a combination of social engineering and spear phishing. Back in April 2013, the hacking of the Associated Press Wire's Twitter account with a false announcement of an attack on the White House led to a temporary fall of 143 points of the Dow Jones Index.[53] In August 2015, the U.S. SEC charged defendants in a scheme to trade on hacked news releases from three news wire services, with hackers and traders allegedly having reaped more than US$100 million in illegal profits.[54]

The following table illustrates possible vulnerabilities faced by trading venues along the transaction value. The motives for the attacks may be financial gains, reputation damage, theft of intellectual property, or political objectives, including economic damage and destruction. Whereas financial institutions might look at confidentiality as their most relevant concern, with respect to trading venues, ensuring data integrity would be the first priority, followed by system availability.[55] Loss of integrity may take different forms, e.g., lost integrity of data feeds, data destruction, exfiltration of non-tampered data, or "low and slow" attacks where data change subtly over a long period of time, making it very difficult to detect and recover.

Examples of cyber security vulnerabilities in the transaction chain

Stage	Potential threats
Pre-trade	▸ Unauthorized access, fraudulent use of a trading participant's algorithm/automated trading systems, unauthorized data patch by non-administrators ▸ Upload of viruses or corrupted files during data transmission from brokers' systems into trading venues' systems ▸ Dissemination of false information triggering trading, disruption in the access to corporate announcements, trading on non-public information ▸ Breach in the order management systems resulting in incorrect feeds, false orders or orders not distributed to all brokers or inability to submit or route orders

[52] FireEye, *FIN4: Stealing Insider Information for an Advantage in Stock Trading?*, November 2014: https://www.fireeye.com/blog/threat-research/2014/11/fin4_stealing_insid.html.

[53] USA Today, *AP Twitter Feed Hacked; No Attack at White House*, 23 April 2013, http://www.usatoday.com/story/theoval/2013/04/23/obama-carney-associated-press-hack-white-house/2106757/. See also the example cited by EY whereby a criminal takes a long position in copper on the London Metal Exchange and then proceeds to use cyber hacking to disrupt supply at key copper production facilities causing prices to spike (http://www.mining-technology.com/features/featuremining-cyber-attacks-mike-elliott-ernst-young-4171663/).

[54] http://www.sec.gov/news/pressrelease/2015-163.html

[55] See, for instance, AMCC Panel Discussion on Cyber security, June 2015 and U.S. CFTC´s Staff Roundtable on Cybersecurity and Systems Safeguards Testing, March 2015.

	▸ Manipulation of index calculation
Execution	▸ Interferences with trading venues' matching engines causing matching errors, unavailability of matching systems ▸ Disruption in price discovery in pre-open sessions or in periodic call auction sessions (*e.g.* due to network issues) affecting trading for the entire day ▸ Manipulation of Financial Information Exchange (FIX) Protocols within the customers' trading interfaces ▸ Disruption in session management / members' connections to trading venue systems ▸ Hacking and insider trading
Risk management	▸ Manipulation of pre-trading limits ▸ Attacks in real-time on risk management systems resulting in erroneous margin calculation
Clearing and Settlement	▸ Fraudulent transfer of funds or securities of other clearing members through the clearing banks ▸ Breaches in the receipts or payments of margin deposits by clearing members ▸ Misuse of early pay-in from another member ▸ Upload of viruses from the clearing members' systems to the trading venues' systems, corruption or unavailability of clearing core data or systems ▸ Manipulation of post trade systems; Deletion, modification, or corruption of transaction records raising ownership issues.
Trade dissemination	▸ Shut down or corruption of the networks for trade data dissemination causing withdrawal of market liquidity and suspension of trading
Surveillance	▸ Unavailability of surveillance systems, data corruption
Other services	▸ Disruption in shared services offered by trading venues such as Mail / Web services (e.g. preventing members from getting billing information, etc.)

Source: AMCC TF on Cyber Resilience and AMCC Working Group.

3.2 Examples of practices to reinforce cyber security

Drawing on information from trading venues collected by the AMCC Working Group, the following are examples of practices in place at trading venues.[56] These examples are organized according to the structure adopted by the U.S. NIST Cybersecurity Framework (see table).[57]

The NIST Framework

Functions	Description and examples of related categories
Identify	*Develop the organizational understanding to manage cyber security risk to systems, assets, data and capabilities* › Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy
Protect	*Develop and implement the appropriate safeguards* › Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Protective Technology
Detect	*Develop and implement the appropriate activities to identify the occurrence of a cyber security event* › Anomalies and Events, Security Continuous Monitoring, Detection Process
Respond	*Develop and implement the appropriate activities to take action regarding a detected cyber security event* › Response Planning, Communications, Analysis, Mitigation, Improvements
Recover	*Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event* › Recovery Planning, Improvements, Communications

Source: NIST Cybersecurity Framework.

[56] Due to the small number of exchanges surveyed, the information should not be taken as a comprehensive view of all approaches to cybersecurity and does not allow drawing general conclusions regarding common trends and the state of preparedness of the exchange industry globally. Many of the examples provided are technical in nature and serve to illustrate the broad range of measures available to trading venues to strengthen their cyber-resilience. Many are common to all institutions and market segments.

[57] This risk-management-based framework identifies five high-level cyber security functions, i.e. the identification of risks, the protection measures, the detection of potential threats, the response and the recovery. These functions, which are mutually reinforcing, rely on several components of similar importance for an effective information security strategy (inclusive a cyber security strategy) based on governance, risk, compliance, people, processes and technology.

3.2.1 Identification

The governance structure established by trading venues to deal with cyber security issues, including the involvement of senior management and company boards, is paramount for the effectiveness of the overall information security framework. It helps organizations focus attention, determine their risk appetite and priorities and allocate resources to cyber security. Surveyed trading venues considered cyber security to be an integral part of the enterprise risk management program as it defines and maintains appropriate interfaces with related disciplines such as business continuity and recovery planning, emergency management, public incident management and disaster management.

As stressed in the AMCC Task Force Report, a key component of the risk management program is the identification of critical assets, information and systems, including order routing systems, risk management systems, execution systems, data dissemination systems, and surveillance systems.

Given the specific exposure of trading venues to cyber attacks, the topic is increasingly seen as a board-level issue, with escalation procedures to the CEO and the appointment of a dedicated committee (with representatives from IT, business, legal, HR, communications, and risk functions). Most trading venues have also appointed a Chief Information Security Officer (CISO), as well as individuals responsible for compliance at the level of the businesses (BISOs).

Practices supporting the identification function include the establishment and maintenance of an inventory of all authorized and non-authorized hardware and software. Trading venue operators must also undertake third-party and technology providers' security assessments.

Accessing information about the evolving threat landscape helps identify the changing nature of the cyber risks. Trading venues can receive threat reports from external vendors on data traffic and fraudulent sites, access vendor feeds, security bulletin service providers, information from CERTs (Computer Emergency Readiness Teams) and other information sharing platforms. In addition, specific/peer-group community information sharing groups such as CHEF (within the Financial Services Information Sharing and Analysis Center (FS-ISAC)) and GLEX (within the World Federation of Exchanges) or other groups established at domestic level (composed, for instance, of the domestic exchange and the largest banks or broker-dealers) usually provide more accurate and real-time information, whereas vendor intelligence provides ex-post analysis.

3.2.2 Protection

There are numerous controls and protection measures that trading venues use to strengthen cyber security. Such measures can be organizational (like the establishment of Security Operations Centers (SOC)) or technical (like anti-virus and intrusion prevention systems). Examples of protection measures mentioned by respondents in the AMCC Survey responses are listed in the Table below, broadly distinguishing between IT management practices and controls, security measures (including physical security), and protective technologies. Some of these measures are explained in further detail below.

IT Management and Control Policy	Security Controls	Protective Technologies
• Compliance with global standards such as ISO, COBIT, SANS Top 20 Controls, NIST Cyber security Framework and other NIST cyber security-related standard • Secured software development practices	• Physical security measures (lost laptops, unsecured workstations, building entrance, etc.) • Security clearances and staff background investigations • Comprehensive password management policy, access control mechanisms • Privilege Identity Management System (PIMS) and Access Control Policies and Software, regular renewal of digital signatures, reduction of administration privileges • Monitoring printing and capturing the printing of sensitive information, email retention policy • Network Access Controls • System and data storage segregation • Third-party and technology providers security measures (before and during the execution of a contract • Vulnerabilities testing and protection building during the development phase of new systems, hardening of all infrastructures and servers before they can communicate with others • Security check points at all Systems Development Life Cycle (SDLC) phases (design, certification, implementation, and maintenance) (to be applied both at internal and external development teams) • Device based risk profiling, mobile device management (MDM) • Vendor management	• Web Applications Firewalls (WAF) • Intrusion Prevention System (IPS) /Intrusion Detection System (IDS) • Advanced Persistent Threats (APT) Prevention System • Distributed Denial of Service (DDoS) Defense System • Data loss prevention (DLP) plan and software • Anti-virus and anti-malware software • Spam filtering • Anti-tamper software • Port blocking, IP blocking, web filtering • Scanning/Penetration testing • Encryption • Forensic Readiness Tools for incident response • Malware Analysis Toolbox

Source: AMCC TF Report and AMCC WG.

Risk assessments help determine the minimum level of controls to be implemented within a project, an application or a database. This applies to new projects, major releases and applications in maintenance mode. It is also important to implement controls requirements together with active coaching to support project managers and users for the application of existing and future security controls and mechanisms, as well as regular checks for compliance.

Employee training and awareness initiatives are critical parts of any cyber security program, including induction programs for new comers, general training, as well as specific training (for instance, social engineering awareness, training on phishing and DDoS attacks, incident handling, application level security training, and cyber security do's and don'ts).

Trading venues also stated that proficiency tests could be conducted to demonstrate staff understanding and that third party training could also be organized. Other initiatives which contribute to raising employees' awareness of cyber security threats include monthly security bulletins emailed to all employees, regular communications regarding new issues and discovered vulnerabilities, use of posters and screen savers, and regular reminders sent to employees. Mock tests can also be conducted to assess employees' preparedness and are usually very effective in reducing human errors. Employees are also often encouraged to report possible attacks.

In addition to employee training, various protection measures listed in the Table above significantly contribute to reducing insider threats (both unintentional and malicious). They include strict monitoring and control of employee access to critical assets, extensive screening combined with a strict hiring policy involving background checks, anomaly detection and a formalized insider risk management program. Other controls can also be implemented to limit risks when employees leave the exchange or change function.

Furthermore, trading venues answered that they operate segregated platforms for trading systems and web services in order to prevent contagion. They also stated that they use secured network communications with members. Trading venues may also engage with their members with respect to IT security and cyber security, e.g. through:

- Specific provisions included in the platforms' rule books and standards, notably with respect to members' order management systems, information security policy, incidence response and business continuity planning requirements;[58]
- Certification activities/security assessments during the membership application, including request for pre-approval or certification of order routing systems and interfaces, possibly including on-site visits by the trading venue;
- Communication of audit findings and any corrective actions implemented or planned at members;
- Guidance and recommendations;
- Dissemination of information regarding possible attacks;
- Audit reports; and

[58] Provisions may cover areas such as management of information security, security resources, security risk assessments and requirements for external reviews, testing, requirements in terms of incident response, security of outsourced services, processing of sensitive information, networking connections and accesses.

- Regular discussions with members' CIOs/CISOs/CROs and exchange of information regarding readiness.

3.2.3 Detection

External and internal monitoring of traffic and logs are necessary to detect abnormal patterns of access and other anomalies. Many trading venues have dedicated cyber threat teams and engage in file server integrity and database activity monitoring (DAM) to prevent unauthorized modification of trading and other critical servers within their organization's enterprise network. Different alarm categories and severity may be defined. Common tools include:

- Security Information and Event Management (SIEM) tools to collect, correlate and analyze a wide variety of security-related data;
- Virus detection and advanced malware detection;
- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to identify and react to possible intrusions from outside the organization as well as misuse (attack from within the organization);
- Vulnerability Assessment and Penetration Testing (VAPT), vulnerability scanners;
- Independent external audits;
- Ordering threat reports from external vendors on data traffic and fraudulent sites;
- Accessing vendor feeds, security bulletin service providers, information from CERTs and other information sharing platforms; and
- Specific/peer-group community information sharing groups.

