Cybersecurity Guide

December/2017

ANBIMA

Contents

This 2nd edition of the Guide was published on December 6, 2017 (1st edition published on 8/3/16). The objective is to contribute to the improvement of optional cyber security practices in the financial and capital markets of Brazil. The guide should not serve as a single, exhaustive source. Institutions should always consult existing legislation and regulations.

Introduction

With the exponential increase in cyber threats in recent years, both in volume and in sophistication, 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 to verify if their structures are equipped to identify and mitigate these risks and recover from possible attacks.

In this respect, ANBIMA understands that it is extremely important that the institutions structure a Cyber Security Program. This program may, at the discretion of each institution, be included in the information security policy, a document required by some of ANBIMA's Codes of Regulation and Best Practices[1].

To develop a cyber security program, institutions can be build in existing national or international standards. (See Appendix). These standards can specifically focus on cybersecurity or more fully treat governance and information technology management within institutions. They can serve as landmarks and help institutions to value their practices and define relevant elements in construction and development of their program.

In 2016, in order to help those institutions who are signatories to its Codes of Regulation and Best Practices, ANBIMA launched 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.

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.

[1] ANBIMA's Code of Regulation and Best Practices for the FIP and FIEE Market; ANBIMA's Code of Regulation and Best Practices of ANBIMA of Investment Funds; ANBIMA's Code of Regulation and Best Practices for the Private Banking Activity in the Domestic Market; and ANBIMA's Code of Regulation and Best Practices of Qualified Services to the Capital Market.

This 2nd edition of the Guide was published on December 6, 2017 (1st edition published on 8/3/16). The objective is to contribute to the improvement of optional cyber security practices in the financial and capital markets of Brazil. The guide should not serve as a single, exhaustive source. Institutions should always consult existing legislation and regulations.

- **The Guide offers examples and recommendations to guide institutions and help improve cybersecurity in Brazil's markets.**
- **The practices described in this Guide do not constitute a unique and exhaustive list of initiatives that institutions can take to strengthen their cybersecurity.**
- **There are several sources and resources available that can also assist institutions as they progress implementing the cybersecurity program.**
- **Implementation of the recommendations depends on the specific characteristics and needs of each institution.**

This 2nd edition of the Guide was published on December 6, 2017 (1st edition published on 8/3/16). The objective is to contribute to the improvement of optional cyber security practices in the financial and capital markets of Brazil. The guide should not serve as a single, exhaustive source. Institutions should always consult existing legislation and regulations.

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 to 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.

For a variety of reasons, these attacks are carried out by several types of agents (criminal organizations or individual hackers, state authorities, terrorists, employees, competitors etc.). 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 inflict 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 following are the most common[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
    - 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 from trustworthy individuals or companies;
    - vishing: attempts to obtain confidential information by telephone calls from purportedly trustworthy individuals or companies;

[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

  - 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 operational risks. 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.**

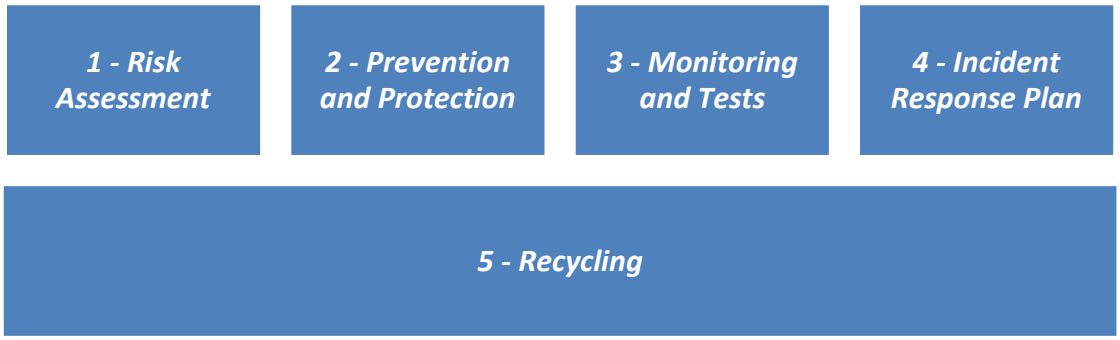
3

This 2nd edition of the Guide was published on December 6, 2017 (1st edition published on 8/3/16). The objective is to contribute to the improvement of optional cyber security practices in the financial and capital markets of Brazil. The guide should not serve as a single, exhaustive source. Institutions should always consult existing legislation and regulations.

