Cybersecurity Guide

August/2016

ANBIMA

Contents

This Guide was published on August 3, 2016 with the aim of helping to improve cybersecurity procedures in Brazil's financial and capital markets. It should not be regarded as a unique and exhaustive source and the institutions should always consult the prevailing legislation and regulations.

Introduction

Purpose of the Guide

Organizations and its representatives rely on technological resources and the internet to carry out their main activities. Not only the physical environment – mobiles, computers, smartphones, tablets – is potentially vulnerable to cyberattack, but also the digital one – systems, e-mail, telecom connectivity, BPO firms, intercompany data transfers, cloud operations, etc. –.

Studies have shown[1] that these attacks have been growing exponentially in terms of volume and becoming increasingly sophisticated, resulting in heightened risk and potential costs and losses for companies. Institutions operating in the financial and capital markets are particularly attractive targets due to the scale of their financial transactions and the sensitivity of the information they possess, exemplified by the following (among others):

- Information on clients (current and potential);
- Database (including historical information);
- Business plan and confidential strategies/investments;
- Intellectual property (e.g. trading algorithms);
- Proprietary portfolio;
- Client portfolio positions;
- List of users and passwords; and
- Trading systems.

Regulators and self-regulators have been paying increasing attention to issues associated with cyber risk in order to provide guidance to the institutions in their respective markets, and verify if their structures are equipped to identify and mitigate these risks and recover from possible attacks.

In order to help those institutions who are signatories to its Codes of Regulations and Best Practices, ANBIMA has prepared this Guide, whose primary purpose is to outline effective practices for the implementation of a cybersecurity program, thereby contribute to the improvement of cybersecurity in Brazil's financial and capital markets. However, the practices described herein do not constitute a unique and exhaustive list of the initiatives institutions can take to strengthen their cybersecurity, there being various sources and resources that can also provide help with the implementation of such a system.

[1] See Appendix, p. 15.

Finally, it is worth emphasizing that threats to cybersecurity, as well as its associated practices and solutions, evolve rapidly, requiring institutions to constantly adapt. Consequently, this Guide may also be reassessed and updated in the future or supplemented by additional material and/or guidelines.

- **The Guide offers examples and recommendations to guide institutions and help improve cybersecurity in Brazil's markets.**
- **There are no maximum or minimum standards.**
- **Implementation of the recommendations depends on the specific characteristics and needs of each institution.**

Cyber risk

Advances in technology have streamlined processes and procedures and allowed institutions to adopt new tools, enabling them to structure and implement services with added speed and flexibility, as well as expand their means of communication, among other benefits. On the other hand, the increasing use of such tools potentializes the risk of cyberattacks, threatening the confidentiality, integrity and availability of the institutions' data and/or systems.

These attacks are carried out by several types of agent (criminal organizations, individual hackers, state authorities, terrorists, employees, competitors etc.) for a variety of reasons, the main ones being:

- For financial gain;
- To steal, manipulate or alter information;
- To obtain competitive advantages and confidential information from competitors;
- To defraud, sabotage or expose the invaded institution, possibly for revenge purposes;
- To promote political and/or social ideas;
- To practice terror and propagate panic and chaos; or
- To confront challenges and/or excite the admiration of famous hackers.

The invaders have several means of cyberattack at their disposal, the most common of which are listed below[2]:

- Malware – malicious software designed to disrupt computers and networks:
  - Virus: software that damages computers, networks, software and databases;
  - Trojan horse: a program within another software that opens a door for invasion of the computer;
  - Spyware: malware for collecting and monitoring the use of information; and

2 See the SANS Glossary of Terms for definitions of the most used terms. Available at: https://www.sans.org/security-resources/glossary-of-terms

  - Ransomware: malware that blocks access to systems and databases and demands a ransom payment to restore it.
- Social engineering – methods of manipulation designed to obtain confidential information, such as passwords, personal details and credit card numbers:
  - Pharming: directs users to a fake site without their knowledge;
  - Phishing: attempts to obtain confidential information through e-mail links to come from trustworthy individuals or companies;
  - Vishing: attempts to obtain confidential information by telephone calls from purportedly trustworthy individuals or companies;
  - Smishing: attempts to obtain confidential information through text messages from purportedly trustworthy individuals or companies; and
  - Personal access: persons located in public places such as bars, cafeterias and restaurants in order to pick up any information that may be used subsequently for an attack.
- DDoS (distributed denial of service) attacks and botnets – attacks designed to deny or delay access to the institution's services or systems; in the case of botnets, the attack comes from a huge number of infected computers used to create and send spam or viruses, or to inundate the network with messages, resulting in denial of service.
- Advanced persistent threats – attacks carried out by sophisticated invaders using knowledge and tools to detect and exploit specific weaknesses in a technological environment.