In terms of monitoring, the latest trend is to combine organizational SIEM tools (covering the organization's own security events) with relevant (sector-specific) threat intelligence services from global service providers. Such a combination ensures greater proactivity in the identification of and response to changing cyber threats. These service providers may also offer cyber response team services or third party computer security incident response team (CSIRT) services.

Detection capabilities for potential breaches and infiltrations are crucial, as attackers can use the period of presence in the target's systems to expand their footprint and their access to gain elevated privileges and control over critical systems. Attackers also look to remove evidence of their presence following a successful infiltration. The privilege escalation and exfiltration phases may possibly take many years, thereby reducing the risk of being recognized.

3.2.4 Response

Responding to cyber threats can be seen as part of trading venues' BCP. However, although incident response planning and BCP are related, they are independent; notably, BCP would generally focus on availability, whereas integrity and confidentiality are also central considerations in the response to any cyber event.

Trading venues should consider developing formalized Incident Response Plans ("IRPs") for those types of incidents to which the organization is most likely to be subject (DDoS attacks, malware infection, data corruption, insider threat, breached user account, etc.). Such plans should be regularly practiced and updated. Crisis management should also consider cyber incidents with the potential to evolve into a crisis.

Response plans include:

- Preparing communication/notification plans (taking into consideration that computers and networks might not be operable) for informing relevant stakeholders such as members, regulators, clearing and settlement market infrastructures, law enforcement, industry information-sharing groups, etc.; notification may be a requirement;
- Conducting forensic analysis (internally-conducted or outsourced) notably to understand the anatomy of a breach or an attack and analyze the failures in controls which have permitted their occurrence; proper investigation is also needed to assess the extent of the damage (e.g. in the case of data theft) and the effectiveness of the containment strategy; the analysis must also allow to identify the responsibilities of employees and/or support/outsourced staff, if any;
- Maintaining a database recording cyber attacks and having a specific unit in place to analyze and disseminate cyber intelligence to respective business units, monitoring of specific metrics to assess evolving security needs; and
- Conducting cyber drills, firm-specific simulation exercises as well as industry-wide scenario exercise such as Quantum Dawn[59] – given their critical function, trading venues and other trading platforms can play a prominent role in such industry cyber drills; scenarios may include a breach at the trading venue-level or cyber attacks at the level of market participants which could impact trading.

Further, trading venues and SROs may require their members to notify them in the event or the suspicion of an information security breach, which may impact their connection with the trading venue and the trading venue's systems. Trading venues may have in place memoranda with other trading venues and market infrastructures in case of technical glitches or other IT issues, including potential breaches.

3.2.5 Recovery

As argued in C2's report on their Electronic Trading and BCP mandates,[60] one of the key steps to address the risks associated with technology, such as cyber risks, is the development of a BCP, which incorporates significant components of operational risk management, and includes policies, standards, and procedures for ensuring that specified operations can be maintained or recovered in a timely fashion in the event of a disruption. The purpose of the BCP is to minimize the operational, financial, legal, reputational and other potential material consequences arising from a disruption. BCPs typically provide for different scenarios,

[59] Quantum Dawn is a cyber security exercise organized by SIFMA that tests incident response, resolution and coordination processes for the financial services sector in the US. In the third exercise held on September 16, 2015, over 650 participants from over 80 financial institutions and government agencies participated, including key industry and government partners such as the U.S. Department of the Treasury. In Canada, IIROC recently conducted a tabletop cyber test of securities firms. The test scenario envisioned multiple cyber attacks on a number of member firms that would likely impact trading on the TSX (the main Canadian stock exchange). In the UK, the CBEST program (*cyber-resilience testing programme*) includes UK exchanges, along with the largest/core banks and market infrastructures. In the US, coordinated testing of business continuity and disaster recovery plans on an industry- or sector- wide basis is a requirement for entities subject to Regulation SCI.

[60] See IOSCO C2, Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity, December 2015.

governance, back-up or redundancy, minimum service levels, communications protocols and regular testing and review.

Effective business continuity management concentrates on the impact, as opposed to the source, of the disruption, in order to provide securities market participants and regulators greater flexibility in addressing a broad range of disruptions. At the same time, however, organizations cannot ignore the nature of the risk to which they are exposed.

The CPMI-IOSCO draft Guidance discusses recovery issues in the context of cyber risks and market infrastructures and notably the application of CMPI-IOSCO's Principle 17 on Operational Risks, which includes a two-hour recovery time objective (RTO) after disruption. The CPMI-IOSCO draft Guidance, although it does not cover trading venues directly, discusses issues of relevance for them. Further, the CPMI Cyber Resilience in Financial Markets Report notes that the recovery objective *"could involve trade-offs with other aspects of cyber security and resumption"*, for example with respect to forensic analysis and the need to preserve the integrity of the evidence collected.[61] The Report also speaks of the ability to roll back to *"the uncorrupted "golden point," from which affected IT environment components, data and/or applications can be restored to the state they were in prior to the attacker´s presence."* In the case of a data corruption event occurring at one trading venue, this would require accessing trading venues' snapshots. In this respect, trading venues may have different practices.

Typically, the risk division of the trading venue would define RTO and RPO (Recovery Point Objective) targets. Just like for response planning, conducting regular drills is important to assess the effectiveness of the recovery planning, and use the learning to strengthen it. Finally, the recovery function includes an important communication component, especially for trading venues.

3.3 Emerging trends in cyber security practices at trading venues

As the threats become more palpable and dangerous, and scrutiny increases from regulators, members and clients, shareholders and other stakeholders, the amount of resources invested at the level of trading venues increases. Although many cyber security practices have been in existence for years, more sophisticated tools to detect threats or respond to them are also becoming available. Below is a selection of trends in terms of approaches to cyber security:

Honey pots, honey nets, and other decoy options: these are complementary efforts to traditional controls and testing. They are used to simulate one or more network services and can serve to log access attempts and collect data on intruders without risks to the trading venue's systems or data; such tool can give advanced warning of a possible attack and may be used by trading venues;

Real time threat information: the development of STIX (Structured Threat Intelligence Expression) and TAXII (Trusted Automated Exchange of Indicator Information) is helping greater automation in the sharing of information so that the information can go directly into the trading venues' defense systems. STIX and TAXII can take threat intelligence from various sources, de-duplicate data and reduce the threat indicator analysis lifecycle, while also allowing better archiving and analyzing of the data enabling to detect trends; the

[61] See CPMI, *Cyber Resilience in Financial Markets*, Nov. 2014: http://www.bis.org/cpmi/publ/d122.pdf.

information focuses on the tactics, techniques and procedures (TTPs) used by attackers so that the firms can quickly assess if they are also being targeted, block the attack or delete the malware. Such evolution helps bring the cost of defense down, while teams can focus on potential high impact/low frequency threats;

Progress in SIEM tools and response team services: organizational SIEM tools (covering the organization's own security events) can be combined with relevant (sector-specific) threat intelligence services from global service providers – such combination ensures greater proactivity in the identification of and response to changing cyber threats. SIEM solutions can also leverage STIX and TAXII standards and Indicators of Compromise (IoCs) received from network groups; service providers are also increasingly offering cyber response team services or third party computer security incident response team (CSIRT) services. Similarly, trading venues' security operations centers (SOCs), operational 24/7, may combine outsourced teams to manage first-level alerts and internal staff;

Protection of internal information: recent cases of market manipulation on hacked information have shown the risks associated with the handling of sensitive information, which is also becoming a key area of focus for trading venues; threats could be external (hackers) or internal (misuse of confidential information by staff – this can be addressed notably by a tighter monitoring of email and internet use and filing);

Third-party management: Like other market participants, trading venues are stepping up their vigilance regarding third parties; security policies in place may regulate identity lifecycle (including necessary background checks, etc.), access control (on- and off-boarding), confidentiality and handling of sensitive documents and data. Tests and homologation are requested before a provider can access the trading venue's systems; policies should also cover the termination of contracts with third parties and information security aspects associated with it;

New approach to cloud security: Dialogue between trading venues and cloud service operators is rapidly evolving, with the objective to provide greater comfort to the trading venues with respect to the security of the information stored in the cloud; this includes exchanges of information regarding incident analysis;

Cyber insurance: There are challenges associated with the adoption of cyber insurance, such as a lack of actuarial data and the unknowable nature of all potential cyber threats. Because of the specificity of their business models, and their role in financial markets, these challenges are particularly acute for trading venues. However, as the frequency of cyber attacks and the potential damages they may cause are increasing, it is expected that more and more trading venues will opt for cyber insurance.

Collaboration: Global communication and sharing of information within the trading venue community – such as the GLEX initiative – is seen as very valuable. Such communication is expected to grow further, covering various areas/levels within the organizations, such as strategic level, security manager level, tactical and operational level, or again between trading venues' security analysts or SOCs/CERTs, etc. Topics covered can include information about security incidents, and the techniques employed, providing actionable advance knowledge on cyber threat activities, as well as sharing of practices, tools, etc. War games and joint drill exercises could also provide further options for collaboration.

Overview of cyber insurance in securities market

Cyber insurance can potentially be a useful and important component of a business' cyber security framework. While existing insurance policies such as commercial property, business interruption or professional indemnity insurance, may provide some elements of cover against cyber risks, businesses are increasingly buying specialized cyber insurance policies to supplement their existing insurance arrangements.

Many insurers now offer comprehensive cyber risk policies, providing both first- and third-party coverages. Perils covered under cyber policies include expenses incurred as a direct result of the breach, such as legal, investigation and public relations expenses, as well as indirect costs, such as business interruption and loss of goodwill. Third party coverages available include losses suffered by customers as a result of the theft and use of their personal financial data. Insurers also offer value-added services, such as network security testing, designed to help companies avoid and mitigate the effects of a data breach, and crisis management services.

The contraction of cyber insurance can also help businesses enhance their cyber security practices to the extent that insurance companies typically make coverage conditional on risk assessments of clients and on the adequacy of their cyber security framework.

The size of the cyber insurance market is relatively modest. Gross annual written premiums are currently estimated at around $2.5 billion globally. But the market is expected to grow significantly in the coming years. PwC expects gross annual written premiums to reach approximately $7.5 billion by the end of the decade.

A relatively small proportion of securities market participants have contracted cyber insurance but that proportion appears to be growing. According to the 2013 IOSCO/WFE survey on trading venues, 22% of respondents noted having contracted cyber insurance or something similar.

According to FINRA's 2015 cyber security report, 61 percent of firms it reviewed purchased standalone cyber security insurance; 11 percent purchased a cyber security rider with their fidelity bond; and 28 percent did not rely on any type of cyber security insurance at the time of the sweep. Larger firms tended to rely to a greater extent on standalone policies that are more suited to their specific need in terms of types and amount of coverage.

According to FINRA's report, firms with insurance articulated three broad reasons for purchasing coverage: 1) to transfer potential unmitigated risk above the firm's risk appetite; 2) to obtain coverage for gaps, such as data breaches, that may not be covered in existing policies, and 3) to reduce the risk of potential impact to a firm's financial statement in the event of an attack.

Market participants should evaluate carefully if and how cyber insurance could be a component of their cyber security framework. But cyber insurance should be viewed as a complement and not a substitute to an effective cyber security framework. And given the wide range of available terms and conditions associated with cyber insurance, there is certainly no one-size-fits-all for market participants, as is the case with other aspects of cyber security.

3.4 Description of current regulatory frameworks related to cyber security applicable to trading venues

This section presents insights of regulatory frameworks governing cyber security at trading venues.

Responses from relevant questions to the C2 survey on "Robustness of electronic trading systems and markets" and related reports were reviewed to provide insight into the current state of regulations with regards to cyber security and trading venues.

