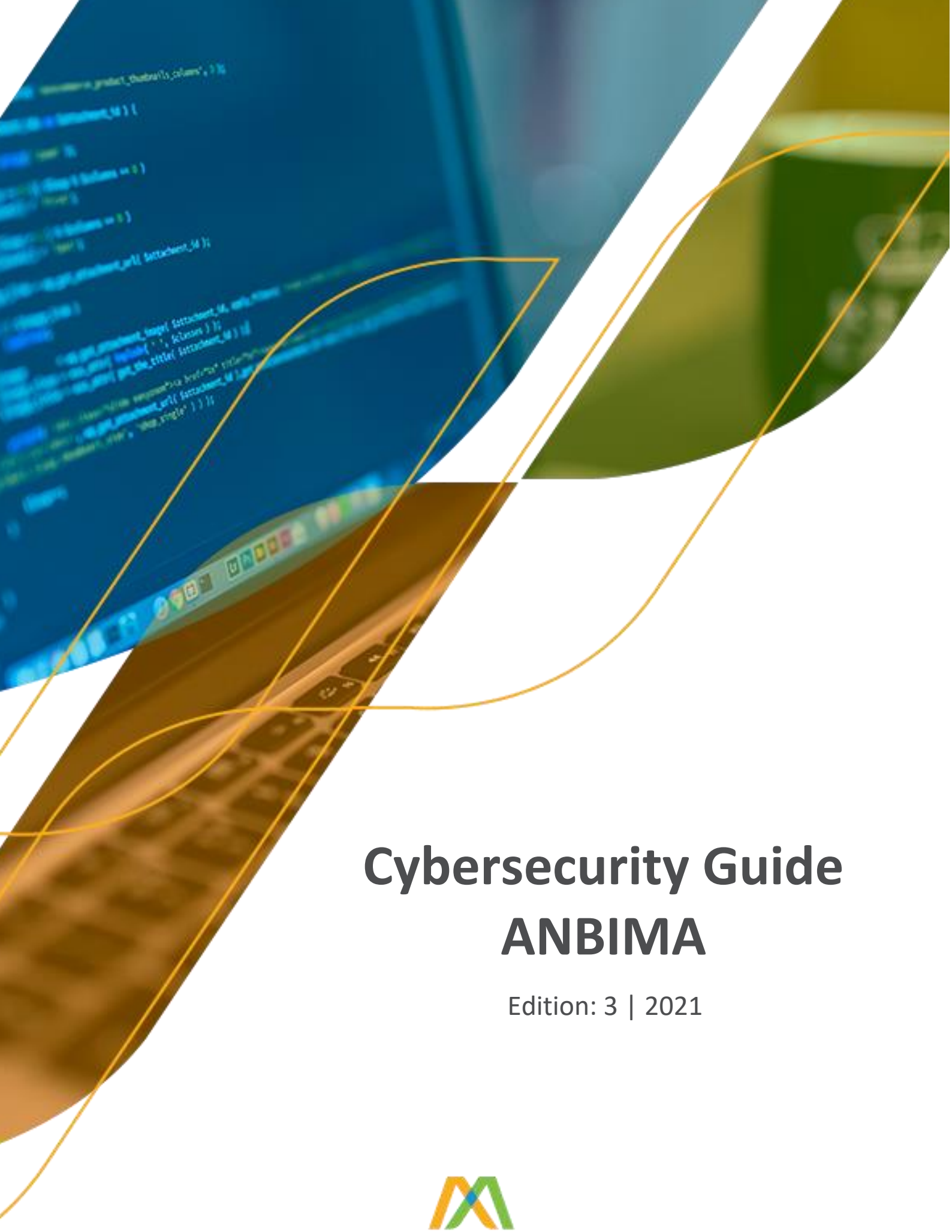


Cybersecurity Guide ANBIMA

Edition: 3 | 2021

ANBIMA

Contents

Presentation

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 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 build on existing national or international standards (See references). 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.

When designing and deploying a cybersecurity program, it is essential to consider that all people linked to the institution are part of the process of securing its assets. From this viewpoint, the concern with cybersecurity is not an issue exclusive to the Information Security department or related areas. Therefore, it is recommended – when developing a cybersecurity program – to consider ways of involving all people linked to the institution, including relevant third-party service providers. For example, this engagement can take place through periodic training that involves the institution's entire hierarchy, in addition to periodic awareness campaigns on the subject matter.