Cyber threats vary in line with each organization's nature, vulnerability and information/goods. Their consequences may be substantial in terms of image risk, financial damage or loss of competitive advantage, not to mention possible compliance risks, while the extent of their impact depends on rapid detection and response after the attack has been identified[3]. Both major and minor institutions can be affected.

- **Financial institutions cannot afford to ignore cyber risk.**
- **Attacks threaten the institutions' confidentiality and integrity and/or the availability of their data and systems.**
- **Regulators are focusing on identifying the weak points in capital market cybersecurity.**
- **Clients and partners have been increasingly questioning the security of the institutions.**

[3] According to FireEye, for example, in 2014, cyber criminals remained inside their victim companies' networks for an average of 205 days before being detected.

Implementing a cybersecurity program

How to begin

Given that cyberattacks are becoming more frequent and increasingly sophisticated, ANBIMA believes it is vital that institutions create cybersecurity programs in order to protect themselves and reduce the risk and possible consequences of such threats. Such programs can, at the criterion of each institution, be included in their information security policy, a document required by some of ANBIMA's Codes of Regulations and Best Practices[4].

Institutions can make use of existing national or international standards to develop their cybersecurity programs. These standards may focus on cybersecurity *per se* or cover the institutions' governance and information technology management systems in a broader manner, serving as points of reference to help the institutions assess their practices and define important elements for the construction and development of the program, always aiming to improve their cybersecurity.

Risk assessment

Institutions are advised to implement a cybersecurity program based on their needs, preparing and maintaining an up-to-date risk assessment. Such efforts should be compatible with the size and characteristics of the institution in question, and the defense and response resources should be proportional to the risks identified.

The assessment should consider the institution's environment, objectives, stakeholders and activities. It's recommend that this assessment, at the very least:

- Identifies the institution's critical assets (whether systems, data or processes) and potential vulnerabilities;
- Identifies the recurrence of global cyber threats, maintaining them in the database;
- Assesses the possible financial, operational and reputational impacts and the likelihood of their occurrence;
- Measures internal and external risks, including systemic risks, whether critical or not, by analyzing vulnerabilities, threats and possible impacts; and

Defines and prioritizes the responses and initiatives needed to deal with the risks identified. One important aspect of risk assessment is the identification of residual risks, i.e., risks that have been

[4] ANBIMA Code of Regulations and Best Practices for Private Equity and Venture Capital Funds (FIP and FIEE); ANBIMA Code of Regulations and Best Practices for Investment Funds; ANBIMA Code of Regulations and Best Practices for Domestic Market Private Banking Activities; and the ANBIMA Code of Regulations and Best Practices for Qualified Capital Market Services.

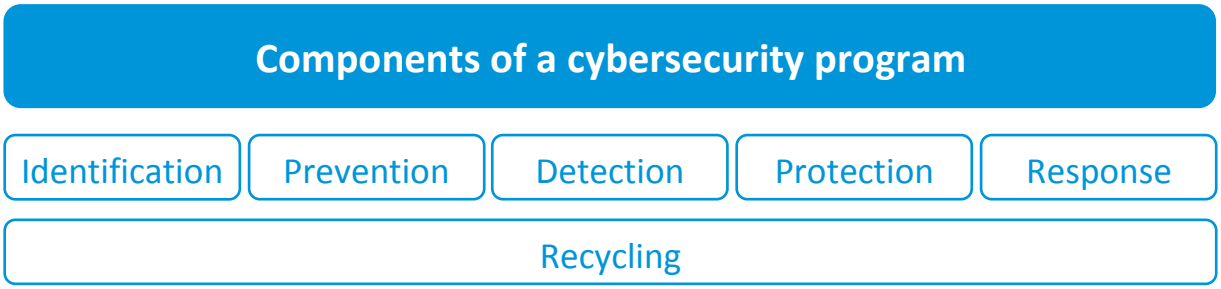
detected and for which there are no appropriate mitigation strategies. In this case, suitable scaling mechanisms should be considered, as well as the means of reducing these risks in the future.