Cyber security related to trading venues is governed by many regulations and technical requirements that regulated entities are expected to comply with. For example, financial market infrastructures and financial services firms are expected to have appropriate risk management systems in place to minimize their exposure to cyber risks, by, for instance, implementing adequate physical and electronic security arrangements, ensuring compliance with financial stability standards, notifying appropriate authorities of any suspicious trading activity, and having appropriate protections for electronic trading.

However, the methods used to achieve these regulatory objectives do differ among jurisdictions. For example, some jurisdictions do not have specific regulatory requirements regarding cyber security but may have other requirements relating to cyber security applicable to trading venues that are part of self-regulatory governance rules, risk control systems procedures or guidelines regarding information and cyber security.[62]

Where regulatory requirements do exist, they vary across jurisdictions and financial authorities. For example, Australia has issued regulatory guidance targeted to market operators that include preventive measures against cyber attacks, depending on the nature, scale and complexity of the entity. Canada requires sufficient cyber security controls on systems that support order entry, order routing, execution, trade reporting, trade comparison, data feeds, market surveillance and trade clearing.[63]

In the United States, the SEC has recently adopted Regulation SCI. It applies to self-regulatory organizations (which include securities exchanges, securities associations, clearing agencies, and the Municipal Securities Rulemaking Board), alternative trading systems exceeding specified trading volume thresholds, plan processors, and certain exempt clearing agencies.[64]

The CFTC recently sought public comments on proposed enhanced rules on cyber security for derivatives clearing organizations, trading platforms and swap data repositories.[65] The

---

62 For example, Switzerland, Brazil, and Canada (IIROC).

63 See National Instrument 21-101. Regulated marketplaces are not only expected to be able to report failures, malfunctions or material delays to regulators, but also security breaches to its systems in a timely manner.

64 Under Regulation SCI, entities are required to, among other things, have comprehensive policies and procedures for their technological systems; take appropriate corrective action when systems issues occur; provide certain reports and notifications to the SEC regarding systems problems and systems changes; inform members and participants about systems issues; conduct business continuity and disaster recovery plan testing; and conduct annual reviews of their automated systems.

65 See System Safeguards Testing Requirements for Derivatives Clearing Organizations, 80 FR 80114 (Dec. 23, 2015); System Safeguards Testing Requirements, 80 FR 80140 (Dec. 23, 2015).

proposals would amend existing regulations addressing cyber security testing and safeguards for the automated systems used by critical infrastructures the CFTC regulates. The proposals identify five types of cyber security testing as essential to a sound system safeguards program: 1. Vulnerability testing; 2. Penetration testing; 3. Controls testing; 4. Security incident response plan testing; and 5. Enterprise technology risk assessments.

Under the proposals, all derivatives clearing organizations, designated contract markets, swap execution facilities, and swap data repositories would be required, consistent with best practices, to conduct the five types of tests. For specified registered entities, there would be a minimum testing frequency for testing, and requirements to engage independent contractors to conduct some of the required testing. The proposals also would clarify rule provisions relating to the scope of system safeguards testing, internal reporting and review of testing results, and remediation of identified vulnerabilities and deficiencies.

In Europe, the European Securities and Markets Authority (ESMA) guidelines on "Systems and controls in an automated trading environment for trading platforms, investment firms and competent authorities"[66] do explicitly require trading platforms to have in place procedures and arrangements to protect their electronic trading systems from misuse or unauthorized access.

Cyber security is one of the issues monitored by the French regulators when assessing BCP of investment firms and trading venues. In July 2009, the French government created a national agency in charge of cyber security across all sectors, including the financial sector.[67]

India adopted guidelines relating to cyber security and cyber resilience similar to the U.S. NIST framework.[68] In Malaysia, both the Securities Commission of Malaysia and Bursa Malaysia apply regulatory requirements that are part of the government's National cyber security Plan (NCSP) initiative. Hong Kong asks major trading venues to provide periodic statistics on its monitoring of cyber security attacks.

Even though regulations regarding cyber security and resilience are still being developed and perfected around the world, many countries have already taken steps to monitor compliance with the requirements set by regulators and to impose penalties for violations and breaches of electronic trading systems.[69] Governments and financial authorities may impose monetary penalties and institute civil proceedings. In addition, they may require compensation, limit activities, and suspend and revoke registration. Specific legal consequences and actions vary among countries.

Cybercrime legislation is constantly evolving in order to safeguard against new methods and approaches that may pose cyber risks to electronic financial markets. The ASIC report presented international developments in that respect and further highlighted the fact that

---

66 http://www.esma.europa.eu/system/files/esma_2012_122_en.pdf

67 Agence Nationale de la sécurité des systèmes d'information : http://www.ssi.gouv.fr/

68 See http://www.sebi.gov.in/cms/sebi_data/attachdocs/1436179654531.pdf

69 For example, Australia has a range of specific remedies that deal with breaches of the market integrity rules and the Corporations Act 2001. Actions include civil penalties, compensation orders, publication orders, infringement notices, enforceable undertakings and money penalties of an amount not exceeding $1 million AUD. Brazil follows a similar practice in which any infringement may be penalized with warnings, fines, suspension and cancellation of the authorization.

cyber risk management is still a voluntary exercise for most companies in the United States, Asia and Europe. Securities regulators recognize cyber risk as a major regulatory concern across the globe and they have focused on industry information-sharing and public-private collaboration. For example, the United States is developing a common framework for cyber security and improving private sector cyber security information sharing by developing information sharing and analysis organizations and enabling them to share standards. As discussed in Chapter 5, CPMI and IOSCO are collaborating to review and evaluate the implications of cyber attacks targeting financial market infrastructures, including financial stability implications, and have produced a draft document that provides guidance to them.

Securities commissions, associations and authorities around the world have taken measures to protect electronic trading.[70] Such measures are in line with government cyber security efforts and aim to ensure safe electronic trading and the protection of investor privacy. For example, surveillance systems, security standards, policies, and procedures are implemented according to regulations. Violations and breaches of electronic trading systems are being identified and appropriate actions are also being taken (e.g., notifying legal authorities, penalties).

In addition, many financial markets have supervisory systems that monitor compliance with the requirements set by regulators with respect to electronic trading. For example, many European market authorities follow ESMA's standard supervision process.[71] Other countries follow their own specifications, for example Malaysia Securities Commission's supervisory team is responsible for monitoring the trading venues' compliance with regulatory requirements as part of the overall oversight of trading venues.[72] Mexico's National Banking and Securities Commission (CNBV) has a full-time team specialized in supervising trading venues including cyber risk management. Globally, securities commissions, associations and authorities have implemented security regulations that aim to procure safer electronic trading systems.

3.5 Conclusions regarding trading venues

As highlighted in this chapter, regulators play different roles and use various tools in order to help ensure the cyber security of trading venues. Amongst these tools, regulators have chosen to raise awareness levels regarding cyber security through the use of examination sweeps and the issuance of guidance, guidelines, or frameworks. While regulators have used diverse tools, their overall approaches are broadly compatible to the extent that they have expressed comparable expectations regarding trading venues' cyber security practices.

---

70 The Financial Services Agency ("FSA") of Japan may order reports and inspect trading venues, suspend part of their business, require them to improve business operations and rescind the license and/or authorization. The Netherlands considers breaches of the requirements of trading venue information as integral parts of the regulatory framework of the trading venue. Any violations of these requirements are subject to legal action including pecuniary fines and ultimately the withdrawal of the authorization of the trading platform. The Monetary Authority of Singapore ("MAS") takes disciplinary actions such as issuing a warning and a fine for any regulatory breach and violations. South Africa refers breaches to the FSB's Enforcement Committee for an administrative penalty. Ireland has a wide range of penalties available for breaches of Central Bank requirements such as a private caution/reprimand, a direction to do or to cease doing a regulated activity, payments of fines and/or disqualifications of certain individuals and withdrawal of an authorization granted.

71 For example, in Germany, Ireland, Italy, the Netherlands, Spain and the United Kingdom.

72 Capital Markets and Services Act (2007), Malaysia.

Furthermore, regulators have also initiated and coordinated drills simulating cyber events and breaches involving all stakeholders from SROs and trading venues to market participants and institutional clients. Finally, regulators have also initiated regulatory changes or developed new regulations requiring trading venues to identify cyber risks, to detect threats, to protect themselves against them and to respond and recover from cyber security events.

With regards to emerging trends and approaches in cyber security practices for trading venues, we noted that exchanges have a multitude of threats to contend with. Exchanges have invested a considerable amount of resources in order to establish an internal structure that addresses the issues relating to cyber security. Whether it is by following an existing cyber security framework such as NIST or by ensuring that third parties meet certain defined security criteria, trading venues have taken steps to try and keep up with the accelerating pace at which cyber threats are evolving.

One overarching aspect that is important in supporting several cyber security functions, from detection to response and recovery, is the need for sound testing regimes. Testing regimes vary depending on the institution's own risk assessment and on the scenarios considered; the tests are usually conducted both internally and by independent contractors so as to benefit from both internal knowledge of the systems and external perspective and expertise. Such tests are performed periodically, depending on the scope and scenarios involved.

Ultimately, trading venues and regulators alike will have to continue to adapt as information technology continues to evolve.

Chapter 4 – Market intermediaries

To support IOSCO's Cyber Risk Coordinators, IOSCO's Committee on market intermediaries (C3) has formed a working group to provide informal feedback and assistance as it collects information to address this issue.[73] Working group members have identified certain information, or taken specific steps, that are detailed below.

As explained below in greater detail, jurisdictions have taken various approaches to address cyber threats. Nevertheless, there appear to be a few consistent themes across the regulators represented in the C3 working group, including:

- The need to assess the nature, location and sensitivity of information firms collect;
- The need to identify and inventory the risks that firms face;
- The need to create a strategy to address and respond to cyber threats, including written policies and procedures to implement the strategy;
- The need to implement proper security and other internal controls;
- The need to test systems, IT and others, for potential vulnerabilities;
- The need to protect customer information from identity theft;
- The need to train employees on appropriate cyber security prevention; and
- The need for greater information sharing, including, in some cases, notification to the regulator of security intrusions as well as an indication of all planned remedial steps.

C3 working group members have also done a literature review of what they believe are the most relevant reports related to intermediaries' activities concerning cyber security. They also produced a summary of these reports according to the five main functions associated with cyber security, namely identification, detection, protection, response, and recovery. The review and the summary are found in appendix A of this report.

They notably provide an overview of C3's Market Intermediary Business Continuity and Recovery Planning Report which proposes standards and sound practices that regulators could consider as part of their oversight of the business continuity and recovery planning by market intermediaries and that might be relevant in the context of cyber security.[74]

The following provides as examples regulatory actions taken in Mexico and the United States in regards to cyber security and intermediaries. Note that the introductory section of this report also provides examples of regulatory steps taken in Australia, the United Kingdom, the United States, and Singapore that are more general in nature.

Readers should also note that the description of cyber security practices contained in Chapters 3 and 5, which are related to trading venues and asset managers, can potentially be relevant for intermediaries.

---

[73] The working group consists of the CNBV of Mexico, the CFTC from the United States, the FCA from the United Kingdom, and FINRA from the United States (including also input from the US Securities and Exchange Commission, Singapore's MAS, and Australia's ASIC).

[74] See: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD523.pdf

4.1 Steps taken in Mexico

In Mexico, cyber security is part of the regulatory requirements applicable to market intermediaries related to technological risk assessment. The specific section of the relevant regulation (also known as "Technology Risk Management") contains four types of requirements:[75]

- To assess vulnerabilities on hardware, software, networks and recovery procedures;
- To implement internal controls on hardware, software, applications, data security, information recovery and telecommunication networks;
- When "all services channels" are offered by the intermediaries to their customers (e.g., branches communications or Internet services), they must also:
    - implement measures and/or mechanisms that enable factors for user identification and authentication in order to grant access to data (generation, storage, transmission and delivery);
    - implement controls regarding protection, security and confidentiality of the transactions' information (essentially by using encryption);
    - have access to control policies and procedures, as well as proper controls in place for access to all critical systems, databases and files related to operations and services provided through electronic channels, and
    - develop contingency plans in order to recover operations after a disruption, to minimize the effects on information losses and service levels.
- To implement mechanisms to prevent and deal with:
    - fraud;
    - contingencies, and
    - inappropriate use of the electronic media channels.