Implementing a cybersecurity program

ANBIMA recommends that an efficient program against cyber threats should contain, at least, five well defined functions:

1. **Risk assessment** – identification of the internal and external risks, the hardware and software assets and processes that need to be protected.
2. **Prevention and Protection** – establishment of a set of measures designed to mitigate threats and minimize the concretization of the risks identified in the previous item, that is, seek to prevent a cyber attack, including the programming and implementation of controls.
3. **Monitoring and Tests** – 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.
4. **Incident Response Plan** – preparation of a response plan and the fixing and repair of incidents, including an internal and external communications plan, if necessary; and
5. **Recycling** – maintenance of a cybersecurity program subject to constant updates, identification of new risks, assets and processes and reassessing residual risks



See below the details of the five functions, with recommendations considered fundamental for the effectiveness of the programs of each of the institutions, but not limited to them.

1 – Risk Assessment

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.

This 2nd edition of the Guide was published on December 6, 2017 (1st edition published on 8/3/16). The objective is to contribute to the improvement of optional cyber security practices in the financial and capital markets of Brazil. The guide should not serve as a single, exhaustive source. Institutions should always consult existing legislation and regulations.

– Recommendations:

1. During the initial risk assessment, all relevant processes and assets of the institution (whether equipment, systems or data) used for its correct functioning must be identified.
2. It is recommended to create rules for the classification of information generated by the institution, allowing the implementation of processes for the proper handling, storage, transport and disposal of this information.
3. The vulnerabilities of the assets in question should be evaluated by identifying the potential threats and the degree of exposure of the assets to them. Several scenarios should be considered in this evaluation.
4. Possible financial, operational and reputational impacts should be considered in the event of a security event. Just as the expectation of such an event.
5. A specific committee, forum or group should be created to address cyber security within the institution, with appropriate representation and governance.
6. Once the risks are defined, prevention and protection actions must be taken.
7. There are several methodologies for evaluating cybernetic risk, suitable for different institutions. Some examples are indicated in the references.

2 – Prevention and Protection

– Recommendations:

1. Control appropriate access to the institutions' assets. The implementation of these controls involves the identification, authentication and authorization of users, or systems, to the assets of the institutions.
2. Establish minimum rules in the definition of access codes for corporate devices, systems and networks - complexity, recurrence and multi-factor authentication - depending on the relevance of the asset accessed.
3. Segregate passwords between services. It is currently recommended to use a password manager than the use of the same password to facilitate the memorization of various services.
4. Limit access, once granted, to only resources relevant to the performance of activities. The granting of access must be implemented so that it can be revoked quickly, if necessary.
5. The login events and change of passwords must be auditable and traceable.
6. It is important to note that the institutions' assets may be located internally or externally to the institution's environment, often in the cloud. Adequate control should provide local or remote access to assets that are also local or remote as well as predict the possibility of using personal devices in such cases. For more references on secure cloud configurations, see the references.
7. By including new equipment and systems in production, ensure that safe configurations of your resources are made. It is highly recommended to test in an environment of approval and proof of concept before being sent to production. Just as a reference, so-called "hardening" can be applied to operating systems, applications, restricting available network services and

encrypting data in transit, as well as configuring cloud structures, among others.
8. Restrict physical access to areas with critical / sensitive information.
9. Implement a backup service of the various assets of the institution.
10. Create logs and audit trails whenever systems allow.
11. Perform diligence in contracting third-party services, including cloud services. Suitability to legal issues should be evaluated. Confidentiality clauses and requirement of security controls in the very structure of third parties are desirable. For proposition of model of diligence with third party, consult the references.
12. Consider security issues during the phases of pre-design and of development of new systems, software or applications.
13. Implement edge security in computer networks through firewalls and other packet filtering mechanisms.
14. Implement anti-malware features on network stations and servers, such as anti-viruses and personal firewalls.
15. Implement segregation of services whenever possible, restricting data traffic only between relevant equipment.
16. Prevent the installation and execution of unauthorized software and applications through process execution controls (for example, whitelisting applications).

3 – Monitoring and Tests

In general, it is recommended that the institution seek to establish mechanisms and monitoring systems for each of the existing controls.

– Recommendations:

1. As a general rule, mechanisms should be created to monitor all protection actions implemented to ensure their proper functioning and effectiveness.
2. Updated hardware and software inventories should be maintained, as well as frequently verified to identify elements alien to the institution. For example, unauthorized computers or unlicensed software.
3. Operating systems and application software should be kept updated by installing updates whenever they become available.
4. Daily backup routines should be monitored by performing regular data restoration tests.
5. External intrusion and phishing tests should be run periodically.
6. Vulnerability analyses should be carried out in the technological structure periodically or whenever there is a significant change in structure.
7. It is suggested to test the incident response plan periodically, simulating the scenarios specified during its creation.
8. The logs and audit trails created should be regularly reviewed to allow rapid identification of attacks, whether internal or external. The use of centralization and log analysis tools is especially recommended.

