THE INVESTMENT FUNDS INSTITUTE OF CANADA

L'INSTITUT DES FONDS D'INVESTISSEMENT DU CANADA

CYBERSECURITY GUIDE

October 2019

TABLE OF CONTENTS

INTRODUCTION

The Cybersecurity Best Practices Guide for IIROC Dealer members notes that cybersecurity has been defined in a variety of ways by different organizations:

> The Committee on National Security Systems (CNSS-4009) defines cybersecurity as the ability to protect or defend an enterprise's use of cyberspace from an attack, conducted via 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.
>
> The National Institute of Standards and Technology defines cybersecurity as "the process of protecting information by preventing, detecting, and responding to attacks." Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line. It can drive up costs and impact revenue. It can harm an organization's ability to innovate and to gain and maintain customers.
>
> The International Organization for Standardization defines cybersecurity or cyberspace security as the preservation of confidentiality, integrity and availability of information in the Cyberspace. In turn, "the Cyberspace" is defined as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."

The Mutual Fund Dealers Association simply defines it as the process of protecting information by preventing, detecting and responding to attacks, damage and unauthorized access.

Regardless of the definition being referenced, cybersecurity is an area of focus for firms and regulators globally due to the potential harm to clients, firms and the investment industry in general. Cybersecurity threats are numerous, wide-ranging and rapidly evolving.

This Guide has been prepared to provide IFIC Members with a list of available resources to help Members develop a robust Cybersecurity program.

FRAMEWORK

All registered securities firms are required to establish, maintain and apply policies and procedures that create a system of controls and supervision to ensure compliance with securities legislation and manage the risks associated with their business in accordance with prudent business practices. Cybersecurity controls should ensure that networks, computers, programs and data are adequately protected from attack, damage or unauthorized access.

- An effective Cybersecurity framework is critical in helping firms to:
- Identify assets in need of protection as well as the threats and risks to them
- Protect such assets with appropriate safeguards
- Detect intrusions, breaches and unauthorized access
- Respond to potential and actual cybersecurity events
- Recover from a cybersecurity event

An effective framework will include the following components. This list is not intended to be exhaustive; rather it is representative of a minimum standard that can be adapted to the size and nature of a firm's operations.

Policies and Procedures

Firms must have policies and procedures that address cybersecurity. Policies and procedures should be reviewed frequently (no less than annually) to ensure they remain current and relevant. Policies and procedures should speak to prevention, detection, training and business continuity plans during a cybersecurity incident. Topics to cover include:

- Using electronic communications, including the types of information that may be collected or sent through email, using secured or unsecured communication systems, verifying client instructions sent electronically and social media practices
- Using devices (firm issued or personal), including the use of such devices to access the firm's network and data internally and externally
- Losing or disposing of an electronic device, including electronic storage devices (e.g. USB keys)
- Using public/personal electronic devices or public/personal internet connections to remotely access the firm's network and data, including to access client communications or client information
- Detecting internal or external unauthorized activity (e.g. hacking, phishing, malware)
- Protecting data, including data encryption, data storage and information portals
- Ensuring software, including anti-virus software, is updated in a timely manner
- Overseeing and conducting due diligence on third-party vendors or service providers with access to the firm's network or data.
- Escalating and reporting cybersecurity incidents.

Training

Employees are often the first line of defense against a cyber-attack. Adequate training is crucial to a firm's readiness to deal with threats or incidents. Given the dynamic nature of cyber activity, training should be conducted with sufficient frequency to remain current, but should be no less than annually.

- Training should focus on:
- Recognizing risks
- Identifying types of cyber threats that employees may encounter and how to respond to those threats
- Handling confidential firm and/or client information
- Using strong passwords
- Securing electronic devices
- Identifying actual or potential cyber threats or cybersecurity incidents
- Identifying when and how to escalate cyber security incidents

Risk Assessment

Firms should consider conducting a periodic cybersecurity risk assessment. The risk assessment may include:

- Identifying the firm's assets and data that needs to be protected
- Identifying vulnerable areas of the firm's operations
- Determining potential consequences for cyber threats
- Evaluating preventative controls and the incident response plan to determine if changes are required

Incident Response Plan

Firms should have a documented incident response plan that is tested periodically. The incident response plan can include:

- Identifying who is responsible for communicating about the cybersecurity event, to whom and what details are to be communicated to each person or group
- Identifying the various types of cyberattacks and procedures to stop the incident from continuing.
- Recovering or restoring data
- Investigating the incident to determine the extent and cause of the damage
- Reviewing and modifying systems, policies and procedures to prevent similar events from occurring

Third Party Vendors or Service Providers

In addition to maintaining robust policies and procedures regarding the due diligence and oversight of third party vendors or service providers, firms should have written agreements with their third party vendors or service providers that include provisions related to cybersecurity and the reporting of cybersecurity incidents to the firm.

Insurance

Firms should periodically review their existing insurance coverage to determine the extent of cybersecurity coverage and consider whether it continues to be sufficient.