In addition, if electronic communications are available to customers, intermediaries must implement the following controls:

- use encryption to protect all transmitted data;
- strong authentication methods;
- monitor activities to detect and prevent fraud, and
- periodically assess vulnerabilities and carry out penetration tests to verify:
    - the security adequacy of access controls on data processing infrastructure and telecommunications, and
    - the tools in place to effectively prevent and detect events that could affect security, confidentiality and integrity of information.

Finally, reporting of data loss events is required from intermediaries with a short time period after an incident is detected. Firms must also send a written report to the CNBV, investigate the incident immediately, submit the results to the CNBV and notify users and the firm's Audit and Risk Committees.

[75] Regulation for Brokerage Houses (Market Intermediaries). Articles 113, 115, 142 and second section. URL: http://www.cnbv.gob.mx/Anexos/Anexo%2012%20CUCB.pdf

As part of Operational Risk requirements, intermediaries must maintain an historical database with the record of all “loss events due to operational risks”.

4.2 Steps taken in the United States

4.2.1 Steps taken by the CFTC:

Recognizing the need to strengthen the security and resilience of financial markets against cyber attacks, which pose a new risk to financial stability, the CFTC addresses cyber security for intermediaries in the context of risk management through the following requirements:

- Requiring identification of risk (including technological risk), a description of risk tolerance limits and underlying methodology in the written policies and procedures of technological and other applicable risks in the Risk Management Program of each futures commission merchant;
- Regular review of the risk tolerance limits (quarterly by senior management and annually by the governing body);
- Requiring periodic risk exposure written reports for all applicable risks, including technological risks, any recommended or completed changes to the Risk Management Program, the recommended time frame for implementing recommended changes, and the status of any incomplete implementation of previously recommended changes to the Risk Management Program. Such reports shall be provided quarterly to senior management and immediately to senior management and the governing body upon detection of any material change in the risk exposure of the futures commission merchant, and must be submitted to the Commission within five business days of doing so;
- Requiring notice to the Commission within 24 hours, in case of a material change in operations or risk profile changes in the senior management of the futures commission merchant, the establishment or termination of a line of business, or a material adverse change in the futures commission merchant's clearing arrangements; and
- Helping to protect investors by ensuring that CFTC-regulated intermediaries create programs to address identity theft risk. The rules in this area require intermediaries to adopt written identity theft programs that would include reasonable policies and procedures to: identify relevant red flags; detect the occurrence of identity theft; respond appropriately; and perform periodic updates.

The CFTC Division of Swap Dealer and Intermediary Oversight outlined best practices for intermediaries regarding security safeguards for the protection of customer records and information. These best practices encourage intermediaries to develop, implement and maintain an appropriate written information security and privacy program which would include: (i) designating an employee with privacy and security oversight duties and training relevant staff members; (ii) identifying, in writing, all reasonably foreseeable internal and external risks to security, confidentiality, and integrity of personal information; (iii) establishing processes, safeguards and controls to assess and mitigate risks, as well as relevant testing and evaluation procedures; and (iv) providing annual assessments to the security and privacy program, and possible adjustments, internally.

In addition, in October 2015 the CFTC approved the National Futures Association (NFA)[76] Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49 entitled Information Systems Security Programs, which becomes effective on March 1, 2016. The Interpretive Notice requires NFA Member firms to adopt and enforce written policies and procedures to secure customer data and access to their electronic systems. It also requires the adoption and enforcement of information systems security program (ISSP) appropriate to its circumstances, which should contain: (i) a security and risk analysis; (ii) a description of the safeguards against identified system threats and vulnerabilities; (iii) the process for evaluating the nature of a detected security event, understanding its potential impact, and taking appropriate measures to contain and mitigate breaches; and (iv) a description of ongoing education and training for information systems security for all appropriate personnel of an NFA Member. The ISSP must be approved by NFA Member firms by an executive-level official and must be monitored and regularly reviewed, at least annually.

4.2.2 Steps taken by FINRA:

In February 2015, FINRA issued a comprehensive report that details specific practices that intermediaries can tailor to their business models as they strengthen their cyber security efforts. FINRA set forth eight general principles as well as effective practices to implement the principles. The principles and practices are set forth below.

1. Governance and Risk Management for Cyber Security

Firms should establish and implement a cyber security governance framework that supports informed decision making and escalation within the organization to identify and manage cyber security risks. The framework should include defined risk management policies, processes and structures coupled with relevant controls tailored to the nature of the cyber security risks the firm faces and the resources the firm has available. Effective practices include:

- defining a governance framework to support decision making based on risk appetite;
- ensuring active senior management, and as appropriate to the firm, board-level engagement with cyber security issues;
- identifying frameworks and standards to address cyber security;
- using metrics and thresholds to inform governance processes;
- dedicating resources to achieve the desired risk posture; and
- performing cyber security risk assessments.

2. Cyber Security Risk Assessment

Firms should conduct regular assessments to identify cyber security risks associated with firm assets and vendors and prioritize their remediation. Effective practices include establishing and implementing governance frameworks to:

- identify and maintain an inventory of assets authorized to access the firm's network and, as a subset thereof, critical assets that should be accorded prioritized protection; and

[76] For a description of the NFA and its role, see https://www.nfa.futures.org/NFA-about-nfa/index.HTML.

- conduct comprehensive risk assessments that include:
  - an assessment of external and internal threats and asset vulnerabilities; and
  - prioritized and time-bound recommendations to remediate identified risks.

3. Technical Controls

Firms should implement technical controls to protect firm software and hardware that stores and processes data, as well as the data itself. Effective practices include:

- implementing a defense-in-depth strategy;
- selecting controls appropriate to the firm's technology and threat environment, for example:
  - identity and access management;
  - data encryption; and
  - penetration testing.

4. Incident Response Planning

Firms should establish policies and procedures, as well as roles and responsibilities for escalating and responding to cyber security incidents. Effective practices for incident response include:

- preparation of incident responses for those types of incidents to which the firm is most likely to be subject, e.g., loss of customer personally identifiable information, data corruption, DDoS attack, network intrusion, customer account intrusion or malware infection;
- incorporation of current threat intelligence to identify the most common incident types and attack vectors;
- containment and mitigation strategies for multiple incident types;
- eradication and recovery plans for systems and data;
- investigation and damage assessment processes;
- preparation of communication/notification plans for outreach to relevant stakeholders, e.g., customers, regulators, law enforcement, intelligence agencies, industry information-sharing bodies;
- involvement in industrywide, and firm-specific, simulation exercises as appropriate to the role and scale of a firm's business; and
- implementation of measures to maintain client confidence, including:
  - provision of credit monitoring services for individuals whose personal information has been compromised to identify potential identity theft or fraud; and
  - reimbursement of customers for financial losses incurred.

5. Vendor Management

Firms should manage cyber security risk that can arise across the lifecycle of vendor relationships using a risk-based approach to vendor management. Effective practices to manage vendor risk include:

- performing pre-contract due diligence on prospective service providers;
- establishing contractual terms appropriate to the sensitivity of information and systems to which the vendor may have access and which govern both the ongoing relationship with the vendor and the vendor's obligations after the relationship ends;
- performing ongoing due diligence on existing vendors;
- including vendor relationships and outsourced systems as part of the firm's ongoing risk assessment process;
- establishing and implementing procedures to terminate vendor access to firm systems immediately upon contract termination; and
- establishing, maintaining and monitoring vendor entitlements so as to align with firm risk appetite and information security standards.

6. Staff Training

Firms should provide cyber security training that is tailored to staff needs. Effective practices for cyber security training include:

- defining cyber security training needs requirements;
- identifying appropriate cyber security training update cycles;
- delivering interactive training with audience participation to increase retention; and
- developing training around information from the firm's loss incidents, risk assessment process and threat intelligence gathering.

7. Cyber Intelligence and Information Sharing

Firms should use cyber threat intelligence to improve their ability to identify, detect and respond to cyber security threats. Effective practices include:

- assigning responsibility for cyber security intelligence gathering and analysis at the organizational and individual levels;
- establishing mechanisms to disseminate threat intelligence and analysis rapidly to appropriate groups within the firm, for example, the firm's risk management and front-line information technology security staff;
- evaluating threat intelligence from tactical and strategic perspectives, and determining the appropriate time frame for the course of action; and
- participating in appropriate information sharing organizations—e.g., FS-ISAC—and periodically evaluating the firm's information-sharing partners.

8. Cyber Insurance

Firms should evaluate the utility of cyber insurance as a way to transfer some risk as part of their risk management processes. Effective practices include:

- for firms that have cyber security coverage, conducting a periodic analysis of the adequacy of the coverage provided in connection with the firm's risk assessment process to determine if the policy and its coverage align with the firm's risk assessment and ability to bear losses; and

- for firms that do not have cyber insurance, evaluating the cyber insurance market to determine if coverage is available that would enhance the firm's ability to manage the financial impact of cyber security events.

4.2.3 Steps taken by the SEC:

Among other aspects,[77] the SEC has focused on cyber security risk issues for registered investment advisers, broker-dealers and funds, including, for example, data protection and identity theft vulnerabilities. In this area, the SEC adopted, in 2013, Regulation S-ID, which requires certain regulated financial institutions and creditors to adopt and implement identity theft programs.[78] S-ID builds upon the SEC's existing rules for protecting customer data, in particular Regulation S-P.[79]

4.3 Conclusions concerning intermediaries

This chapter has provided a description of some of the measures adopted by regulators and other organizations to enhance the oversight of cyber security in the context of intermediaries. The review has highlighted that jurisdictions tend to approach cyber security in a similar fashion to the extent that they have expressed comparable expectations regarding intermediaries' cyber security practices, by focusing for instance on the adequacy of their internal controls. They have, however, adopted diverse approaches in communicating these expectations, ranging from adopting high-level regulatory requirements, to more granular approaches such as outlining best practices and publishing reports that detail specific practices that may be adopted by intermediaries. Recognizing that each regulator operates in different institutional and market environments, the review of regulatory initiatives contained in this chapter highlights a number of avenues that could be considered for adoption by other IOSCO members. Note that approaches adopted by regulators tend to allow for flexibility in how they are implemented by intermediaries.

Further, we encourage intermediaries to consider the description of cyber security practices contained in Chapters 3 and 5 that are related to trading venues and asset managers, as well as other available materials.[80] The CPMI-IOSCO draft guidance on financial market infrastructures, which is described in Chapter 6, could also potentially be relevant to intermediaries in some instances, and could be used by them to enhance their cyber resilience. As was observed earlier, there is no "one size fits all" approach, and different segments of securities markets may require different approaches to cyber security. Nonetheless, there are some commonalities in approaches adopted, and the description of cyber security practices in other segments of securities markets can be relevant in the context of intermediaries.

---

[77] See Chapter 1 for a more complete description of steps taken by the SEC in regards to cyber security.

[78] See Identity Theft Red Flags Rules, Release No. 34-69359 (April 10, 2013), available at: http://www.sec.gov/rules/final/2013/34-69359.pdf

[79] See Final Rule: Privacy of Consumer Financial Information (Regulation S-P) (November 13, 2000), available at http://www.sec.gov/rules/final/34-42974.htm

[80] See list of references in the Appendix, including among other sources SIFMA's Cybersecurity Resource Center.

Chapter 5 – Asset managers

This chapter pertains to cyber security in the specific context of asset managers. It is based on a large extent on a contribution from IOSCO's AMCC, which was reviewed by IOSCO's Committee 5 on Investment Management (C5). In order to develop a better understanding of the trends and practices in cyber security within the asset management sector of the financial services industry, a small AMCC working group[81] was created with an initial objective to develop and administer a global cyber security benchmarking survey. Drawing on the results of that survey and other materials, the following highlights the main potential cyber security risks for asset managers, presents the high-level results of the survey, and provides some concluding remarks.