Still as an initial step in the preparation of a cybersecurity program, and in light of Brazil's General Data Protection Act, it should be considered that cybersecurity is one of the components so that the privacy of the holder is ensured by data protection mechanisms[2]. In this way, the importance of involving different areas in the elaboration and treatment of the cyber security program is highlighted, so that it contemplates and addresses concerns that permeate the areas of technology.

In 2016, in order to help those institutions who are signatories to its Codes of Regulation and Best Practices, ANBIMA launched this Guide, which outlines effective practices for the implementation of a cybersecurity program, thereby contributes to the improvement of

[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.
[2] Law 13709 ("LGPD" [*Lei Geral de Proteção de Dados*]), article 5, V- Owner: the individual to whom refer the personal data being processed.

This 3rd edition of the Guide was published in June 2021 (1st edition published in March 2016). The objective is to contribute to the improvement of optional cybersecurity practices in the financial and capital markets of Brazil. **Adherence to the guide is optional** and it should not serve as a single and exhaustive source. Institutions should always consult current legislation and regulations.

cybersecurity in Brazil's financial and capital markets. In 2017, based on the work developed by the ANBIMA Technical Cybersecurity Group, the first version of the document was reformulated and updated, leading to the second edition of the Guide. In 2020, governance for addressing cybersecurity at ANBIMA was restructured, and the Technical Group was replaced by the Advisory Group[3] to the Executive Board, responsible for proposing and conducting the Association's cybersecurity agenda. The COVID-19 pandemic brought lessons that were incorporated into this edition of the Guide, due in large part to the greater incidence of remote work. In this regard, the Guide now has recommendations related to the risk assessment highlighted for third-party service providers, including cloud providers, and recommendations regarding Bring Your Own Device (BYOD), in addition to new aspects related to the Incident Response Plan. It is worth highlighting that the new edition of the Guide does not exclusively address issues related to the pandemic; it also updates the document with best practices evolutions since its last update.

Given the fact that cybersecurity practices and solutions evolve rapidly, requiring constant adaptation by institutions, this Guide will be re-assessed and updated or supplemented by additional guidelines and materials on a timely basis.

- **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.**

[3] For more information, see: http://www.anbima.com.br/pt_br/representar/grupos-detrabalho/ciberseguranca.htm

Cyber Risk

On the one hand, technological advances 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 others. 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:[4]

- 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 cyber invasion;
  - 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.[5]

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

[5] See the US Treasury Department's positioning in the references.

- 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;
  - 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.

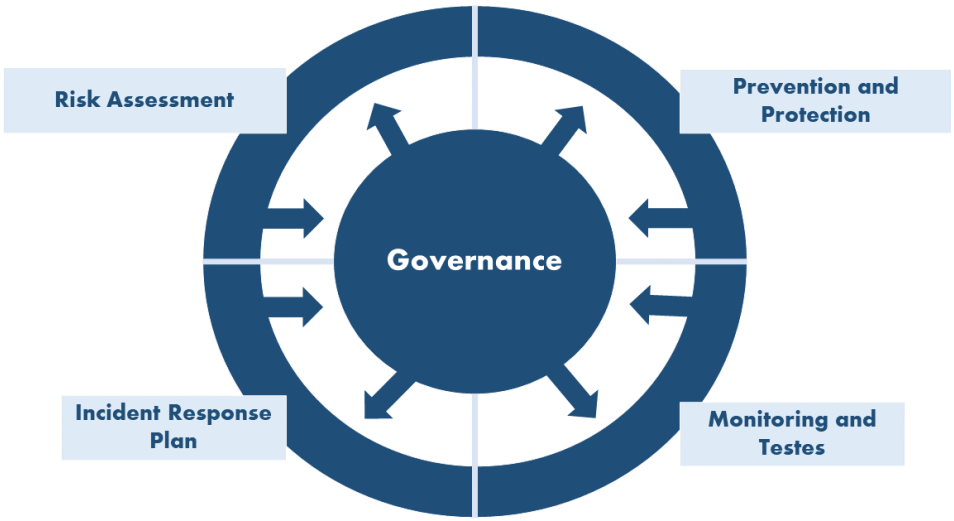
Cyber threats can vary according to the nature, vulnerability and information or assets of each organization. Their consequences may be substantial in terms of image risk, financial damage or loss of competitive advantage, not to mention operational risks. The possible impacts also depend on rapid detection and response once the attack has been identified. 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 cybersecurity weaknesses in capital markets.**
- **Clients and partners have been increasingly questioning the security of the institutions.**

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 internal and external risks, 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;
5. **Governance** – keep the cybersecurity program continuously updated, ensuring that actions, processes, and indicators are regularly carried out, providing feedback to the defined strategy.