- **The cybersecurity program is based on an analysis of the specific risks of the institution in question.**
- **Implementation of the program may take several years.**
- **Institutions can base their initiatives on existing standards.**

Components of a cybersecurity program

An effective program for combating cyberattacks should have at least six well-defined functions:

- **Identification** – identification of the internal and external risks and the assets and processes that need to be protected, as dealt with in the risk assessment section above;
- **Prevention** – establishment of a set of measures designed to mitigate threats, i.e., anticipate and prevent cyberattacks, through the application of due diligence, either by raising the awareness of the various stakeholders or through research into and investigation and analysis of the communications and information under attack;
- **Detection** – detection of threats in a timely manner, strengthening controls if necessary, and identification of possible anomalies in the technological environment, including the presence of unauthorized users, components or devices;
- **Protection** – the programing and implementation of the necessary controls to combat detected threats and attacks;
- **Response** – preparation of a response plan and the remedying and repair of incidents, including an internal and external communications plan, if necessary; and
- **Recycling** – maintenance of a cybersecurity program subject to constant testing and updates.



Source: ANBIMA, GT Cybersecurity.

Elements of a successful cybersecurity program

Based on recently published cybersecurity guides[5], ANBIMA has listed below certain items that sustain and complement the components outlined in the previous section and are considered to be important elements for the effectiveness of the programs in all the institutions.

Governance

Establishing internal cybersecurity governance procedures is an absolutely essential element of the program. In this context, the main points to be observed in the specific internal policies and procedures for protecting against cyberattacks are:

- Definition of decision-making responsibilities within the action plan, including at the moment of incident response;
- Creation of a specific committee, forum or group to deal with cybersecurity, with appropriate representation and governance;
- Periodic audits of the measures and initiatives defined by the responsible body; and
- Promotion of a security culture within the institution (tone from the top).

The commitment of senior executives, business lines and other stakeholders is a critical factor in ensuring progress with institutional security. Initiatives such as the definition and maintenance of key performance indicators can corroborate the awareness and involvement of top management and other bodies of the institution.

- **One of the major obstacles is the cultural issue.**
- **Senior executives have an important role to play in advancing the maturity of the structure.**

User control and awareness

Institutions' employees are almost certainly the most sensitive link in any cybersecurity program, given that the program's effectiveness is not only dependent on equipment and security solutions, but also on employees' awareness of the importance of security practices. It is therefore important to adopt the following procedures and controls:

- A minimum set of rules for defining the passwords giving access to corporate devices, systems and the network;
- Periodic changes to access passwords and network and workstation administrator

[5] See Appendix, p. 16.

authorizations;

- Definition of employees' and network administrators' access profiles, limiting employee access to confidential information and critical systems, and the periodic review of these accesses – users with "normal" privileges should also be prevented from installing or disabling any software or service being executed in the system;
- Rigorous control over the use of privileged accounts, including to ensure that this type of account is not used for activities posing a high risk to the user, e.g. to gain access to external e-mails or for browsing the internet;
- Prevention of the installation and execution of unauthorized software and applications through process execution controls (e.g. whitelisting);
- Definition of service provider access profiles, restricting access to confidential information and critical systems (e.g. data warehouses or others related to business intelligence or strategic decision-making aids);
- Management and control of privileged access, including measures for the rapid annulment of access to systems and information when no longer necessary;
- Access control policies for tasks performed outside the office via mobile phone and other personal and corporate devices, imposing rules and limits on the granting of said access;
- Cybersecurity training for executives and employees in general (including for new entrants and periodically over time), observing that the effectiveness of such programs gaining considerable strength if accompanied by simulations (e.g. phishing tests for the institution's employees), which help promote cultural change in the teams; and
- The establishment of communications and disclosure channels for internal policies and procedures to help with their propagation and the definition of practices and procedures, including new guidelines.

Technological controls

In order to protect against cyber threats, institutions should possess at least a basic technological structure, which includes items such as:

- Protection for data in storage or in transit, containing secure backup and encryption tools if necessary; databases and network devices should be sent to a dedicated security system that is strictly controlled in order to preserve the integrity, confidentiality and availability of the content;
- The use of digital signatures for key processes/employees;
- Up-to-date hardware and software inventories;
- Updating of the institutions' systems, infrastructure and software;
- Threat prevention through the use of firewalls, antivirus programs, specific access profiles for equipment administrators, spam filters, control over the use of peripheral devices (flash drives, CDs and HDs), invader penetration tests and internet filters;
- Control over the use of peripheral devices to prevent unauthorized copies of data (e.g. flash drives, CDs and HDs) and monitoring of the printing of confidential data;
- Detection of threats and the monitoring of anomalies (e.g. through operating system

activity logs, analysis of erroneous logins or unusual downloads) and unauthorized users in the institution's networks;
- Inclusion of security concerns in the development phase of new system software and applications;
- Audit controls, such as password management systems and access trails and logs;
- The use of fictitious data (masking of critical data) in non-productive environments, or other measures aimed at improving the security of non-productive environments and the protection of the associated data;
- Physical and digital separation of the development, test and production environments; and
- Establishment of the same level of security and protection for applications as for critical information.