5.1 Threat landscape

Data theft, which goes to data confidentiality, is a significant concern for asset managers, and appropriately so. The industry is also acutely aware of the threat to data integrity; the manipulation of data such as net asset values, trading algorithms, portfolio holdings, etc., are highlighted by asset managers as growing areas of concern. Whereas the industry, in general, has mostly experienced attacks on the confidentiality (data theft) and availability of systems (DDoS), the potential consequences of a data integrity attack are potentially far more serious. A partial list of some of the threats the industry faces include:

- the theft or manipulation of trading information and information regarding investment strategies, as well as other market-sensitive information;
- the theft or manipulation of trading algorithms and the underlying codes;[82]
- the threat posed by trusted insiders;[83] and
- other risks such as ransomware, or manipulation of valuation models, and other general intellectual property theft.

The U.S. SEC's data from 2014 shows that an average of 74% of advisers stated that they had experienced cyber attacks directly or through one of their vendors.[84] The following table illustrates some of the threats, with differing implications in terms of financial and reputational damage, loss of competitive advantage, as well as legal and regulatory non-compliance issues. The relevance and severity of those threats depend on the business model of the individual asset manager and its risk profile. In addition, the possible impacts (and costs) also are a function of the amount of time an adversary has access to a system before the attack is identified and mitigated.

---

81 The AMCC WG was chaired by ICI Global and also included ANBIMA, EFAMA, KOFIA, the Hedge Funds Standards Board (HFSB), as well as the CFA Institute. In addition to the presentation of the AMCC Cybersecurity Benchmarking Survey, this contribution is largely based on existing materials from ICI and the Hedge Funds Standards Board. See notably, ICI *Information Security Centre*, https://www.ici.org/info_security, and HFSB, *Cyber Security Memo*, http://www.hfsb.org/files/cybersecurity_hfsb_toolbox_.pdf

82 Cybercriminals target trading algorithms, Financial Times, 22 February 2015.

83 E.g. *Morgan Stanley Fires Employee Over Client-Data Leak*, WSJ, 5 January 2015.

84 U.S. Securities and Exchange Commission, *Cybersecurity Examination Sweep Summary*, Feb. 2015, http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf

Targeting asset managers: illustration of potential threats

Target	Impact	Other considerations
Client data / shareholder information	HIGH Reputation/headline risk Investor trust Regulatory action	Possible threats on confidentiality (spying/publication on the internet) or integrity (destruction/manipulation/sabotage) Indirect threat of cyber attacks on service providers who hold or have access to a firm's critical data or network Possible second order effects (e.g. stolen data used to pursue clients)
Proprietary algorithms / strategies	MEDIUM-HIGH Business damage Investor trust	Function of sophistication/digitization of process (e.g. automated Commodity Trading Advisor (CTA) vs. discretionary manager)
Trading book	MEDIUM Business damage/ reputation risk Investor trust	Particularly relevant to active managers Risk of short squeeze
Ability to execute trades	MEDIUM-HIGH Fund at risk Investor trust	Particularly relevant to automated traders; manual/voice-based fall back solutions
Public website / client login	LOW-MEDIUM Reputation/ headline risk	Public visibility of damage might require a swift and proactive approach to communicate with clients and, possibly, regulators

Source: HFSB.

As the risks become more palpable, and focus from regulators and investors on cyber security risks increase, asset managers have continued to increase their efforts to address the threat and strengthen their resilience. The AMCC Cybersecurity Benchmarking Survey was aimed at assessing the prevalence of some security practices across a broad spectrum of managers. The methodology and high-level findings are presented in the following section, before we provide additional examples of some prudent practices.

5.2 The AMCC Asset Management Cybersecurity Benchmarking Survey

5.2.1 Methodology

The survey consisted of approximately 85 questions covering such areas as corporate structure, policies and procedures, encryption, access control, and training. The survey was distributed to individual asset managers via the members of the AMCC working group.[85] Respondent's identities were kept anonymous and only aggregated results were produced. Globally, 195 asset managers responded to the survey providing a wide sample of firms from large multi-national to small regional participants. The survey is expected to be administered annually.

Given the diversity of the global asset management sector, from large firms with multinational presence to small local niche providers of financial products, what is an appropriate information security program for one firm may be wholly inappropriate for another when risk profile and resources are taken into consideration. As such, only general inferences can be made from these survey results and they may be perishable as threats and vulnerabilities evolve.

5.2.2 High-level findings

Some general findings of this initial exercise include:

1) widespread practice of ensuring an information security program is consistent with a recognized security framework or parts of various frameworks;

2) the use of long and complex passwords;

3) periodic inventory of physical devices, software, and applications; and

4) having a detailed, written incident response plan.

Some examples of the changing nature of information security are highlighted in the table below. These changes are reflective of a deeper understanding of cyber security risk from years past. There are, however, other results that require more careful interpretation such as the use of personal email accounts, access to social media platforms, and the degree to which some functions (e.g. email, disaster recovery, application development) are outsourced. The responses to these questions appear to be a function of firm size and the allocation of resources in order to, for example, appropriately monitor, capture, and subsequently produce communications via a third party platform. It is expected that the working group will further refine certain questions and response options to be able to get additional detail in future surveys.

[85] In addition to ANBIMA, EFAMA, ICI and KOFIA, which all encouraged their members to respond to the survey, a few other associations representing investment managers were also contacted. It is expected that, at the next iteration of the survey, more associations will take part in the exercise.

Illustrative findings from the AMCC Cybersecurity Benchmarking Survey on the changing nature of information security

- 45% of firms employ a named Chief Information Security Officer (CISO) and in only 25% of the cases does the CISO report to the Chief Information Officer;
- 79% of firms have made certain their security architecture is consistent with one, or an amalgam of, recognized security frameworks (e.g. ISO, NIST, etc.);
- 75% of firms require all employees to undergo information security training, while 20% are considering doing so;
- There is mixed perspective on cloud-based file sharing applications: 38% of respondents use them, 56% don't, 5% are considering;
- 40% of firms have contracted cyber security insurance policies and 18% are considering doing so;
- 43% of firms have information sharing arrangements in place to exchange information regarding possible cyber threats.

Source: AMCC Working Group. The survey was conducted in July and August 2015. A total of 195 individual asset managers responded voluntarily to the questionnaire, although not all respondents responded to all questions.

5.3 Selected prudent practices for investment managers

The AMCC Benchmarking Survey provides some preliminary evidence of a broad and increasing adoption of good cyber security practices across the investment management industry. Some actions are relatively basic but effective in preventing most breaches. Others, such as the development of a detailed incident response plans, are more challenging to implement and require more time and effort from firms. Firms should appropriately allocate their resources to their defense mechanisms but as perfect security is not feasible, re-doubling efforts on response capabilities is essential.

Prudent practices identified in the AMCC Benchmark Survey include:

- Identify the **firm's key digital assets** (including intellectual property, critical business processes, shareholder information and other confidential data, and key operating facilities) to allocate resources where the risks may be higher for the firm; firms should develop a clear understanding of normal network functions, activity, and links;

- Implement effective **control and protection measures**, involving, among other tools, username and password protection, control of administrative and privileged access, removal of "undesirable" applications, anti-virus protection, mobile device security, and encryption of data;

- Implement **ongoing training** for employees (including legal staff) and develop an effective security culture of responsibility and accountability throughout the firm;

- Ensure an appropriate **monitoring** of system and data usage to facilitate the identification of abnormal patterns;

- Develop **detailed and actionable incident response plan**, with clear roles and responsibilities, communication procedures and possible remediation measures; when an incident does occur, firms should be prepared to document their actions;

- Access and share actionable threat **information,** as well as building peer network to share expertise and increase circles of trust that include law enforcement;

- Engage with **third parties** to conduct due diligence reviews of a service providers' information security program, and understand if 4th party service providers are utilized; and
- Ensure an **ongoing reassessment** of the firm's cyber resilience, its vulnerabilities, and protection, including by benchmarking against industry practices and peers.

5.4 Concluding remarks

5.4.1 Regulatory approaches

Regulators around the globe have taken different approaches to cyber security concerns. Some focus on specific management arrangements to address cyber threats (e.g. policies, procedures, etc.). Other regulators have a more principles-based approach, whereby cyber security is covered by the broader conduct obligations/operational risk management arrangements.[86]

In addition to clarifying their expectations with regard to how firms approach cyber security, regulators have started conducting specific examinations,[87] and an increasing number of investment managers may start to be sanctioned for failings in their cyber security practices.[88]

Generally, many regulators promote a robust cyber security posture across the industry through guidance. It is broadly acknowledged that a detailed and prescriptive approach to regulating "cyber security risk" is unlikely to work, given the pace of technological innovation, the changing sophistication of adversaries, the expansion of the threat landscape, and the fact that there cannot be a "one-size-fits-all" approach.

5.4.2 Role for industry initiatives

Various industry associations have launched, or are considering launching, initiatives aimed at supporting their members' efforts at strengthening their cyber security posture. Initiatives such as industry conferences,[89] where information security practitioners share experiences, help raise awareness, educate attendees, and disseminate information about cyber threats. Attack simulation exercise may also be organized. For instance, a HFSB "Table top" attack simulation exercise took place for the first time in December 2015, mirroring other cyber security exercises which previously mostly focused on other segments of the industry (e.g. Quantum Dawn in the United States).

---

86 See HFSB Cybersecurity Toolbox (Appendix A) for an overview of existing regulatory requirements, guidance and approaches to cyber security.

87 E.g., U.S. SEC, Office of Compliance and Examinations' 2015 Cybersecurity Examination Initiative, Sep. 2015; Central Bank of Ireland, Review of the management of operational risk around cybersecurity with the investment firm and fund services industry, Sep. 2015.

88 E.g., *SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach*, 22 September 2015.

89 For instance, ICI held its Second Annual Cybersecurity Forum on Thursday, November 5 in Washington, DC.

Chapter 6 – Financial market infrastructures

The safe and efficient operation of FMIs is essential to maintaining and promoting financial stability and economic growth. If not properly managed, FMIs can be sources of financial shocks, such as liquidity dislocations and credit losses, or a major channel through which these shocks are transmitted across domestic and international financial markets. In that context, the joint CPMI-IOSCO Working Group on Cyber Resilience (WGCR) was established in September 2014 to address issues cyber risk may pose to the well functioning of FMIs and to financial stability. Drawing to the extent possible upon previous and current CPMI and IOSCO work, the WGCR's mandate is to further investigate the implications of cyber attacks against FMIs, including financial stability implications, and consider any guidance as necessary and appropriate for both authorities (regulators, overseers) and FMIs.

The WGCR has notably released for comments a draft document to provide guidance for FMIs to enhance their cyber resilience.[90] The draft guidance outlines five primary risk management categories and three overarching components that should be factored across an FMI's cyber resilience framework. The risk management categories are: governance; identification; protection; detection; and response and recovery. The overarching components are: testing; situational awareness; and learning and evolving. In order to achieve resilience objectives, investments across these guidance categories can be mutually reinforcing and should be considered jointly. Below are short overviews of each category and components.

Governance: Consistent with effective management of other forms of risk faced by an FMI, sound governance is key. Effective governance should start with a clear and comprehensive cyber resilience framework that accords a high priority to the safety and efficiency of the FMI's operations while supporting broader financial stability objectives. The framework should define the FMI's cyber resilience objectives, as well as the requirements for people, processes and technology necessary to manage cyber risks. This framework should include timely communication and collaboration with relevant stakeholders.

Identification: Given that FMIs' operational failure can negatively impact financial stability, it is important that FMIs identify their critical business functions and supporting information assets that should be protected, in order of priority, against compromise. The chapter on identification outlines how an FMI should identify and classify business processes, information assets, system access and external dependencies.

Protection: Cyber resilience depends on effective security controls that protect the confidentiality, integrity and availability of FMIs' assets and services. The chapter on protection urges FMIs to implement appropriate and effective controls and design systems and processes in line with leading cyber resilience and information security practices to prevent, limit and contain the impact of a potential cyber incident.