Information Sharing

Firms may benefit from opportunities to share information. Information sharing may occur through a government sponsored website or through a trusted network of peers. Information sharing can help identify potential vulnerabilities and threats early, or even before, your firm is impacted.

Cyber Security Certification

Canada has launched a federal cyber certification program to help raise the cyber security baseline among Canadian firms. The program targets small to medium size enterprises and is part of the National Cyber Security Strategy.

CyberSecure Canada is a voluntary program based upon the 13 baseline controls outlined in Baseline Cyber Security Controls for Small and Medium Organizations issued by the Canadian Centre for Cyber Security. The program allows businesses to use the CyberSecure Canada certification mark for a period of two years.

APPENDIX A – REGULATORY CYBERSECURITY RESOURCES

CANADIAN REGULATORY RESOURCES

CSA Staff Notice 11-332 Cybersecurity Notice
https://www.osc.gov.on.ca/documents/en/Securities-Category1/sn_20160927_11-332-cyber-security.pdf

CSA Staff Notice 33-321 Cybersecurity and Social Media
http://www.osc.gov.on.ca/documents/en/Securities-Category3/csa_20171019_33-321_cyber-security-and-social-media.pdf

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

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

Mutual Fund Dealers Association (MFDA) Bulletin #0690-C Cybersecurity
http://www.mfda.ca/regulation/bulletins16/Bulletin0690-C.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

The Office of the Superintendent of Financial Institutions (OSFI) Technology and Cyber Security Incident Reporting
http://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/adv-prv/Pages/TCSIR.aspx

INTERNATIONAL REGULATORY RESOURCES

CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures
http://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf

FCA Cyber Resilience Website
https://www.fca.org.uk/firms/cyber-resilience

FINRA Report on Selected Cybersecurity Practices – 2018
https://www.finra.org/sites/default/files/Cybersecurity_Report_2018.pdf

FINRA Review of Cybersecurity Practices
https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf

FINRA Cybersecurity Checklist
http://www.finra.org/industry/small-firm-cybersecurity-checklist

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

NASAA Cybersecurity Checklist
http://nasaa.cdn.s3.amazonaws.com/wp-content/uploads/2011/08/NASAA-Cybersecurity-Checklist.pdf

SEC Observations from Cybersecurity Examinations
https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf

SIFMA Cybersecurity Resources
https://www.sifma.org/cybersecurity-resources/

APPENDIX B - ADDITIONAL CYBERSECURITY RESOURCES

Baseline Cyber Security Controls for Small and Medium Organizations
https://cyber.gc.ca/sites/default/files/publications/Baseline%20Cyber%20Security%20Controls%20for%20Small%20and%20Medium%20Organizations.pdf

British Columbia Information Security Website
https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security

British Columbia Cyber Security Alerts & Notifications
https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/cyber-security-alerts-notifications

Canadian Centre for Cyber Security
https://cyber.gc.ca/

Center for Internet Security
https://www.cisecurity.org/

Cloud Security Alliance's Consensus Assessments Initiative Questionnaire V3.0.1
https://downloads.cloudsecurityalliance.org/initiatives/cai/caiq-v3.0.1.zip

CyberSecure Canada
https://www.ic.gc.ca/eic/site/137.nsf/eng/h_00000.html

Enhancing Canada's Critical Infrastructure Resilience to Insider Risk
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nhncng-crtcl-nfrstrctr/index-en.aspx

Federal Financial Institutions Examination Council (FFIEC) Cyber Security Assessment Tool
https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf

Financial Stability Board Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices
http://www.fsb.org/wp-content/uploads/P131017-1.pdf

Financial Stability Board Cyber Lexicon
http://www.fsb.org/wp-content/uploads/P121118-1.pdf

GCHQ National Cyber Security Centre
https://www.ncsc.gov.uk/

Government of Canada Cyber Security Event Management Plan (GCCSEMP) 2018
https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html

Infragard
https://www.infragard.org/

IIFA Cybersecurity Program Basics
https://www.iifa.ca/files/1571405868_IIFA%20Cybersecurity%20Program%20Basics.pdf

Information Systems Audit and Control Association (ISACA) Control Objectives for Information and Related Technology (COBIT)
http://www.isaca.org/cobit/pages/default.aspx

National Institute of Standards and Technology
https://www.nist.gov/topics/cybersecurity

National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity
https://doi.org/10.6028/NIST.CSWP.04162018

RCMP National Cybercrime Coordination Unit (NC3)
http://www.rcmp-grc.gc.ca/en/the-national-cybercrime-coordination-unit-nc3

SANS Top 20 Critical Security Controls
http://www.cisecurity.org/critical-controls/

University of British Columbia's Third-Party Assessment Questionnaire
https://it.ubc.ca/sites/it.ubc.ca/files/3rd%20Party%20Outsourcing%20Information%20Security%20Assessment%20Questionnaire%20V1.4.xlsx