Institutions should define appropriate controls for client access to their online services and for communications with their clients, either recurring (e.g. statements) or one-off.

Recent advances such as the use of cloud technology may generate additional risks by establishing porosity between the institutions' internal and external systems. Although cloud technology can bring certain cybersecurity benefits, especially for smaller institutions, it would be wise to take special care with this issue, including in terms of access management.

Physical controls

It is vital that institutions adopt physical security procedures, as well as controls over access to their installations, including:

- Office installation access profiles;
- Access control and management;
- Suitable and secure physical space for equipment storage;
- Restricted physical access to critical/sensitive information location;
- Security and access controls for contingency installations;
- Remote access for users duly identified and authenticated and, if necessary, the use of encrypted connections to access the company's environment from outside;
- Exclusive use of registered equipment by the information technology and architecture area.

- **Basic controls substantially increase the level of security, being capable of preventing a good deal of the more simple attacks.**
- **These controls should be the object of training programs.**
- **The choice of specific controls depends on the circumstances of each institution.**
- **Institutions should assess the need for tools such as encryption or penetration tests.**

Incident response plan

Institutions must be capable of reacting to incidents in a timely manner with a scaling and response plan. Consequently, it is important to define:

- Incident classification criteria, by degree of severity;
- A list of critical assets, in accordance with the risk assessment already drawn up by the institution;
- Detection and investigation procedures (including, whenever possible, evidence collection procedures – see below) to streamline problem identification and correction;
- A plan for the engagement of key employees and important external contacts;
- The taking of decisions and implementation of technical initiatives in line with the various possible attack scenarios (loss of client data, DDoS attacks, infection, intrusion, etc.);
- A communications plan involving, in line with the concrete risks inherent to the incident, clients and other partners, regulators and, if necessary, the media;
- Remedial measures; and
- A business continuity plan[6] and recovery processes, including, if the case, the restoration, reconstruction and replacement of the affected systems and databases.

The incident management process should be developed in line with business activities in order to cover the entire range of cyber incidents that can occur in the corporate infrastructure.

Documentation related to incident management should be duly filed for use as evidence in possible inquiries.

It is vital that the response plan consider the possibility that systems, networks and databases, as well as the physical structure of the institution, may be rendered inaccessible or be corrupted. We also recommend that institutions regularly update and test their response plans.

It is also advisable that various areas of the institution take part in preparing the plan in addition to the technological security area, including the legal, compliance and communication departments.

- **Testing and rehearsing the response plan are important elements in the identification of failures and in the improvement of the associated mitigation strategies.**
- **Exercises help employees become more comfortable with their roles and responsibilities when faced with a real cybersecurity incident.**

[6] Some ANBIMA Codes of Regulations and Best Practices already require member institutions to have a BCP

Investigative process

Cybersecurity investigations include data collection, analysis and preservation (as applicable) with the aim of identifying the origin and characteristics of each invasion or attack. In order for the investigations to be successful, a protocol should be defined to guide the analysis, with the interruption of the attack or not, accompanied by the use of forensic techniques for the preservation of evidence in the case of legal requirements.

It is recommended that a historical record of the analyses is kept in order to identify indicators capable of predicting tendencies and behaviors.

Dialogue with third parties

Suppliers, service providers and partners ("third parties") can represent a significant source of risk for the institutions. It is recommended that the institutions discuss their cybersecurity controls with these parties before entering into service provision agreements and during their execution. In general, the desirable level of diligence depends on the risk that the relationship with the supplier could generate for the institution. Specific care may also be needed when concluding relations with third parties (annulment of system access, etc.). Special attention should also be given to suppliers who receive and/or deal with client data or data deemed to be confidential, as well as those with digital links with the institution.