Detection: An FMI's ability to detect the occurrence of anomalies and events indicating a potential cyber incident is essential to strong cyber resilience. Early detection provides an FMI with useful lead time to mount appropriate countermeasures against a potential breach, and allows proactive containment of actual breaches. Given the stealthy and sophisticated nature of cyber attacks and the multiple entry points through which a compromise could take place, advanced capabilities to extensively monitor for anomalous activities are needed.

[90] See https://www.iosco.org/library/pubdocs/pdf/IOSCOPD513.pdf

Response and recovery: Financial stability may depend on the ability of an FMI to settle obligations when they are due, at a minimum by the end of the value date. An FMI should design and test its systems and processes to enable the safe resumption of critical operations within two hours of a cyber disruption and to enable itself to complete settlement by the end of the day the disruption occurred, even in the case of extreme but plausible scenarios. Although authorities recognize the challenges that FMIs face in achieving cyber resilience objectives, it is also recognized that current and emerging practices and technologies may serve as viable options to attain those objectives.

Testing: Once employed within an FMI, all elements of a cyber resilience framework should be rigorously tested to determine their overall effectiveness. Sound testing regimes produce findings that should be used to identify gaps against stated resilience objectives and provide credible and meaningful inputs to the FMI's management of cyber risks.

Situational awareness: Strong situational awareness can significantly enhance an FMI's ability to understand and pre-empt cyber events, and to effectively detect, respond to and recover from cyber attacks that are not prevented. Specifically, a keen appreciation of the threat landscape can help an FMI better understand the vulnerabilities in its critical business functions, and facilitate the adoption of appropriate risk mitigation strategies.

Learning and evolving: The last chapter emphasizes the importance of implementing an adaptive cyber resilience framework that evolves with the dynamic nature of cyber risks and strategies to mitigate those risks. FMIs should aim to instill a culture of cyber risk awareness and demonstrate ongoing re-evaluation and improvement of their cyber resilience posture at every level within the organization.

While the guidance is directly aimed at FMIs, the document also notes that it is important for FMIs to take on an active role in outreach to their participants and other relevant stakeholders to promote understanding and support of resilience objectives and their implementation. Given the extensive interlinkages and interdependencies in the financial system, adequate cyber security practices at an FMI do not necessarily ensure cyber resilience in the markets it serves. In particular, the markets' overall cyber resilience is dependent not only on the resilience of a single FMI, but also on that of interconnected FMIs, of service providers and of the participants.

The guidance could potentially be relevant to other securities market participants, and could be considered by them to enhance their cyber resilience. Its content is consistent with the approach taken in this document, which is to present a broad range of tools that may be relevant to market participants and regulators depending on the specific circumstances under which they operate. We therefore encourage market participants to consult this guidance and determine the extent to which it might be relevant for them.

Chapter 7 – Information sharing and the role of securities regulators

Information sharing is central to cyber security. It provides numerous benefits by allowing organizations to tap into a broader community's capabilities, knowledge and experience related to cyber security. It can provide an organization with a better understanding of the cyber security landscape, including techniques used by cyber criminals. Information sharing can also allow organizations to emulate the measures put in place by others to prevent, detect, and respond to cyber attacks. Ultimately, information sharing can reduce systemic risks by enabling entities or systems to promptly react to a cyber threat.[91]

In order to investigate further issues related to cooperation and sharing of information on cyber security, the IOSCO Cyber Risk Coordinators organized an international roundtable on September 14, 2015 in Montreal, Canada ("the Montreal roundtable"). The meeting attracted more than twenty high-level officials from the industry and the regulatory community across various jurisdictions. The discussion allowed for the development of a deeper and broader understanding on the current state of information sharing, the different models of successful information sharing initiatives, the hurdles to information sharing, and the potential roles for regulators and IOSCO. This chapter integrates some of the key takeaways from the Montreal roundtable.

7.1 A primer on information sharing

There are basically two types of information that can be shared:

1) Technical/operational information: This type of information is technical in nature. In many instances, this information can be transferred in real-time and in an automated fashion, from computer to computer. It can relate to vulnerabilities, cyber security threats, or incident information. Examples of such information include malicious file hashes, URLs, domains and IP addresses.

2) Strategic information: This type of information is more detailed and provides more contextual evidence. Similarly to more technical information, it can relate to vulnerabilities, cyber security threats, or incident information. But it is difficult to automate and to transmit in real-time due to the fact that it might include detailed and specific information about threat actors, techniques used, and corrective measures put in place. It can also be more general in nature, such as the sharing on best approaches to cyber security.

7.2 The role of securities regulators in information sharing

In general terms, governments have an integral role to play in promoting and facilitating the sharing of cyber security information among industry participants and governments. Governments can help establish and promote networks for information sharing and remove legal impediments to that sharing. Governments can also be active participants in information

[91] Source : Center for Strategic & International Studies, "Cyber Threat Information Sharing: Recommendations for Congress and the Administration," March 2015, Denise E. Zheng and James A. Lewis

sharing networks; many governments have access to the latest technologies and to cyber threat intelligence that can usefully be shared with market participants.

Securities regulators can also promote and benefit from information sharing. Given the nature of their mandates, securities regulators typically place greater emphasis on strategic rather than technical information because it provides more context and details. Such information can provide regulators with more information on the types of threats faced by market participants, on their cyber security practices, and on their general level of preparedness. Ultimately, this information can help ensure that rules, regulations, and supervisory activities are effective and appropriate.

Participants in the Montreal roundtable argued that many of the most successful information sharing initiatives are led by the private sector. These participants were of the view that regulators can encourage the participation of regulated entities in these initiatives but should not try to establish new or competing initiatives. Examples of successful information sharing networks tend to be bottom-up structures, which are established and operated by and for the membership. These networks tend to be associated with higher levels of trust among participants, which entails a very slow building process. Accordingly, participants suggested that regulators may not want to impose a specific network in which to participate, but rather encourage participation in any network that meets certain pre-specified criteria in terms, notably, of the type and quality of the information shared. The information shared should be relevant and actionable.

The participants were of the view that, as part of their regulatory framework, securities regulators can therefore usefully require or encourage market participants to participate in information sharing networks in an effort to ensure they have in place appropriate cyber security measures. As discussed above, information sharing is perceived as an integral part of any effective cyber security framework, and regulators may therefore usefully require or encourage such sharing as part of their regulatory/supervisory framework.

Participants in the Montreal roundtable did caution, however, that participation in these information sharing networks may not be suited for all types of firms, notably those of smaller sizes. Firms are often overwhelmed by the amount of information they receive. And smaller firms may not have the capacity or the technological sophistication to process and act on the information received. Among others, regulators can share high-level information with smaller firms – drawing for instance on government intelligence – to help alleviate some of these capacity or sophistication constraints.

Participants in the Montreal roundtable highlighted that information confidentiality and legal hurdles are important impediments to effective information sharing. Participants noted that regulators can potentially contribute to reducing the many legal hurdles to effective information sharing among market participants. For example, regulators can initiate a conversation with their government in order to make sure that entities sharing such information are protected from liabilities. Legal issues regarding information sharing, ranging from data and privacy protection issues, liability protection matters to potential antitrust concerns, remain a challenge in many countries.[92]

[92] *Preliminary fact-finding exercise,* Cyber-Resilience Task Force of the Affiliate Members Consultative Committee (AMCC) of IOSCO, December 2014.

Participants noted that information related to cyber security is often sensitive in nature and can affect the reputation of an organization and lead to potential legal and regulatory consequences. Trust is therefore essential for information sharing networks. Organizations will naturally be reluctant to share information if they do not have confidence in the fact that other organizations that will have access to this information will use it confidentially and as intended. Some participants noted that the direct participation of regulators in information sharing networks may in some instances discourage participants to share relevant information for fear of regulatory action. More broadly, participants were of the view that regulators can contribute to ensuring that market participants have the appropriate incentives to actively participate in information sharing networks.

An Overview of the Financial Services Information Sharing and Analysis Center

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is a global initiative for cyber and physical threat intelligence analysis and sharing for the financial services industry. Its mission is to share timely, relevant, actionable cyber and physical security information and analysis. It is a nonprofit private sector initiative but collaborates closely with various government entities. It was formed in 1999, in response to a 1998 U.S. Presidential Directive.

The FS-ISAC has grown tremendously in recent years, from 68 members in 2004 to about 5700 members in 2015. It processes thousands of threat indicators per month in an effort to mitigate cyber crime, hacktivist and nation state activity. It also contributes to the development and testing of crisis management procedures for the financial sector in collaboration with other industry bodies. The types of information shared include:

- Malicious sites
- Threat actors and their objectives
- Threat indicators
- Threat actors tactics, techniques and procedures
- Exploit targets
- Denial of services attack
- Malicious emails: phishing/spearfishing
- Software vulnerabilities
- Malicious software

The FS-ISAC, in collaboration with The Depository Trust & Clearing Corporation (DTCC), launched in 2014 a cyber threat intelligence initiative known as *Soltra*. The purpose of this initiative is to deliver software automation and services that collect, distill and speed the transfer of threat intelligence from multiple sources to help safeguard against cyber attacks. It leverages open standards including Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII).

In addition to encouraging the participation in an information-sharing network, some securities regulators also require the disclosing of cyber attacks to them.[93] These regulators tend to require the disclosure of material attacks that may have had an impact on the operations of a regulated entity or on the confidentiality of consumer information. The requirement or the encouragement to participate in information sharing networks on the part of regulators is often separate from the requirement to disclose material cyber attacks.

Requiring the disclosure of material cyber attacks to regulators can serve a number of objectives. This disclosure can help regulators determine on an on-going basis if regulated entities are taking actions that are appropriate given the regulatory framework under which they operate. More broadly, this disclosure can help ensure that the overall regulatory framework is effective and appropriate. The disclosure of cyber attacks can also inform the audits or sweeps performed by regulators. For instance, the strategic information gathered could help inform actions which could be taken through the regulatory/supervisory framework to mitigate the risks revealed by a cyber attack. The sharing of strategic information can more generally ensure that regulatory audits actually add value in terms of enhancing cyber security by addressing issues that would be most relevant to a particular firm and the market in which it operates, consistent with a risk-based approach to securities regulation.

7.3 The sharing of information among regulators at the international level

Given the international nature of cyber risk, there is a widespread recognition that information sharing at the international level is essential. And international organizations such as IOSCO, as some have suggested, may be well placed to establish mechanisms at the international level to promote greater cross-jurisdiction information sharing.

Some information is currently shared at the international level but not necessarily in a structured way. Also, some organizations have set up information sharing networks that are now operating at the international level, but they do not operate seamlessly between jurisdictions.

Furthermore, securities regulators can and do share information in an effort to enforce and secure compliance with their respective securities laws and regulations. Under the IOSCO's Multilateral Memorandum of Understanding (MMoU), regulators can exchange information concerning a securities related offence involving a cyber attack. IOSCO's Committee 4 on Enforcement and the Exchange of Information and the Multilateral Memorandum of Understanding Screening Group (C4) considered the IOSCO MMoU framework for information sharing in the context of cyber crime.[94] For this purpose, C4 members considered the extent to which the MMoU could be used in the context of any act which involves a computer or network of computers leading to misselling, misappropriation of assets, market abuse, disruption to firms' systems and controls and / or sabotage of firms or market infrastructure. That is to say, the "act", must have some nexus to misconduct, which falls

---

[93] For instance, in Canada, *National Instrument 21-101 Marketplace Operation* requires marketplaces to promptly notify the regulator "of any material systems failure, malfunction, delay or security breach and provide timely updates on the status of the failure, malfunction, delay or security breach, the resumption of service and the results of the marketplace's internal review of the failure, malfunction, delay or security breach."

[94] A report with C4's analysis, conclusions and recommendations was presented to the IOSCO Cyber risk Coordinators in April 2015. The following is based to a large extent on their report.

within a regulator's remit. To that extent, such an act will usually exclude purely criminal actions.

