IIROC OCRCVM
Investment Industry Regulatory Organization of Canada
Organisme canadien de réglementation du commerce des valeurs mobilières

IIROC NOTICE

Administrative Notice
General

Please distribute internally to:

Legal and Compliance
Senior Management

Contact:
Wendy Rudd
Senior Vice President, Member Regulation and Strategic Initiatives
416 646-7216
wrudd@iiroc.ca

15-0294
December 21, 2015

Dealer Member Cyber-security

As noted in IIROC's Annual Compliance Report for 2014/2015, cyber-security continues to be a key issue for investment firms and for IIROC. For regulators and financial market participants, the increased efficiencies and improved capabilities of today's information technology infrastructure come with incremental cyber-risks. Given the increasing automation of, and interconnections among business functions, information and operational systems, an appropriate response to the challenge of cyber-security must take an enterprise-wide perspective and be part of each firm's overall risk-management program.

Proactive management of cyber-risk is critical to the stability of IIROC-regulated firms, the integrity of capital markets and the protection of investors. In February and March 2015, we surveyed IIROC-regulated firms to collect information concerning their assessment of their cyber-security preparedness. In March 2015, we conducted a "table-top" exercise with a cross-section of firms to test their preparedness to deal with cyber-attacks. The exercise included coordination among firms and with regulators for sharing information to mitigate the impact of an attack, and protocols for updating clients and other stakeholders during such an incident.

Defining the current state of defences against cyber-threats was a core objective of the exercise, and a necessary pre-condition for IIROC to define a strategy to assist its Dealer

Members to adequately protect themselves against these threats. We have used the results of the survey and table-top exercise to assist in developing best-practice recommendations that can be applied by all IIROC-regulated firms, irrespective of size and business model, as well as a cyber-incident management planning guide. These resources draw on input from a focus group made up of a number of Dealer Members that participate in the Investment Industry Association of Canada's cyber-security working group. They also draw on our review of the approaches of other domestic and global financial services regulators.

This Notice:

- provides an overview of the results of our survey and table-top exercise;
- describes IIROC's *Cyber-security Best Practices Guide* and *Cyber Incident Management Planning Guide*; and
- outlines IIROC's planned next steps to continue informing and working with Dealer Members to increase their cyber-security preparedness.

Cyber-security Survey

IIROC conducted the survey of Dealer Members in February-March, 2015. Response to the survey was good, with 140 Members (77%) responding.

Based on the survey results, respondents appear to be well-aware of cyber-risk and a good percentage of respondents have taken steps to deal with cyber-risk. On a scale of 1 to 5 (with 5 being the highest), 91% of respondents rated their ability to deal with cyber-threats as 3, 4 or 5.

It was also encouraging to find that 83% of respondents viewed cyber-issues as a threat. In addition, 98% of respondents have adopted information security measures, 69% have cyber-security policies in place and 80% reported senior management / board involvement in cyber issues.

The other detailed results (as self-reported by respondents) are as follows:

- 98% have tight controls of administrative privileges with respect to access to their systems.
- 91% have strong authentication mechanisms to manage user identities and access to systems.
- 94% have protocols for protection of client information.
- 81% have the ability to automatically detect and block cyber-related threats/attacks.
- 80% have detection and remediation software in place.

- 80% of Members use third parties for cyber protection.
- 79% have the tools to secure mobile devices and wireless networks.
- 76% of Members do not provide their clients with access to their networks.
- 66% have a communication protocol for handling cyber-security issues.
- 56% reported having separate cyber budgets.
- 47% have protocols to keep clients informed of cyber-related issues.
- 33% have cyber insurance policies in place.
- 7% reported a service outage in last 12 months due to malicious acts of third parties.

Respondents noted that IIROC could assist Dealer Members in a number of areas, including information sharing, developing and sharing best practices, and conducting education and awareness sessions.

Table-top Exercise

On March 3, 2015, we conducted an IIROC-sponsored table-top exercise which involved 27 selected IIROC Members and IIROC's Market Surveillance Department. The test was facilitated by Juno Risk Solutions, a consulting firm that specializes in this field and has been involved in similar tests for the Bank of Canada and the Department of Finance.

IIROC Members participating in the test included bank-owned and large independent IIROC Dealer Members, who in total are estimated to account for over two-thirds of IIROC Dealer Members' total activity, as well as Marketplace Members. The exercise was observed by representatives from the Ontario Securities Commission and the Autorité des marchés financiers.

The test scenario envisioned multiple cyber-attacks on a number of IIROC Members that would also likely impact trading on marketplaces.

Cyber-security Best Practices Guide and Cyber Incident Management Planning Guide

Included with this Notice are the guides, which we developed in conjunction with Juno Risk Solutions.

The *Cyber-security Best Practices Guide* provides Dealer Members with a voluntary risk-based cyber-security framework comprising industry standards and best practices to help Dealer Members manage cyber-security risks. This comprehensive guide addresses the following areas:

- Governance and risk management
- Personnel screening and insider threats
- Physical and environmental security
- Awareness and training
- Network security
- Information system protection
- User account management and access control
- Asset management
- Incident response
- Information sharing and breach reporting
- Cyber insurance
- Vendor risk management (including cloud computing)
- Cyber-security policies

The *Cyber Incident Management Planning Guide* assists Dealer Members in the effective preparation of internal response plans for cyber-threats and cyber-attacks. It will assist Dealers in effectively deploying their resources and establishing communication procedures to be used following an attack. It is meant to minimize the impact of a cyber-security incident and mitigate threats and vulnerabilities as incidents occur.

We will continue to update these guides based on Dealer Members' feedback, the evolution of the cyber-security landscape and our ongoing experience with assessing Dealer Members' preparedness.

IIROC's Next Steps

Over the coming months, IIROC will further develop a cyber-security program with the following primary objectives:

- host webinars to help Dealer Members understand the guides and stay informed about emerging cyber-security issues, challenges and best practices;
- conduct a more extensive self-assessment survey among Dealer Members to measure the adequacy of Dealer Members' cyber-security infrastructure;
- inform Dealer Members regarding how well their cyber-security practices compare to the practices of their peers;
- evaluate systemic or sector-wide practices as a means of gaining insights into the overall vulnerability of the industry to disruption by risk factors arising from individual firms; and
- collaborate with and advise Dealer Members to help them to assess their own readiness and to implement cyber-security systems and procedures for the protection of customer data against cyber-security threats.

Where Dealer Members are already subject to similar cyber-security oversight by other regulators, such as OSFI and/or FINRA, we will consider working with and/or relying on those regulators in order to avoid duplication.