Mutual Fund Dealers Association of Canada
Association canadienne des courtiers de fonds mutuels

Contact: Brett Konyu
Manager, Member Education
Phone: 416-943-4609
E-mail: bkonyu@mfda.ca

BULLETIN #0690–C
May 19, 2016

MFDA Bulletin

Compliance

For Distribution to Relevant Parties within your Firm

Cybersecurity

Background

The purpose of this Bulletin is to enhance Member awareness and understanding of cybersecurity issues and resources, and to provide guidance to Members regarding the development and implementation of cybersecurity procedures and controls.

Cybersecurity is an important issue for all Members to consider due to the potential for harm to clients, Members, and to the investment industry in general. Such harm can be reputational and/or monetary, and may lead to a major disruption in a Member's operations.

As a result of the foregoing risks, Members should establish and maintain appropriate cybersecurity procedures and controls to ensure that they are adequately protecting networks, computers, programs, and data from attack, damage and unauthorized access.

What is Cybersecurity?

Cybersecurity can be defined as the process of protecting information by preventing, detecting and responding to attacks, damage and unauthorized access.

Sources of Cybersecurity Threats

Threats to cybersecurity are numerous and wide-ranging, originating from internal and external sources. In the United States, the Financial Industry Regulatory Authority (FINRA) cybersecurity surveys of 2011 and 2014 identified the top three threats to the securities industry as:

1. Hackers penetrating firm systems
2. Insiders compromising firm or client data, and
3. Operational risks

Creating a Cybersecurity Framework

This Bulletin outlines some basic, and widely used, cybersecurity concepts. Members should evaluate their cybersecurity programs and implement additional controls and risk management techniques, where it is appropriate to do so, having regard to the particular operations and potential vulnerabilities of the Member. Cybersecurity is a shared responsibility. As a result, people, processes, tools, and technologies must work together to protect access and control of an organization's systems and data. Measures that are appropriate for a small Member may not be appropriate for a large Member and vice versa.

Protecting your organization's systems and data requires a focus on the following three fundamental goals:

1. **Confidentiality** Any important information you have that should be kept confidential. This information should only be accessed by people to whom (or systems to which) authorization has been given.
2. **Integrity** Maintain the integrity of information assets to keep everything complete, intact, and uncorrupted.
3. **Availability** Maintain the availability of systems, services, and information when required by the business or its clients.

Members should perform the following Cybersecurity Framework functions:

1. Identify assets in need of protection, as well as threats and risks to them.
2. Protect such assets with the appropriate safeguards.
3. Detect intrusions, breaches, and unauthorized access.
4. Respond to a potential cybersecurity event.
5. Recover from a cybersecurity incident by assessing the incident, restoring normal operations and services, and applying enhanced safeguards that are specific to the nature of the incident.

When developing a Cybersecurity Framework, Members should consider each of the following areas, taking into account the size and nature of their operations:

- Setting a governance and risk management framework including the involvement and buy-in of the Board and senior management.
- Implementing personnel screening and identifying insider threats from new, current and departing employees and contractors.
- Physical security for human, environmental and supply chain threats including consideration of "clean desktop" policies, physical location security and back-up of information.

- Cybersecurity awareness including mandatory, on-going, training of all staff on Member policies and procedures.
- Assessing threats and vulnerabilities through regular vulnerability testing of existing systems, regularly updating systems with security patches and evaluating critical patches before implementation.
- Network security measures including multilayered defenses with next-generation firewalls, wireless network encryption, securing the network and limiting access to certain devices by using password protection.
- Information system protection including backup and recovery processes, comprehensive anti-malware solutions and control of external devices, including limiting the access of personal devices to any information that is or might be deemed sensitive.
- User account management and access control, through such measures as password protocols and levels of access.
- Asset management, including ongoing inventory controls for all technology connected to the Member's systems.
- Cybersecurity incident response procedures, including an incident response team.
- Information sharing and incident/breach reporting, such as the requirement to notify the Privacy Commissioner of specified breaches.
- Obtaining cyber insurance coverage.
- Managing threats posed by vendors, ensuring the level of risk posed by each third party vendor is appropriately assessed and mitigated.
- Cybersecurity policy, setting out mandatory conduct of employees and other relevant parties.

Additional Resources

The following documents, principles, and best practices constitute foundational references:

1. Cybersecurity Best Practices Guide (Investment Industry Regulatory Organization of Canada (IIROC))
    - Provides guidance on the Cybersecurity Framework for investment dealers.
2. Cyber Incident Management Planning Guide (IIROC)
    - Sets out procedures for investment dealers to consider when recovering from a cybersecurity incident.
3. Report on Cybersecurity Practices (FINRA)
    - Provides guidance to assist individual broker-dealers, and the industry as a whole, in responding to cybersecurity threats.

4. CSA Staff Notice 11-326 - Cyber Security

    - Comments on the appropriate protective and security hygiene measures registrants should implement to safeguard themselves and their clients and stakeholders.

5. Consultative Report: Guidance on Cyber Resilience for Financial Market Infrastructures

    (Board of the International Organization of Securities Commissions (IOSCO) - Committee on Payments and Market Infrastructures)

    - Provides guidance for financial market infrastructures to enhance their cyber resilience in five primary risk management categories and three overarching components.

6. Get Cyber Safe Guide for Small and Medium Businesses (Government of Canada)

    - Provides guidance to Canadians who own or manage a small or medium business, to help them understand the cybersecurity risks they face, and to provide them with practical advice on how to better protect their business and employees from cyber crime.

7. Framework for Improving Critical Infrastructure Cybersecurity (National Institute of Standards and Technology)

    - Provides guidance and best practices on how to protect information and assets from cyber attacks.

DM#473665v4