7.3.1 How the MMoU can be of assistance to regulators in the context of cyber attacks which stem from securities offences

The MMoU provides that:

> *"The Authorities will, within the framework of this Memorandum of Understanding, provide each other with the fullest assistance permissible to secure compliance with the respective Laws and Regulations of the Authorities."*

The scope of the Laws and Regulations covered by the MMoU is broad, and encompasses a wide variety of activities and topics, such as those mentioned under Paragraphs 4(a) and (c):

- *"insider dealing, market manipulation, misrepresentation of material information and other fraudulent or manipulative practices relating to securities and derivatives, including solicitation practices, handling of investor funds and customer orders";*
- *"markets, exchanges, and clearing and settlement entities".*

Although to date few requests for assistance have been made to investigate a securities offence arising from a cyber crime, it is likely that such requests would be complied with under the current MMoU. The Laws and Regulations of the MMoU cover all the relevant securities offences and all potential victims and perpetrators that are likely to arise from a cyber crime.

The MMoU provides a non-exhaustive description of the assistance that signatories undertake to provide one another. This includes obtaining information, documents, records and testimony held in any form, which is generally accepted to include electronic records. The information requested can be directly or indirectly linked to the offence investigated by the requesting authority. For example, the request may target the perpetrators of a market disruptive cyber attack or a web-based "pump & dump" scheme. The request may also be aimed at compelling testimony from witnesses or unwilling participants or victims of a scheme, who may hold vital information to the case being investigated.

C4 members concluded that the MMoU is sufficiently flexible in allowing assistance to be sought when investigating breaches of securities laws that involve cyber crime. This assertion is supported by the Objectives of securities regulation and by the IOSCO Principles relating to cooperation, which stress the importance of cooperation channels in cross-border enforcement cases and for other regulatory purposes.

7.3.2 Examples of how the MMoU can be of assistance to regulators in the context of cyber attacks

In the cyber crime report C4 presented a series of examples of cyber crime in financial markets. These examples are intended to provide more information on how the MMoU played or can play a role in assisting regulators with their investigations.

Example 1 – Hacking of a trading account

A client of a securities broker discovered that his share trading account had been hacked and a sell order fraudulently placed on his behalf. The proceeds of the sale were paid to the fraudsters, who then transferred the monies to an account in a foreign jurisdiction.

When investigating the client's complaint, the brokerage firm discovered weaknesses in its systems that exposed its clients to these sorts of attacks. It self-reported to its regulator, who then opened a formal enforcement investigation into the adequacy of the firm's systems and controls to protect its clients (the fraud was being handled separately by the police).

In order to obtain evidence in its investigation, the regulator needed to establish where the proceeds of the unauthorized sale of the securities had been transferred to, and the identity of the beneficial owner of the account to which they were sent overseas.

It therefore made a request under the MMoU to the overseas regulator in the jurisdiction where the bank account was located.

Example 2 – Market manipulation relating to high frequency trading

The requesting authority was investigating suspected market manipulation activities relating to high frequency trading in stocks on the markets that it regulated. The firm suspected of carrying out the manipulative high frequency trading was located overseas.

The requesting authority was interested in obtaining from the firm the algorithms that executed pre-programmed trading instructions in order to determine whether the trading was legitimate, reflecting investment strategy and management of trading and risk, or whether it was in fact abusive, aimed at causing volatility. It therefore made a request under the MMoU as the algorithms fell within the very broad definition set out in paragraph 7(b) of the MMoU.

Example 3 – Scenario involving a broker-dealer computer-trading glitch

A broker-dealer experiences significant losses as a result of a computer-trading glitch caused by an error in its software. It is unlikely that the computer-trading glitch in and of itself would lead an authority to make a request under the MMoU. However, if there were suspicion that some form of offence in financial markets had been committed in the requesting authority's jurisdiction, such as the glitch being intentionally caused to allow some form of market manipulation, then the MMoU would likely be relevant. If the requesting authority suspected that insider dealing was occurring in its jurisdiction, based on material non-public information related to the glitch or the talks with potential buyers, it could under the MMoU request information on the basis of an insider dealing investigation to confirm its suspicions.

7.4 The sharing of information at the international level – outstanding issues

Over and beyond information related more narrowly to enforcement actions, there may be a need for regulators to exchange information on cyber risk more broadly given their responsibilities to ensuring that markets are fair, efficient and transparent and to reducing systemic risk. To the extent that some regulators require disclosure of cyber attacks from regulated entities, and that they might otherwise gather information on cyber risk in the

conduct of their regulatory and supervisory responsibilities, regulators might benefit from greater cross-jurisdiction information sharing.

Regulators could exchange among them strategic information on threats, vulnerabilities, and cyber attacks that could be ultimately relevant for their regulated entities. The focus could be on trends and typologies relevant to the work of securities regulators. The information that could be shared includes:

- The methods used by cyber criminals;
- The vulnerabilities which have been exploited;
- The ways in which similar attacks could be prevented in the future; and
- Emerging cyber risk trends

From such information, conclusions could be drawn on actions that could be taken globally to mitigate the risks revealed by cyber attacks. More broadly, regulators could beneficially learn about regulatory approaches adopted in other jurisdictions. And such interaction could lead over time to greater convergence, to some extent, of the various approaches to the regulation of cyber security.

To prevent violations of privacy, data spill and misuses of information, care would have to be taken to ensure that the circulated information is not confidential in nature and related to the business and other affairs of any person or firm, any personal data, or any details about techniques used which might be turned to the advantage of any would-be cyber criminal. There are other concerns that may need to be addressed, such as prioritizing national security or criminal issues over other matters such as securities laws violations, and dealing with the varying domestic regimes that apply to information sharing around the world.

The means by which cyber security information would be transmitted could be of various natures. It could potentially take the form of an alert system, similar to the existing IOSCO's investor alert system, which allows the sharing of information through IOSCO's member web portal about firms that are not authorized to provide investment services in the jurisdiction that issued the alert. Preliminary discussions within IOSCO and within C4 more specifically have, however, highlighted many technical and legal challenges associated with such an initiative. An alternative avenue could be to produce a periodic bulletin bringing together key issues on cyber risk worldwide that would be made available to IOSCO member organizations, and potentially to other stakeholders.

The sharing of information could also occur within structured discussion forums. Participants in the Montreal roundtable agreed on the usefulness of structured discussions, such as those provided by the roundtable, among regulators and market participants at the international level on cyber security.[95]

[95] The Information Technology Supervisors Group (ITSG) is an example of such a forum. The ITSG consists of technology risk specialists and computer security professionals from 19 financial regulators in America, Europe, Asia and Australia. The group provides a forum for exchanging and sharing information and knowledge in addressing technology risk and systems security issues confronting the financial industries.

Chapter 8 – Conclusion

In constantly evolving securities markets, market participants and regulators alike must regularly adapt and respond to new challenges. Cyber security is arguably one of the most important challenges facing market participants and regulators today. This report was intended to provide a broad overview of the challenges associated with cyber security in securities markets from an international perspective by describing approaches adopted by markets participants in various segments of securities markets, and by describing initiatives adopted by regulators.

The review of potential tools available to regulators can serve as a valuable point of reference to IOSCO members as they consider policy responses appropriate to the specific markets they regulate. For market participants, the report outlines various plans and measures participants have put in place to enhance cyber security in terms of identification, protection, detection, response and recovery. In doing so, the report describes some of the practices adopted by market participants and aims to encourage, where appropriate, the adoption of those or similar practices.

The review of regulatory initiatives shows a wide diversity of avenues that can be usefully adopted by regulators. Regulators do indeed play a variety of roles and have adopted various tools in order to help enhance the cyber security frameworks of market participants, in the context of their jurisdiction's overall approach to cyber security. Amongst these tools, regulators have chosen to raise awareness levels regarding cyber security through the use of examination sweeps and the issuance of guidance, guidelines or frameworks.

Furthermore, regulators have also initiated and coordinated drills simulating cyber events and breaches involving all stakeholders including SROs and various market participants. Finally, regulators have also initiated regulatory changes or developed new regulations requiring market participants to identify cyber risks, to detect threats, to protect themselves against them and to respond and recover from cyber security events.

The report has also analyzed the disclosure of cyber security risks and incidents by reporting issuers. The review highlights the need for issuers to rely properly on the existing disclosure framework to ensure that investors receive material information, including as it relates to cyber risk. Based notably on a review of issuer disclosure practices, the report has highlighted a number of factors that issuers might consider when preparing their disclosure, if they have determined that cyber risk is a material risk, and which IOSCO members may take into account when considering issuer disclosure in their jurisdictions.

With regards to emerging trends and approaches in cyber security practices, this report has highlighted the fact that securities market participants have a multitude of threats to contend with. Some participants have invested a considerable amount of resources in order to establish an internal structure that addresses the issues relating to cyber security. Whether it's by following an existing cyber security framework such as NIST or by ensuring that third parties meet certain defined security criteria, market participants have taken steps to try and keep up with the accelerating pace at which cyber threats are evolving, with emerging trends in cyber attacks and with the ever changing regulatory landscape in which they operate. Market participants will have to continue to adapt their cyber security measures as information technology continues to evolve.

This report has highlighted a number of processes that regulated entities should consider in implementing or reviewing their cyber security framework. Appropriate governance is at the heart of any effective cyber security framework. The governance structure established by market participants to deal with cyber security issues, including the involvement of senior management and company boards, is paramount for the effectiveness of the overall information security framework. It helps organizations focus attention, determine their risk appetite and priorities and allocate resources to cyber security. Cyber security should be an integral part of a regulated entities' risk management program. The report further highlights a number of cyber security practices that regulated entities should consider in terms of identification, protection, detection, response, and recovery. Given that the cyber security landscape is constantly evolving, it is important to note that cyber security practices will undoubtedly change and evolve over time.

Finally, the report has considered issues surrounding the importance of sharing information related to cyber security among market participants and regulators. The report has described the current state of information sharing, the different models of successful information sharing initiatives, the hurdles to information sharing, and the potential roles for regulators and IOSCO. Securities regulators can and do promote and benefit from information sharing. Given the international nature of cyber risk, there is a need for information sharing at the international level. And international organizations such as IOSCO may be well placed to establish or promote mechanisms at the international level to achieve greater cross-jurisdiction information sharing.

APPENDIX 1 – OVERVIEW OF DOCUMENTS RELEVANT TO CYBER SECURITY FOR INTERMEDIARIES

This section presents an overview of important reports that are relevant to cyber security for market intermediaries, particularly in an international context, and that may also be relevant for other securities market participants. A table summarizes these reports according to the five main functions associated with cyber security, namely identification, protection, detection, response, and recovery.[96]

NIST - Framework for Improving Critical Infrastructure Cybersecurity
In 2013, the United States President issued an Executive Order calling for the development of a voluntary risk-based Cyber security Framework – a set of industry standards and best practices to help organizations manage cyber security risks.

In February 2014, the National Institute of Standards and Technology (NIST) issued The Framework that aims at enabling organizations – regardless of size, degree of cyber security risk, or cyber security sophistication – to apply the principles and best practices of risk management improving the security and resilience of critical infrastructure.[97]

The Framework Core is a set of cyber security activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. It consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. The Framework relies on a variety of existing standards, guidelines and practices relevant to core functions and outcomes, and present different ways to complete existing processes to address cyber risk.

IOSCO - AMCC Cyber-Resilience Task Force - Preliminary fact-finding exercise
This Report presents the results of a preliminary fact-finding exercise conducted by the Cyber-Resilience Task Force of the Affiliate Members Consultative Committee (AMCC) of IOSCO. The Task Force was established in December 2013 to complement the work previously conducted by the IOSCO Research Department and the World Federation of Exchanges, which focused on exchanges and central clearing counterparties. In addition to extending the survey to other institutions, the objective of the AMCC Task Force was to provide more granular and practical information regarding cyber threats and security measures in place at exchanges, securities brokers and other organizations including SROs.

The document presents the survey findings of the 56 responses received from AMCC members (22) and market participants (34). It sets out several points for authorities and market participants to consider at both the macro and micro levels as they develop responses to cyber threats.

