

## CSA Staff Notice 11-336

### *Summary of CSA Roundtable on Response to Cyber Security Incidents*

**April 6, 2017**

The Canadian Securities Administrators (CSA) hosted a roundtable on February 27, 2017 to explore cyber security issues and opportunities for greater collaboration, communication and coordination in the event of a large-scale cyber security incident. This Staff Notice provides an overview of the themes discussed and some of the main takeaways.

Roundtable participants represented a cross-section of Canadian securities market stakeholders – including marketplaces, clearing agencies, registrants, reporting issuers, regulatory authorities, and cyber security experts – and reflected a diversity of roles and views. A list of organizations that participated in the roundtable is available in the Appendix to this notice.

During the roundtable, participants considered two hypothetical cyber incident scenarios intended to guide the discussions. The scenarios were designed to explore how participants, individually and as a group, would respond in the event of a large-scale cyber security incident and to gain a better understanding of the roles of entities and regulators with respect to incident response, coordination and information sharing.

The first scenario involved a cyber incident affecting clearing agencies, which resulted in incorrect clearing member margin requirements being generated by the agencies' risk systems. The second scenario involved the tampering of certain orders sent to a marketplace which resulted in erroneous trade fills being received by some dealers.

The discussions highlighted the interconnected nature of the Canadian securities markets ecosystem and the importance of cooperation and information sharing in responding to a cyber security incident and reducing the risk of contagion. In the view of roundtable participants, cyber security incidents can potentially have far-reaching implications beyond the immediate organizations that are affected, notably if core systems are impacted.

At a high level, the discussions were focussed on the following issues:

- the response of an entity subject to a cyber security event, including matters related to governance, assessment of damage, personnel involved in decision making and information flow;
- the response of entities both downstream and upstream from the affected entity, including possible steps that may be taken to minimize the impact to their organizations;
- people who should be involved in discussions and decision making for a coordinated response to a market-wide incident, including which organizations need to be involved,

who should be driving the resolution process and how communication and coordination amongst organizations may be achieved;

- information that should be communicated internally and externally, including organizations' communication protocols and information that organizations not directly attacked expect to be supplied with from an affected entity; and
- factors that may contribute to coordination, communication and collaboration, including what information is needed to ensure smooth coordination and communication among different stakeholders and challenges organizations may face to reach that goal.

More specifically, the discussions covered elements associated with robust Incident Response Plans (IRPs) for entities, including those indirectly affected by a cyber incident. Participants indicated that IRPs are generally quite detailed and complete with regards to internal procedures in the event of an incident but ought to also address coordination and information sharing with other stakeholders, particularly in the context of a potentially market-wide cyber security incident.

With respect to information sharing and cooperation amongst stakeholders, participants indicated that reliance on existing organizations that provide intelligence analysis and information sharing services, coupled with informal, peer-to-peer communication channels, is generally effective. However, relying on more formal communication channels and coordination in the event of a market-wide cyber security incident may contribute to improved response and recovery.

Roundtable participants also discussed the need to test and update IRPs, including communication and coordination protocols. Conducting regular drills and assessments of IRPs and protocols is essential in ensuring that they are up-to-date and effective.

Finally, the discussions also underscored the public and private resources available to organizations that may be subject to a cyber security incident. Resources include Public Safety Canada's Canadian Cyber Incident Response Centre, the RCMP and provincial law enforcement authorities, and information sharing organizations such as The Financial Services Information Sharing and Analysis Center.

As highlighted in [CSA Staff Notice 11-332 Cyber Security](#), 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. CSA members also expect that registrants continue to remain vigilant in developing, implementing and updating their approach to cyber security hygiene and management.

Cyber security has been identified as a priority area in the CSA 2016-2019 Business Plan. Accordingly, in light of the roundtable, CSA members will continue to collaborate with market participants, other regulators and stakeholders to enhance cyber security preparedness and will work towards a more formal coordination process beyond the existing processes that are in place.