It is important that the institutions maintain policies[7] for verifying the cybersecurity procedures of contracted third parties, assessing and monitoring their ability to avoid cyberattacks. They are also advised to have a process in place for assessing and monitoring the risks represented by these parties, as well as procedures for their formal approval by the responsible internal bodies, with the periodic review of said approvals.

If necessary, and depending on the risk assessment, the due diligence process may include the verification of the third parties' internal policies and procedures, as well as visits to their facilities. In certain cases, this verification may also cover subcontractors.

As part of the dialogue with suppliers and service providers, institutions may consider including specific provisions related to cyber risk in their service agreements.

- **Third parties represent another source of risk.**
- **Institutions should assess and manage cyber risk throughout their relationship with third parties.**

[7] Certain ANBIMA Codes of Regulations and Best Practices require, in certain situations, that the institution maintain an internal policy describing its selection, contracting and monitoring processes for certain determined service providers.

Prevention of internal attacks

Good practices[8] for the prevention of internal attacks combine technological tools (e.g. for network monitoring) with internal knowledge of the institutions' human factors. Certain indicators can reveal dubious behavior (repeated login failures, massive data downloads, etc., as well as conflicts between employees or threats).

There are various initiatives to help prevent internal attacks, such as user and physical controls (see above), raising the awareness of employees (e.g. through the use of concrete cases), complaint and ombudsman's channels for reporting indications of dubious behavior, including, in certain cases, the creation of a specific team, as well as any other procedures that help detect the leaking of data and/or fraud on the part of the institution's employees, service providers and suppliers. Legal aspects (privacy of information and confidentiality, among others) should also be considered.

Access to information

Given their pace of change, it is vital to define tools for accessing intelligence of threats in the media, internet and dark web, as well as through mechanisms for sharing information or via specialized suppliers with intelligence on the evolution of threats.

Institutions will also benefit from participating in groups or forums to exchange experience and information, including for the purpose of ensuring that the cybersecurity program is always up to date, fully equipped to meet new needs and incorporating the industry's most recent advances in regard to confronting cyber risk.

- **The establishment of relations of trust and mechanisms of collaboration help ensure a collective response to cyber risk.**
- **Whenever possible, institutions should procure access to information and incorporate it into their responses.**

[8] For example, see SIFMA, *Best Practices for Insider Threats*. Available at: http://www.sifma.org/uploadedFiles/Issues/Technology_and_Operations/Cyber_Security/insider-threat-best-practices-guide.pdf?n=45727.

Disclosure of the cybersecurity program

As already mentioned, one of the greatest difficulties when implementing a cybersecurity program is educating the executives and employees to habitually adopt the necessary routines and controls, e.g. restrictions on internet use and access to personal e-mails and social media. Some cyberattacks can originate internally if employees use devices, applications, sites and social media not authorized by the institution or that are not compatible with its security protocols. The program should therefore encourage executives and employees to adopt good practices (e.g. when defining passwords) and become sensitive to possible threats (e.g. in the case of phishing).

It is therefore advisable to create internal communications channels for the efficient disclosure of the cybersecurity program, the raising of awareness of security risks and practices, and the reception of eventual denunciations of program non-compliance.

We recommend that the institutions implement periodic employee training courses on the issue, as well as maintain open channels for the clarification of doubts and the reception of suggestions or alerts. The holding of periodic simulated exercises with the main areas involved, incorporating the most likely attack scenarios, strengthens the awareness-raising process and permits the constant improvement of the program. Finally, it is worth emphasizing once again employees' responsibility in regard to cyber risk and the need to ensure the involvement of the institution's senior management. It is therefore advisable to indicate a specific officer as being responsible for cybersecurity in order to ensure that sufficient resources (both financial and human) are allocated to the efficient implementation of the program and the propagation of a security culture within the institution.

Basic procedures

In general, ANBIMA believes it is possible to adopt basic, low-cost procedures by implementing the following measures.

Function	Description
Definition of roles and responsibilities	Indication of the executive and area responsible for implementing the cybersecurity program and dealing with any incidents.
Definition of the systems, network, database and server access systems	Access profile matrix, clearly separating functions and responsibilities, in order to avoid undue access and permit the monitoring of all accesses.
Password definition rules	Minimum rules governing the number and type of characters used in the passwords and the frequency of change.
Monitoring of internet use	Rules governing internet use, the blocking of sites that may generate additional risks and the monitoring of use by employees.
Download rules	Rules governing downloads in order to prevent the downloading of files from dubious sources, as well as unnecessary items.