IOSCO - Market Intermediary Business Continuity and Recovery Planning Report
The Report proposes standards and sound practices that regulators could consider as part of their oversight of the business continuity and recovery planning by market intermediaries.[98]

---

96 This table was produced by IOSCO's C3 working group.

97 See: http://www.nist.gov/cyberframework/upload/cyber security-framework-021214-final.pdf

98 See: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD523.pdf

In particular, sound practices regarding protection of data, systems and client privacy, including against cyber attacks are proposed.

IOSCO - Cyber-crime, securities markets and systemic risk -Joint Staff Working Paper of the IOSCO Research Department and World Federation of Exchanges

This document presents the results of the survey of the world's exchanges and provides keys insights on the current cyber threat landscape and potential systemic risk aspects.[99] It presents the potential future role of securities market regulators in engaging with cyber crime:

- Updating/implementing regulation and standards;
- Identifying and providing guidance on best practices, principles and/or frameworks;
- Building, partaking in and promoting information sharing networks; and
- Acting as a repository of knowledge for securities market participants to tap into.

The report underlines the need to reinforce the cyber security framework but to avoid being prescriptive in order to maintain flexibility. Also, the report lists and categorizes some common types of cyber attack techniques and prevention, detection and recovery mechanisms.

Table – Report summary according to five functions associated with cyber security

	IDENTIFICATION	**PROTECTION**	**DETECTION**	**RESPONSE**	**RECOVERY**
*NIST - **Framework for Improving Critical Infrastructure Cyber security (February, 2014)***	The "Identification" core function aims at developing the organizational understanding to manage cyber security risk to systems, assets, data and capabilities. Examples of outcomes within this Function include: - Asset Management (data, personnel, devices, systems and facilities to achieve the business purposes) - Business Environment (mission, objectives, stakeholders	The "Protection" core function aims at developing and implementing the appropriate safeguards to ensure delivery of critical infrastructure services. Examples of outcomes within this Function include: - Access Control (limited authorizations) - Awareness and Training (information security related to duties and responsibilities) - Data Security (information and	The "Detection" core function aims at developing and implementing the appropriate activities to identify the occurrence of a cyber security event. Examples of outcomes within this Function include: - Anomalies and Events (periodic tests) - Security Continuous Monitoring (identifying cyber security events and verifying the effectiveness of protective	The "Response" core function aims at developing and implementing the appropriate activities to take action regarding a detected cyber security event. It supports the ability to contain the impact of a potential cyber security event. Examples of outcomes within this Function include: - Response Planning - Communications (with internal and external stakeholders)	The "Recovery" core function aims at developing and implementing the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event. Examples of outcomes within this Function include: - Recovery Planning - Improvements (by incorporating lessons learned into future activities) - Communications (restoration activities

[99] See: http://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf

	IDENTIFICATION	PROTECTION	DETECTION	RESPONSE	RECOVERY
	and activities) - Governance (policies, procedures and processes) - Risk Assessment (cyber security risks to organizational operations, organizational assets and individuals) - Risk Management Strategy (priorities, constraints, risk tolerances and assumptions)	records managed to protect the confidentiality, integrity and availability of information) - Information Protection Processes and Procedures - Maintenance (industrial control and information system performed consistent with policies and procedures) - Protective Technology (technical security solutions)	measures) - Detection Processes (ensuring timely and adequate awareness of anomalous events)	- Analysis - Mitigation (preventing expansion of an event, mitigating its effects and eradicating the incident) - Improvements of the organizational activities (incorporating lessons learned from current and previous detection/response activities)	coordinated with internal and external parties)
IOSCO - ***AMCC Cyber-Resilience Task Force - Preliminary fact-finding exercise (December, 2014)***	The report underlines the following elements in identifying cyber risk: - Collaboration and Information sharing - Dedicated committee/specific unit - Cyber security intelligence - Identification of potential high-risk and/or high vulnerability providers	The following elements could permit to address cyber risk: - Staff training - IT/technical controls - Regular system audits - Cyber insurance - Independent vendors penetration testing - Cyber drills		The report sets out the followings ways: - Crisis management plan - Scenario planning - Investigation and enforcement capabilities - Response mechanisms	Recovery solutions could be: - Disaster recovery plan - Business continuity plan
IOSCO - ***Market Intermediary Business Continuity and Recovery Planning - Report (December, 2015)***				A comprehensive BCP must be flexible and tailored to the size and needs of an intermediary. Sound practices that merit consideration include: - The combination of several elements in Market	

	IDENTIFICATION	PROTECTION	DETECTION	RESPONSE	RECOVERY
				Intermediary's BCP, including: Identifying critical business functions and systems, and the major risks, threats and impacts for the firm; Assessing the potential impact of a major operational disruption through qualitative and quantitative analysis; Ensuring client accessibility to their funds and securities; Establishing general policies and procedures and specifically for internal and external communications; Having an appropriate internal corporate governance structure; Allowing back-up sites; Testing and evaluating the BCP on a periodic basis; Conducting BCP training exercises. - Mechanisms to protect data, systems and client privacy, including against cyber attacks: Establishing a defined security	

	IDENTIFICATION	PROTECTION	DETECTION	RESPONSE	RECOVERY
				and IT policy outlining the appropriate controls (technical, logical and administrative) to restrict access to physical assets and information, particularly during a major operational disruption, including procedures (e.g., security controls, encryption) that address both the frequent back-up and recovery of hard copies and electronic information; Whenever appropriate, considering the use of offsite storage facilities or backup data centers for electronic data or hardcopies, as applicable, and/or encryption of the electronic information that are backed up; and Using firewalls, Internet security (anti-virus, spyware and –malware tools) and third-party vendors for IT services and systems protection and monitoring.	

	IDENTIFICATION	PROTECTION	DETECTION	RESPONSE	RECOVERY
*IOSCO - **Cyber-crime, securities markets and systemic risk - Joint Staff Working Paper of the IOSCO Research Department and World Federation of Exchanges (July, 2013)***	A list of cyber-attack techniques is available in the report (See Annex A of the Report)	Reactive defence mechanisms could be: - Firewalls and Antivirus - Anti-DDoS and Anti-Bot detection systems - Intrusion Prevention Systems - Clean Pipe solutions - End-point security - Terminal safety controls Proactive defence could include: - Penetration Testing, Ethical hacking and simulations - Vulnerability assessment - Internal and external audits - Data encryption - Counter attacks - Air-gapping or partial air-gapping	Detection mechanisms listed are: - Intrusion Detection Systems - Automated Monitoring Systems and outsourcing monitoring - Security Incident and Event Management systems for all devices - Database activity monitoring - Security Operation Centres		Two main mechanisms could be used: - Back-up systems and data loss prevention software - Redundancy and disaster recovery sites

List of other relevant reports and resources

Anderson, R., Jr., Criminal Cyber Response and Services Branch, Federal Bureau of Investigation, *Statement before the Senate Committee on Homeland Security and Governmental Affairs*, Sept. 2014

Central Bank of Ireland, *Review of the management of operational risk around cybersecurity with the investment firm and fund services industry*, Sep. 2015

CFTC, *Best practices for the required administrative, technical and physical safeguards for the protection of customer records and information*, Feb. 2014

Committee on Payments and Market Infrastructures, *Cyber Resilience in Financial Market*, Nov. 2014

CPMI/IOSCO, Consultative Report: Guidance on Cyber-resilience for Financial Market Infrastructures, Nov. 2015

DTCC, *A White Paper to the Industry on Systemic Risk*, August 2013

DTCC, *Cyber Risk – A Global Systemic Threat*, Oct. 2014

FINRA, *Report on Cybersecurity Practices*, February 2015,

HM Government, *Cyber-security in Corporate Finance*, Jan. 2014

HFSB, *Cyber Security Memo*

ICI *Information Security Centre*

IOSCO, *Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity*, December 2015

Martin, C., Director General for Cyber Security, UK Government Communications Headquarters, *Financial Services Cyber Security Summit*, July 2014

MAS, *Technology Risk Management Guidelines*, June 2013

National Futures Association, *Cybersecurity Interpretative Notice*, October 2015

Oliver Wyman, Point of View, Financial Services, *A New Approach to Cybersecurity*, 2014

SANS Institute, *Glossary of security terms*

Joint UK Government and insurance industry release, Nov. 2014

SEBI, Circular on Cyber Security and Cyber Resilience Framework of Stock Exchanges, Clearing Corporation and Depositories, Aug. 2015

U.S. SEC, *Roundtable on Cyber-crime*, March 2014

U.S. SEC, *OCIE Cybersecurity Initiative*, March 2014

U.S. SEC, *OCIE Cybersecurity Examination Sweep Summary*, February 2015

U.S. SEC, *Office of Compliance and Examinations' 2015 Cybersecurity Examination Initiative*, Sep. 2015

U.S. SIFMA, *Cybersecurity Resource Center*

APPENDIX 2 – ACRONYMS

ORGANIZATIONS, ASSOCIATIONS & COMMITTEES

AMF: Autorité des marchés financiers
ASIC: Australian Securities and Investments Commission
C1: IOSCO's Committee on Issuer Accounting, Audit and Disclosure
C2: IOSCO's Committee on Secondary Markets
C3: IOSCO's Committee on Market Intermediaries
C4: IOSCO's Committee on Enforcement and Exchange of Information and the MMoU Screening Group
C5: IOSCO's Committee on Investment Management
CER: IOSCO's Committee on Emerging Risks
CFTC: Commodity Futures Trading Commission (United States)
CNBV: National Banking and Securities Commission (Mexico)
CPMI: Committee on Payments and Market Infrastructures
CSA: Canadian Securities Administrators
CSRC: China Securities Regulatory Commission
DTCC: Depository Trust & Clearing Corporation
EFAMA: European Fund and Asset Management Association
ESMA: European Securities and Markets Authority
FCA: Financial Conduct Authority (U.K.)
FSA: Financial Services Agency (Japan)
FS-ISAC: Financial Services Information Sharing and Analysis Center
FINRA: Financial Industry Regulatory Authority (United States) HFSB:
Hedge Funds Standards Board
ICI: Investment Company Institute (United States)
IIROC: Investment Industry Regulatory Organization of Canada
IOSCO: International Organization of Securities Commissions
KOFIA: Korea Financial Investment Association
MAS: Monetary Authority of Singapore
NIST: National Institute of Standards and Technology (United States)
NYSE: New York Stock Exchange
PwC: PricewaterhouseCoopers
SEC: Securities and Exchange Commission (United States)
SIFMA: Securities Industry and Financial Markets Association (United States)
WFE: World Federation of Exchanges
WGCR: CPMI-IOSCO's Working Group on Cyber Resilience

TERMS

APT: Advanced Persistent Threats
ATS: Alternative Trading System
BCP: Business Continuity Planning
CBEST: Cyber-resilience Testing Programme
CERT: Computer Emergency Readiness Team
CISP: Cyber-security Information Sharing Platform
CSIRT: Computer Security Incident Response Team

DAM: Database Activity Monitoring
DDoS: Distributed Denial-of-service
DLP: Data loss prevention plan
FIX: Financial Information Exchange
FMI: Financial Market Infrastructure
IoC: Indicator of Compromise
IPS: Intrusion Prevention System
IRP: Incident Response Plan
IDS: Intrusion Detection System
ISSP: Information Systems Security Program
IT: Information Technology
MMoU: Multilateral Memorandum of Understanding
NCSP: National cyber security Plan
OTF: Organized Trading Facility
Reg SCI: Regulation Systems, Compliance and Integrity
RPO: Recovery Point Objective
RTO: Recovery Time Objective
SEF: Swap Execution Facility
SIEM: Security Information and Event Management
SOC: Security Operations Center
SQL: Structured Query Language
SRO: Self-Regulatory Organization
STIX: Structured Threat Intelligence Expression
TAXII: Trusted Automated Exchange of Indicator Information
TF: Task Force
TRM: Technology Risk Management
TTP: Tactics, Techniques and Procedure
VAPT: Vulnerability Assessment and Penetration Testing
WAF: Web Applications Firewalls
WG: Working Group