CSA/ACVM Canadian Securities Administrators Autorités canadiennes en valeurs mobilières

# CSA Staff Notice 11-332
## *Cyber Security*

**September 27, 2016**

### Introduction

On September 26, 2013, the Canadian Securities Administrators (CSA) published Staff Notice 11-326 *Cyber Security* (the 2013 Notice). The 2013 Notice stated that strong and tailored cyber security measures are an important element of issuers', registrants' and regulated entities' (collectively, Market Participants) controls.[1] Market Participants were reminded that they should take the appropriate protective measures necessary to safeguard themselves and their clients or stakeholders. Examples of such measures, as described in the 2013 Notice, include:

- educating staff on the importance of, and their role in, promoting cyber security;
- following guidance and best practices from industry associations and recognized information security organizations;
- as appropriate, conducting regular third-party vulnerability and security tests and assessments; and
- reviewing cyber security risk control measures on a regular basis.

Since the 2013 Notice, the cyber security landscape has evolved considerably, as cyber attacks have become more frequent, complex and costly for organizations. Accordingly, the CSA is publishing this Notice on cyber security in order to:

- further highlight the importance of cyber risks for Market Participants;
- inform stakeholders about recent and upcoming CSA initiatives;
- reference existing standards and work published, including work published by the Investment Industry Regulatory Organization of Canada (IIROC), the Mutual Fund Dealers Association of Canada (MFDA) and international regulatory authorities and standard-setting bodies;
- communicate general expectations for Market Participants with respect to their cyber security frameworks; and
- examine ways to coordinate communication and information sharing between regulators and Market Participants.

### The Evolving Cyber Threat Landscape

The cyber threat landscape is constantly changing as technology advances and business strategies evolve. Given the electronic linkages within the financial system, the impact of a cyber attack

[1] Regulated entities include self-regulatory organizations, marketplaces, clearing agencies, and information processors.

can spread quickly, potentially affecting the integrity and efficiency of markets globally as well as trust and confidence in the financial system.

With advancing technology, cyber adversaries are becoming more sophisticated and the potential for damage is ever increasing. The number of entities experiencing financial losses, intellectual property theft, reputational damage, fraud, and legal exposure is rising.
Some studies examining the impact of cyber breaches, such as those released by the Ponemon Institute[2] and PricewaterhouseCoopers,[3] found that:

- In 2015, 38% more cyber security incidents were detected than in 2014; and
- The average total cost of a data breach for the companies participating in the 2016 Ponemon survey stood at USD$4 million.

Given these trends, as well as recent high-profile hacking incidents, authorities globally are considering or implementing various policy responses to encourage Market Participants to improve their cyber defences.

**Cyber Security: Priority Area for the CSA**
Cyber security has been identified as a priority area in the CSA 2016-2019 Business Plan as well as by some CSA members. Accordingly, the CSA is working to promote cyber security awareness and resilience. More specifically, the CSA is working to:

- Improve collaboration and communication on cyber security issues with Market Participants;
- Assess the level of Market Participant cyber security resilience, including measures for protection of personal investor data; and
- Improve Market Participants' understanding of CSA members' cyber security oversight activities, including providing guidance on expectations for market participants' cyber security preparedness.[4]

As the financial services industry is a high-value target for cyber attacks, the CSA has a central role to play in assessing and promoting readiness and cyber resilience with Market Participants.

**Recent and Upcoming CSA Initiatives**
Since the publication of the 2013 Notice, the CSA has been monitoring developments and undertaking a number of initiatives to integrate cyber-related activities into its work and to interact with industry and stakeholders. The goal is to better understand Market Participants' environment, challenges and level of preparedness, and ultimately to improve overall resilience in our markets. The following provides an overview of recent and upcoming CSA initiatives.

---

[2] *2016 Cost of Data Breach Study: Global Analysis*. The benchmark research, sponsored by IBM and independently conducted by Ponemon Institute LLC, studied 383 companies spanning 12 countries.
[3] *The Global State of Information Security Survey 2016* is a worldwide annual study by PwC, CIO, and CSO that analyzes responses of more than 10,000 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and directors of IT and security practices from more than 127 countries.
[4] Source: http://www.csa-acvm.ca/aboutcsa.aspx?id=1504

*Issuers:* The 2013 Notice stated that issuers should consider whether they need to disclose – in a prospectus or a continuous disclosure filing – information on their exposure to cyber risks, on controls they have in place to address these risks, as well as on cyber incidents they may experience. Since then, some CSA members have been reviewing the disclosure of issuers to analyze what is being disclosed with respect to cyber security risk and cyber attacks. The reviews were generally focused on the disclosure of risk factors, legal proceedings and corporate governance. Many issuers either did not have any disclosure or only had non-entity specific, boilerplate disclosure.