Upload rules	Restricting the permission to upload to internet sites to users duly authorized to do so, subject to periodic review procedures.
Controls over e-mail, media and peripheral device use	Rules governing the use and monitoring of these tools, in order to prevent the entry of harmful items and/or the exit of confidential/sensitive information. Monitoring and authorizing the sending of external e-mails, as well as forbidding the use of external e-mail services (e.g. gmail, hotmail, yahoo etc.).
Audit trails and keeping of the logs	Filing of audit trails and logs, permitting the detection of suspect commands and undue accesses. Log-keeping period also to be defined.
Backup rules	Determine the backup frequency and the means of storage and access control, ensuring that all the information has a secure secondary data source.
Control over the entry and exit of equipment	Control over the movement of equipment to ensure non-alteration.
Control of service providers	Rules governing service providers' physical and digital access, as well as the inclusion of confidentiality clauses in their contracts.
Security software	Use of security software such as firewalls, antivirus programs and others.
Upgrading of systems, infrastructure and software	Ensuring that systems, infrastructure and software are always up to date.
Classification of information	Rules governing the classification of information, preventing undue access or disclosure, or requiring its encryption.
Information life cycle	Secure processes for the due handling, storage, transport and disposal of information.
Dissemination of the security culture	Mechanisms to disclose the anti-cyberattack program, such as the holding of training programs, and the creation of internal communication channels or simulations.

Appendix

There follows a (non-exhaustive) list of the main reports and sources consulted when preparing this Guide:

- Alternative Investment Management Association (AIMA), *Guide to Sound Practices for Cybersecurity* (available to AIMA members), October 2015.
- BM&FBovespa, *Programa de Qualificação Operacional, Roteiro básico*. Available at: http://www.bmfbovespa.com.br/pt_br/regulacao/programa-de-qualificacao-operacional-pqo/roteiros/
- Commodities and Futures Trading Commission (CFTC), *Recommended Best Practices for the Protection of Customer Records and Information*, February 2014. Available at: http://www.cftc.gov/idc/groups/public/@lrlettergeneral/documents/letter/14-21.pdf
- Central Bank of Ireland, *Review of the Management of Operational Risk Around Cybersecurity within the Investment Firm and Fund Service Industry*, September 2015. Available at: https://www.centralbank.ie/regulation/industry-sectors/investment-firms/mifid-firms/Documents/Industry%20Letter%20-%20Thematic%20Review%20of%20Cyber-Security%20and%20Operational%20Risk.pdf.
- Comissão Parlamentar de Inquérito dos Crimes Cibernéticos, *Relatório final,* May 2016. Available at: http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos
- Financial Industry Regulatory Authority (FINRA), *Report on Cybersecurity Practices*, January 2015. Available at: https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf
- Hedge Fund Standards Board (HSFB), *Cybersecurity Toolbox for Hedge Funds Managers*, October 2015. Available at: http://www.hfsb.org/sites/10377/files/regulators_on_cybersecurity.pdf
- Investment Company Institute (ICI), *Information Security Resource Center*. Available at: https://www.ici.org/info_security.
- Investment Industry Regulatory Organization of Canada (IIROC), *Cybersecurity Best Practices Guide for IIROC Dealers Members*, March. 2016. Available at: http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf.
- Investment Industry Regulatory Organization of Canada (IIROC), *Cybersecurity Incident Management Planning Guide*, March 2016. Available at: http://www.iiroc.ca/industry/Documents/CyberIncidentManagementPlanningGuide_en.pdf

- International Organization of Securities Commissions (IOSCO), *Cyber Security in Securities Markets - An International Perspective*, Available at: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf
- National Futures Association (NFA), *Information Security Programs*, October 2015. Available at: http://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9.
- National Institute of Standards and technology (NIST) Cybersecurity Framework. Available at: http://www.nist.gov/cyberframework.
- SANS Institute. Available at: http://www.sans.org.
- Securities Industry and Financial Markets Association (SIFMA), *Cybersecurity Resource Center*. Available at: http://www.sifma.org/issues/operations-and-technology/cybersecurity/resources.
    - SIFMA, *Guidance for small firms*, July 2014;
    - SIFMA, *Best practices for insider threat*, July 2014; and
    - SIFMA, *Third Party Management Program Implementation Tips*.
- US Securities and Exchange Commission (SEC), *Investment Management Cybersecurity Guidance*, April 2015. Available at: https://www.sec.gov/investment/im-guidance-2015-02.pdf.