See the details of the five functions, with recommendations considered essential for the effectiveness of the institutions' security programs, but not limited thereto.

1 - Risk Assessment

Institutions can make use of existing national or international standards to develop their cybersecurity programs. Cybersecurity efforts should be compatible with the characteristics and size of the institution; likewise, defense resources and responses should be commensurate with the risks identified. The assessment must consider the institution's environment, its objectives, its stakeholders, and its activity.

Recommendations:

1. During the initial risk assessment[6] all relevant assets of the institution (whether equipment, systems, processes or data) used for its correct functioning must be identified.
2. It is recommended to create rules to classify the 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.[7]
4. Possible financial, operational and reputational impacts should be considered in the event of a security event, as well as the expectation that such an event will occur.
5. The risk assessment process should include activities developed by third-party service providers, including cloud services.
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.

[6] For a better understanding of the development of an initial risk assessment in the context of cybersecurity, see (for example): CSA, Guide to Conducting Cybersecurity Risk Assessment for Critical Information Infrastructure (complete data available in the references section).

[7] For a better understanding of the likelihood and impact of occurrences, we recommend using cyber threat information from internal and external sources, such as the framework established by the NIST (e.g., ID.RA-3, available at: https://nvd.nist.gov/800-53/Rev4/control/RA-3, and ID.RA-5, available at: https://nvd.nist.gov/800-53/rev4/control/ra-5)

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 defining access to corporate devices, setting highly complex passwords.
3. Provide for multi-factor authentication whenever possible.
4. Avoid reusing passwords. It is currently recommended to use a password manager rather than repeating the same password, no matter how sophisticated it may be, to facilitate the memorization in various services.
5. Limit access, once granted, only to resources relevant to the performance of activities. The granting of access must be implemented so that it can be revoked quickly, if necessary.
6. The login events and change of passwords must be auditable and traceable.
7. 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 (local or remote) and predict the possibility of using personal devices in such cases (Bring Your Own Device - BYOD).[8]
8. We recommend that remote access be performed using a tool that contains encryption and multiple authentication factors.
9. By including new equipment and systems in production, ensure that secure resource configurations are made. Before being sent to production, the test in approval and proof environment is highly recommended. 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.
10. Restrict physical access to areas with critical/sensitive information.
11. Implement a backup service of the various assets of the institution. We recommend that the backup service be kept separate from the institution’s network.

[8] For more information on secure configurations in cases of BYOD, please see the references. e.g.: NCSC, Guidance for organizations on enabling staff to use their own smartphones, tablets, laptops and desktop PCs to access work information (complete data available in the references section).

12. Create logs and audit trails whenever systems allow.
13. 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.
14. Consider security issues during the phases of pre-design and of development of new systems, software or applications.
15. Implement edge security in computer networks through firewalls and other packet filtering mechanisms.
16. Implement anti-malware features on network stations and servers, such as anti-viruses and personal firewalls.
17. Implement segregation of services whenever possible, restricting data traffic only between relevant equipment.
18. Prevent the installation and execution of unauthorized software and applications through process execution controls (for example, whitelisting applications).
19. Establish controls to mitigate risks and ensure responsibility for possible risks if institutions choose to allow the use of BYOD devices to access their systems and information.
20. Have a policy of control over the institution's data on BYOD devices, ensuring such control will be triggered in employee termination processes.

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, monitoring mechanisms should be created for all implemented protection actions to ensure their proper functioning and effectiveness.
2. Hardware and software inventories should be maintained and updated, and frequently verified to identify elements alien to the institution, including in prolonged remote work and/or access. For example, unauthorized computers or unlicensed software.

3. Operating systems and application software should be kept updated by installing updates whenever they become available. This recommendation also applies to the remote work environment, including in cases of BYOD.
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[9] or external. The use of log centralization and correlation tools is especially recommended, e.g. SIEM (Security Information and Event Management).
9. It is recommended to share attack data through tools or organizations, such as MISP and/or FS-ISAC, among others[10]. Sharing attack incidents on specialized platforms will potentially benefit the industry in general by enabling institutions to assess cybersecurity beforehand and respond to current attacks.
10. The monitoring of security controls must be implemented by adopting a risk-based approach, and intensified according to the level of risk, considering the context in which the institution operates and the emerging needs.