CSA members intend to re-examine the disclosure of some of the larger issuers in the coming months and, where appropriate, will contact issuers to get a better understanding of their assessment of the materiality of cyber security risks and cyber attacks. CSA findings and recommendations stemming from those reviews are anticipated to be published subsequently.

*Registrants:* On an ongoing basis, CSA staff discusses cyber security policies and procedures with registered firms as part of compliance reviews. Areas of focus include:

- firms' cyber security risk assessment and information security governance programs;
- firms' IT safeguards and controls;
- use of encryption;
- risks related to third-party service providers;
- vulnerability tests and compliance monitoring;
- evidence of regular employee training and awareness;
- incident response plans; and
- practices for accepting client instructions to withdraw or transfer funds via electronic means.

Some CSA members are gathering data about registrants' cyber security practices. A risk assessment questionnaire was sent to a large number of registered firms in May 2016 to collect high-level data about their cyber security practices and training programs. Another CSA member organized a focus group involving registrants in May 2016 to discuss their concerns and examine ways to increase their awareness and support them in regards to cyber security risk management. A more targeted desk review is planned for the remainder of 2016, which will assess in more detail the areas discussed in regular compliance reviews.

*Regulated entities:* The independent system review (ISR) that marketplaces, clearing agencies and information processors must perform has always had a cyber security component. However, since 2013, the ISRs for all regulated entities have contained a specific focus on cyber security. In addition, trade repositories that operate in Canada since the fall of 2014 are also subject to similar requirements with respect to ISRs. Further, the CSA has been gathering information to better understand how regulated entities are positioned with respect to their adoption of adequate cyber security frameworks to better manage and reduce cyber security risk.[5]

[5] A cyber security framework consists of a complete set of organizational resources, including policies, staff, processes, practices and technologies used to assess and mitigate cyber risks and attacks.

One CSA member has also examined interconnections, key processing interdependencies and single points of failure to understand the potential impact and contagion if an attack directed towards a regulated entity or site occurs.

*International activities:* CSA staff has engaged in IOSCO and CPMI-IOSCO work streams related to cyber risk and resilience. This work has included development of cyber resilience frameworks, and the publication of reports on regulatory approaches and tools to address cyber security matters as well as on mechanisms for trading venues to effectively manage cyber security risks.

The focus of current initiatives is on enhancing cross-border information sharing among regulators related to cyber security, including use of the IOSCO Multilateral Memorandum of Understanding (MMoU) to investigate cyber-related market manipulation and misconduct.

**Existing Cyber Security Resources**

Various regulatory authorities and standard-setting bodies have published information and guidance in an effort to enhance sharing of information about cyber security threats and improve preparedness to deal with cyber incidents as well as to inform and educate on cyber security issues and risks. A number of reference documents that may be useful to Market Participants are set out below:

CPMI-IOSCO guidance on cyber resilience for financial market infrastructures
http://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf

Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Initiatives
http://www.ffiec.gov/cybersecurity.htm

IIROC Cybersecurity Best Practices Guide
http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf

IIROC Cyber Incident Management Planning Guide
http://www.iiroc.ca/industry/Documents/CyberIncidentManagementPlanningGuide_en.pdf

IOSCO report on cyber security in securities markets
http://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

IOSCO report on mechanisms for trading venues to effectively manage electronic trading risks and plans for business continuity
http://www.iosco.org/library/pubdocs/pdf/IOSCOPD522.pdf

Mutual Fund Dealers Association (MFDA) Bulletin
http://www.mfda.ca/regulation/bulletins16/Bulletin0690-C.pdf

Securities and Exchange Commission (SEC) Division of Corporation Finance Disclosure Guidance
https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Securities Industry and Financial Markets Association (SIFMA) Principles for Effective Cybersecurity Regulatory Guidance
http://www.sifma.org/issues/item.aspx?id=8589951691

SIFMA's Guidance for Small Firms: How Small Firms Can Protect Their Business
http://www.sifma.org/issues/operations-and-technology/cybersecurity/guidance-for-small-firms/

The Financial Industry Regulatory Authority (FINRA) Report on Cybersecurity Practices
https://www.finra.org/file/report-cybersecurity-practices

The National Institute for Standards and Technology (NIST) Cybersecurity Framework
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

The Office of the Superintendent of Financial Institutions (OSFI) Cyber Security Self-Assessment Guidance
http://www.osfi-bsif.gc.ca/eng/fi-if/in-ai/pages/cbrsk.aspx

It is important to note when reviewing these types of resources that there is no one-size-fits-all approach to cyber security and that organizations should establish and view their cyber security frameworks accordingly. Among other themes, the aforementioned publications highlight the need for an organization to:

- manage cyber security at an organizational level with responsibility for governance and accountability at executive and board levels;
- organize its cyber security activities at a high level: Identify, Protect, Detect, Respond, and Recover;
- establish and maintain a robust cyber security awareness program for staff;
- formulate a clear understanding of the business drivers and security considerations specific to its use of technology, systems and networks;
- understand the likelihood that an event will occur and the resulting impact in order to determine the acceptable level of risk appetite according to its risk tolerance, budget and legal requirements;
- manage cyber security risk exposures that arise from using third-party vendors for services;
- consider methodology to protect individual privacy as well as any obligations to report cyber security breaches to a regulatory authority;
- consider whether to share information about cyber incidents with Market Participants;
- communicate, collaborate and coordinate with other entities;
- establish plans to restore any capabilities or services that may be impaired due to a cyber incident in a timely fashion; and
- treat cyber security programs as living documents that will continue to be updated and improved on an ongoing basis.

**Next Steps and CSA Expectations**

While Market Participants are already taking action to understand and mitigate cyber security risks, continued vigilance in this area will be required. The CSA intends to hold roundtable sessions in the coming months to discuss cyber security issues and risks, regulatory expectations and the need for coordination. Though full details will follow, the general purposes of holding roundtable discussions will be to:

- promote an open dialogue with cyber security experts and Market Participants;
- discuss relevant developments related to cyber risks and how to address those risks;
- develop opportunities for greater collaboration and improved communication on issues of common concern relating to cyber security; and
- discuss coordination in the event of a cyber security incident.

In the meantime, we expect Market Participants to take steps to protect themselves against cyber threats. In particular:

- *Issuers:* In general, to the extent that an issuer has determined that cyber risk is a material risk, CSA members expect issuers to provide risk disclosure that is as detailed and entity specific as possible. Furthermore, issuers should address in any cyber-attack remediation plan how materiality of an attack would be assessed to determine whether and what, as well as when and how, to disclose in the event of an attack. In the assessment, issuers should consider the impact on the company's operations and reputation, its customers, employees and investors.
- *Registrants:* CSA members expect that registrants continue to remain vigilant in developing, implementing and updating their approach to cyber security hygiene and management. They should review and follow guidance issued by self-regulatory organizations such as IIROC and the MFDA.
- *Regulated entities:* CSA members expect that regulated entities examine and review their compliance with ongoing requirements outlined in securities legislation and terms and conditions of recognition, registration or exemption orders, which include the need to have internal controls over their systems and to report security breaches. We also expect regulated entities to adopt a cyber security framework provided by a regulatory authority or standard-setting body that is appropriate to their size and scale.

**For more information:**

Tom Graham
Director, Corporate Finance
Alberta Securities Commission
403-297-5355
tom.graham@asc.ca

Jean Lorrain
Senior Director, International Affairs and Strategic Monitoring
Autorité des marchés financiers
514-395-0337 ext. 4311
jean.lorrain@lautorite.qc.ca

Philippe Bergevin
Senior Economist, International Affairs and Strategic Monitoring
Autorité des marchés financiers
514-395-0337 ext. 4285
philippe.bergevin@lautorite.qc.ca

Isaac Z. Filaté
Senior Legal Counsel, Capital Markets Regulation Division
British Columbia Securities Commission
604-899-6573
ifilate@bcsc.bc.ca

Chris Besko
Acting Director
Manitoba Securities Commission
204-945-2561
cbesko@gov.mb.ca

Jake van der Laan
Director, Enforcement and Chief Information Officer
Financial and Consumer Services Commission, New Brunswick
506-658-6637
jake.vanderlaan@fcnb.ca

John O'Brien
Superintendent of Securities
Office of the Superintendent of Securities, Newfoundland and Labrador
709-729-4909
johnobrien@gov.nl.ca

Tom Hall
Superintendent of Securities
Office of the Superintendent of Securities, Northwest Territories
867-767-9305
tom_hall@gov.nt.ca

Jack Jiang
Securities Analyst, Corporate Finance
Nova Scotia Securities Commission
902-424-7059
jack.jiang@novascotia.ca

Jeff Mason
Superintendent of Securities
Department of Justice, Government of Nunavut
867-975-6591
jmason@gov.nu.ca

Tracey Stern
Manager, Market Regulation
Ontario Securities Commission
416-593-8167
tstern@osc.gov.on.ca

Alex Petro
Trading Specialist, Market Regulation
Ontario Securities Commission
416-263-3796
apetro@osc.gov.on.ca

Steven Dowling
Acting Director
Government of Prince Edward Island, Superintendent of Securities
902-368-4551
sddowling@gov.pe.ca

Dean Murrison
Director, Securities Division
Financial and Consumer Affairs Authority of Saskatchewan
306-787-5879
dean.murrison@gov.sk.ca

Rhonda Horte
Securities Officer
Office of the Yukon Superintendent of Securities
867-633-7969
rhonda.horte@gov.yk.ca