4 – Incident Response Plan

– Recommendations:

1. It is recommended the involvement of several areas of the institution in the elaboration of the formal plan, besides the area of technological security, such as legal, compliance and communication departments.
2. There should be definition of roles and responsibilities within the action plan, providing for the activation of key employees and relevant external contacts.
3. The plan shall take into account the threat scenarios identified in the risk assessment.
4. There should be criteria for classification of incidents by severity. They can require simple duplication of equipment for continuity of services or the use of contingency facilities in more severe cases, among other measures. In such cases, the plan should also contemplate the return process to the original facilities after the end of the incident.
5. Attention should be paid to security issues and access controls in contingency facilities as well.
6. We recommend filing documentation related to incident management and to the business continuity plan, to serve as evidence in any inquiries.

5 – Recycling

– Recommendations:

1. The cyber security program should be periodically reviewed, keeping its risk assessments, protection deployments, incident response plans and environment monitoring up to date.
2. The groups involved in the program must keep updated with new identified vulnerabilities and threats that may alter the institution's exposure to the originally assessed risks. This can be done, inter alia, through participation in information-sharing groups, or via specialized suppliers.
3. Institutions should promote and disseminate the security culture by creating effective internal communication channels to promote the cyber security program, as well as to raise awareness of security risks and practices, to train and to refer new directions.
4. Initiatives such as the definition and maintenance of key performance indicators can strengthen the awareness and involvement of top management and other institutions.
5. As part of the mechanisms for raising awareness about the subject, it is important to create a policy of appropriate use of the institution's technological structure, either independently or as part of a more comprehensive document.

Users should be forewarned and pay special attention to any external links, even if they were sent from people they know, before clicking on them. This is currently one of the main vectors of invasion.

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.
- ANBIMA, GT of Cybersecurity, *Referência técnica para configuração segura de ambiente em nuvem* (4/12/2017) – http://www.anbima.com.br/data/files/50/F7/30/E0/D9C206101703E9F5A8A80AC2/Tecnica-para-nuvem-Referencia.pdf
- ANBIMA, GT of Cybersecurity, *Modelos de diligência com terceiros* – Incluindo Provedores de Serviços em Nuvem (4/12/2017) – http://www.anbima.com.br/data/files/84/B7/86/09/B9C206101703E9F5A8A80AC2/Modelo-de-Diligencia-com%20Terceiros-Referencia.pdf
- Central Bank of Brasil, BC Public Consultation 57/2017 - Published in 19/9/2017 (*Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento, armazenamento de dados e de computação em nuvem, a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo BCB)*. Available at: https://www3.bcb.gov.br/audpub/HomePage?1
- BM&FBovespa, *Programa de Qualificação Operacional, Roteiro básico*. Available at: http://www.bmfbovespa.com.br/pt_br/regulacao/programa-de-qualificacao-operacional-pqo/roteiros/
- Câmara dos Deputados, Projeto de Lei 5276/2016 (*Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural*). Available at: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378
- 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
- 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
- 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.
- National Institute of Standards and technology (NIST), *Cloud Computing Program – NCCP*. Available at (acess on 13/9/17): https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp
- New York State Department of Financial Services (DFS), *Cybersecurity Requirements for Financial Services Companies - 23 NYCRR Part 500* (28/12/16). Available at: http://www.dfs.ny.gov/about/press/pr1612281.htm
- New York State Department of Financial Services (DFS), *Cybersecurity*. Available at: http://www.dfs.ny.gov/about/cybersecurity.htm
- SANS Institute. Available at: http://www.sans.org.
- Securities Industry and Financial Markets Association (SIFMA), *Insider Threat Best Practices Guide.* Available at: https://www.sifma.org/wp-content/uploads/2017/08/insider-threat-best-practices-guide.pdf
- 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*.
- 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

- Senado Federal, Projeto de Lei do Senado n° 330/2013 (*Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências*). Available at: https://www25.senado.leg.br/web/atividade/materias/-/materia/113947
- US Securities and Exchange Commission (SEC), *Observations From Cybersecurity Examination*, 7/8/2017. Available at: https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf
- US Securities and Exchange Commission (SEC), *Investment Management Cybersecurity Guidance*, April 2015. Available at: https://www.sec.gov/investment/im-guidance-2015-02.pdf.