4 - Incident Response Plan

Recommendations:

1. We recommend the involvement of multiple departments/areas at the institution in the preparation of the formal plan and the handling of incidents, including senior management. In addition to the technological security and risk area, which deal with operational risks, departments such as Legal, Compliance and Communication should also be included. For better response treatment, events and incidents already incurred must be reported to the corporate governance department and evaluated by internal committees formed by multiple areas.
2. The action plan must contain mechanisms that ensure immediate communication to all relevant employees regarding incidents that may generate risks to the company. There should be clearly defined roles and responsibilities, and provide the activation of key

[9] For best practices in preventing and monitoring internal attacks, see (for example): SIFMA, Best Practices for Insider Threats (complete data available in the references section).

[10] The mention of the specified tools serves merely as an example and does not represent any prior evaluation by the Association. It is each institution's responsibility to carry out its own assessments to use any tool for sharing information on cyber incidents.

employees and relevant external contacts, including regulators, considering current criteria and deadlines, where applicable.

3. The plan shall consider the threat scenarios identified in the risk assessment.
4. There should be criteria for classification of incidents by severity. These may require anything from simple redundancy of equipment for the continuity of services; creation of a structure for remote access, in cases of restrictions of physical access to the offices; or even the implementation of contingency facilities, whether physical or in the cloud, in more severe cases. Regarding these, the plan should also contemplate the return process to the original facilities after the end of the incident.
5. Attention should also be paid to security and access control issues in contingency facilities, whether physical or in the cloud, as well as secure configurations for cloud contingency services.
6. We recommend filing documentation related to incident management and to the incident response plan, to serve as evidence in any inquiries.

5 - Governance

Recommendations

1. A specific committee, forum or group should be created to address cyber security within the institution, with appropriate representation and governance.
2. The cyber security program should be periodically reviewed, keeping its risk assessments, protection deployments, incident response plans and environment monitoring up to date. It is recommended that the program review be conducted on an annual basis.
3. 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.
4. 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.
5. Initiatives such as the definition and maintenance of key performance indicators can strengthen the awareness and involvement of top management and other institutions.
6. 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.
7. 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.

8. It is recommended for the cybersecurity program to contain provisions for periodic training on information security. It must be periodically given to all employees, in addition to a special training plan for newly hired employees at the time of onboarding.
9. Training and awareness campaigns should be intensified for employees who work remotely and for employees who have been victims of a cyber incident.
10. Online services, such as instant messaging apps and sending direct messages over social media, can be used in an irregular attempt to extract information from employees. To avoid this situation, employees must be informed about what constitutes suspicious contact through online services and how to report it to the organization.

References

There is 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), out. 2015.

- Autoridade Nacional de Proteção de Dados (ANPD), *Comunicação de incidentes de segurança,* March 2021. Available at: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca/.

- Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA) - Grupo Técnico de Cibersegurança, *Referência técnica para configuração segura de ambiente em nuvem,* December 2017. Available at : https://www.anbima.com.br/data/files/50/F7/30/E0/D9C206101703E9F5A8A80AC2/Tecnica-para-nuvem-Referencia.pdf.

- Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA) - Grupo Técnico de Cibersegurança, *Modelos de diligência com terceiros - incluindo provedores de serviços em nuvem,* December 2017. Available at: https://www.anbima.com.br/data/files/84/B7/86/09/B9C206101703E9F5A8A80AC2/Modelo-de-Diligencia-com%20Terceiros-Referencia.pdf.

- Autorité des marchés financiers (AMF), *Stock Market Cybercrime - Definition, cases and perspectives,* February 2020. Available at: https://www.amf-france.org/sites/default/files/2020-02/study-stock-market-cybercrime-_-definition-cases-and-perspectives.pdf.

- Brasil, Lei 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados.* Available at: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

- Brasil, Bolsa e Balcão, *Programa de Qualificação Operacional,* January 2019. Available at: http://www.b3.com.br/pt_br/antigo/s_regul-antigo/programa-de-qualificacao-operacional-pqo/roteiros/.

- Comissão Parlamentar de Inquérito dos Crimes Cibernéticos, *Relatório final,* May 2016. Available at: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D>+RCP+10/2015.

- 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.

- Conselho Monetário Nacional (CMN), Resolução 4.893, de 26 de fevereiro de 2021, *que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.* Available at: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3 %A3o%20CMN&numero=4893.

- Cyber Security Agency of Singapore (CSA), *Guide to conducting Cybersecurity risk assessment for critical information infrastructure,* December 2019. Available at: https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/guide_to_conducting_cybersecurity_risk_assessment_for_cii.pdf.