**For more information:**

Philippe Bergevin  
Senior Economist, International Affairs and  
Strategic Monitoring  
Autorité des marchés financiers  
[philippe.bergevin@lautorite.qc.ca](mailto:philippe.bergevin@lautorite.qc.ca)

Jean Lorrain  
Senior Director, International Affairs and  
Strategic Monitoring  
Autorité des marchés financiers  
[jean.lorrain@lautorite.qc.ca](mailto:jean.lorrain@lautorite.qc.ca)

Tom Graham  
Director, Corporate Finance  
Alberta Securities Commission  
[tom.graham@asc.ca](mailto:tom.graham@asc.ca)

Sasha Cekerevac  
Regulatory Analyst, Equity Markets  
Alberta Securities Commission  
[Sasha.Cekerevac@asc.ca](mailto:Sasha.Cekerevac@asc.ca)

Isaac Z. Filaté  
Senior Legal Counsel, Capital Markets  
Regulation Division  
British Columbia Securities Commission  
[ifilate@bcsc.bc.ca](mailto:ifilate@bcsc.bc.ca)

Chris Besko  
Acting Director  
Manitoba Securities Commission  
[cbesko@gov.mb.ca](mailto:cbesko@gov.mb.ca)

Jake van der Laan  
Director, Enforcement and Chief  
Information Officer  
Financial and Consumer Services  
Commission, New Brunswick  
[jake.vanderlaan@fcnb.ca](mailto:jake.vanderlaan@fcnb.ca)

John O'Brien  
Superintendent of Securities  
Office of the Superintendent of Securities,  
Newfoundland and Labrador  
[johnobrien@gov.nl.ca](mailto:johnobrien@gov.nl.ca)

Tom Hall  
Superintendent of Securities  
Office of the Superintendent of Securities,  
Northwest Territories  
[tom\\_hall@gov.nt.ca](mailto:tom_hall@gov.nt.ca)

Jack Jiang  
Securities Analyst, Corporate Finance  
Nova Scotia Securities Commission  
[jack.jiang@novascotia.ca](mailto:jack.jiang@novascotia.ca)

Jeff Mason  
Superintendent of Securities  
Department of Justice, Government of  
Nunavut  
[jmason@gov.nu.ca](mailto:jmason@gov.nu.ca)

Tracey Stern  
Manager, Market Regulation  
Ontario Securities Commission  
[tstern@osc.gov.on.ca](mailto:tstern@osc.gov.on.ca)

Alex Petro  
Trading Specialist, Market Regulation  
Ontario Securities Commission  
[apetro@osc.gov.on.ca](mailto:apetro@osc.gov.on.ca)

Steven Dowling  
Acting Director  
Government of Prince Edward Island,  
Superintendent of Securities  
[sddowling@gov.pe.ca](mailto:sddowling@gov.pe.ca)

Dean Murrison  
Director, Securities Division  
Financial and Consumer Affairs Authority  
of Saskatchewan  
[dean.murrison@gov.sk.ca](mailto:dean.murrison@gov.sk.ca)

Rhonda Horte  
Securities Officer  
Office of the Yukon Superintendent of  
Securities  
[rhonda.horte@gov.yk.ca](mailto:rhonda.horte@gov.yk.ca)

<b>Appendix – List of Participating Organizations at Roundtable</b>		
Aequitas Neo Exchange Inc.	eSentire Inc.	National Bank of Canada
Bank of America	Fidessa group plc	NPC Dataguard
Bank of Canada	Financial Services Information Sharing and Analysis Center	Omega ATS
BMO Financial Group	FundSERV Inc.	Office of the Superintendent of Financial Institutions Canada
Broadridge Financial Solutions	Greystone Managed Investments Inc.	Payments Canada
Canadian Pension Plan Investment Board	Hedge Fund Standards Board	Public Safety Canada
Canadian Securities Exchange	IGM Financial	PwC Canada
CanDeal	Investment Industry Association of Canada	RBC Capital Markets
CIBC	Investment Industry Regulatory Organization of Canada	RCMP
Deloitte LLP	Investment Technology Group, Inc.	Ridge Canada
Department of Finance Canada	KPMG Canada	Sun Life Financial
Desjardins Group	Lumen Asset Management Inc.	TD Bank Financial Group
Emera Inc.	Mutual Fund Dealers Association of Canada	TMX Group Limited
Ernst & Young LLP	Nasdaq CXC Limited	