- Cyber Security Agency of Singapore (CSA), *Singapore's Operation Technology Cybersecurity Masterplan 2019,* October 2019. Available at: https://www.csa.gov.sg/news/publications/ot-cybersecurity-masterplan.

- Department of The Treasury, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,* October 2020. Available at: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

- European Insurance and Occupational Pensions Authority (EIOPA), *Guidelines on outsourcing to cloud service providers,* February 2020. Available at: https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en.

- European Securities and Markets Authority (ESMA), *Guidelines on outsourcing to cloud service providers,* December 2020. Available at: https://www.esma.europa.eu/sites/default/files/library/esma50-157-2403_cloud_guidelines.pdf.

- European Systemic Risk Board (ESRB), *Systemic cyber risk,* February 2020. Available at: https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200219~61abad5f20.en.html.

- Federal Financial Institutions Examination Council's (FFIEC), *Cybersecurity Assessment Tool,* June 2015. Available at: https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017_All_Documents_Combined.pdf.

- Federal Reserve (FED), *Sound Practices to Strengthen Operational Resilience,* October 2020. Available at : https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201030a1.pdf.
- Financial Conduct Authority (FCA), *Cyber resilience,* October 2020. Available at: https://www.fca.org.uk/firms/cyber-resilience.
- Financial Conduct Authority (FCA), *Cyber Security - industry insights,* March 2019. Available at: https://www.fca.org.uk/publications/research/cyber-security-industry-insights.
- Financial Industry Regulatory Authority (FINRA), *Observations on Cybersecurity,* October 2019. Available at: https://www.finra.org/rules-guidance/guidance/reports/2019-report-exam-findings-and-observations/cybersecurity.
- Financial Industry Regulatory Authority (FINRA), *Report on Selected Cybersecurity Practices,* December 2018. Available at: https://www.finra.org/rules-guidance/guidance/reports/2018-cybersecurity-report.
- Financial Industry Regulatory Authority (FINRA), *Small Firm Cybersecurity Checklist,* June 2020. Available at: https://www.finra.org/compliance-tools/cybersecurity-checklist.
- Financial Stability Board (FSB), *Effective Practices for Cyber Incident Response and Recovery,* October 2020. Available at: https://www.fsb.org/wp-content/uploads/P191020-1.pdf.
- Global Financial Markets Association (GFMA), *Framework for the Regulatory Use of Penetration Testing in the Financial Services Industry,* April 2018. Available at:: https://www.gfma.org/correspondence/updated-gfma-framework-for-the-regulatory-use-of-penetration-testing-in-the-financial-services-industry/.
- Government Digital Service (Gov.UK), *Cyber security incentives & regulation review,* August 2020. Available at: https://www.gov.uk/government/publications/cyber-security-incentives-regulation-review-government-response-to-the-call-for-evidence.
- Hedge Fund Standards Board (HSFB), *Cybersecurity Toolbox for Hedge Funds Managers,* October 2015. Available at: http://www.sbai.org/wp-content/uploads/2016/04/Cybersecurity-HFSB-Toolbox.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,* April 2016. Available at: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf.

- National Cyber Security Centre (NCSC), *Guidance for organizations on enabling staff to use their own smartphones, tablets, laptops and desktop PCs to access work information,* Available at: https://www.ncsc.gov.uk/collection/mobile-device-guidance/bring-your-own-device.

- National Cyber Security Centre (NCSC), *Effective steps to cyber exercise creation,* February 2020. Available at: https://www.ncsc.gov.uk/guidance/effective-steps-to-cyber-exercise-creation.

- National Cyber Security Centre (NCSC), *10 steps to cyber security,* November 2018. Available at: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security.

- 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.

- New York State Department of Financial Services (DFS), *Cybersecurity Requirements for Financial Services Companies - 23 NYCRR Part 500,* December 2016. Available at: https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default).

- New York State Department of Financial Services (DFS), *Cybersecurity.* Available at: https://www.dfs.ny.gov/industry_guidance/cybersecurity.

- SANS Institute, *Securing the Human.* Available at: https://www.sans.org/security-resources/posters/securing-the-human.

- Securities Industry and Financial Markets Association (SIFMA), *Insider Threat Best Practices Guide,* February 2018. Available at: https://www.sifma.org/wp-content/uploads/2018/02/insider-threat-best-practices-guide.pdf.

- Securities Industry and Financial Markets Association (SIFMA), *Cybersecurity Resource Center.* Available at: https://www.sifma.org/resources/cybersecurity-resources/.

    - SIFMA, *Data Protection Principles,* January 2020;
    - 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), *Observations from Cybersecurity Examination,* August 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.