Baseline Principles for managing cyber security risk

In cooperation with the Centre for Cyber security Belgium.

This is a communication of the FSMA pursuant to Article 66 of the Law of 2 August 2002.

This document results from a fruitful cooperation with the Centre for Cyber security Belgium.

The FSMA has consulted, and gratefully acknowledges the input of, the National Bank of Belgium and various specialized industry representatives.

Foreword:

Cyber threats are a major operational risk that firms active in the financial sector face. They deserve every firm's full attention, since their clients, data regarding them as well as their reputation are their most valuable asset.

The FSMA wishes to raise awareness and provide guidance on the foundations of managing cyber risks in collaboration with the Centre for Cyber security Belgium (hereafter also "CCB"). This document contains Baseline Information and Cybersecurity Principles to assist all firms in the implementation of organizational and technical measures concerning Cyber security.

The words linked to "cyber" used in this document have the meaning given in the Cyber Lexicon of the Financial Stability Board.

The FSMA expects all firms under its supervision[1] to adopt the measures necessary to manage information security risk and more particularly cyber risk[2], taking into account the nature, scale and complexity of their business, including when they outsource activities. Such measures should be reassessed and updated regularly to incorporate the latest techniques and best practices.

The financial sector is diverse in terms of the size and legal structure of firms, varying from large firms to one-person operations. The FSMA acknowledges that the relevance and importance of the issues raised in this document will vary according to the business model, size and technological complexity of the firm. Therefore, the depth and scope of the topics addressed in this document are not exhaustive.

This document does not address the consequences, if any, of a data breach from a GDPR[3] perspective. All firms should perform their own analysis on a case-by-case basis.

---

1 ***This document does <u>not</u> address the cyber resilience of systemically important exchange or settlement platforms (which are expected to respect more stringent guidance and requirements), such as EURONEXT, and listed firms whose information is under the supervision of the FSMA.***

2 Most of the definitions included in this document are taken from the Cyber Lexicon published by the Financial Stability Board (12 November 2018) (hereafter, "the **Cyber Lexicon**"). The words linked to "cyber" used in this document have the meaning given in the Cyber Lexicon.

Cyber Risk is defined as "the combination of the probability of Cyber Incidents occurring and their impact".

Cyber Incidents are defined as "a Cyber event that either i) jeopardizes the Cyber Security of an Information System or the information the system processes, stores, or transmits; or ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not".

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Cyber security is an organizational challenge, not merely an IT problem.

Cyber security[4] has become an organizational challenge that every business manager must understand. It is a crucial element in any organizational strategy aimed at securing its essential resources (assets). Cyber security incidents can originate inside or outside the firm. The cause may be unforeseeable events, human error, as well as malicious intent (from inside or outside the firm).

Belgian insurance brokers specialized in this area estimate that internal risks (like human error) within firms represent 60 to 70% of security incidents like unwanted displays of data to unauthorized persons, sending emails with the wrong attachments, inadvertent publication of confidential databases, etc[5].

IT infrastructure may also be threatened by ordinary perils such as fire, flooding or lightning striking a firm's office, or the outsourcing of parts of a firm's IT to external suppliers that are unable to deliver the expected services or that have themselves been the victim of security or cyber incidents.

The sophistication of external cyber threats, on the other hand, continues to evolve. The financial sector has been one of the sectors most under attack[6]. Even robust cyber security measures can be compromised when, for example, an employee opens an email attachment that contains malware or downloads a malicious software on the firm's systems. Common attacks include phishing and spear phishing attacks[7], malware/ransomware[8] and fraudulent third-party wires that frequently involve use of email or stolen customer or financial advisor credentials.

---

4 **Cyber Security** is the "preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved".

5 Results from a round-table conference with specialized insurance brokers organized by the FSMA at its premises in May 2019.

6 According to the IBM X-factor 2018 data analysis, the finance and insurance sector has been the most frequently attacked industry for three years in a row. "Human "error" such as misconfigured servers, unsecured cloud databases and improperly secured (…) backups were responsible for 43% of publicly disclosed information incidents, resulting in a more than 20 % increase since last year.

7 **Phishing and spear phishing attacks**: Phishing is a broader term for any attempt to trick victims into sharing sensitive information such as passwords, usernames, and credit card details for malicious reasons. Unlike spear-phishing attacks, phishing attacks are not personalized to their victims, and are usually sent to masses of people at the same time (https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing).

8 **Malware**: software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems.

Ransomware is a type of malware used to extort a user by blocking its IT system against payment of a ransom (often in cryptocurrency).

Cyber security incidents, whatever their cause, can be very damaging, and can even put a firm out of business.

Not being able to deliver financial services due to a Cyber incident is harmful in the first place to the public, but to a firm's reputation and business alike and possibly to the financial sector's reputation.

Are firms obliged to do something?

All firms are legally required to conserve customer and transaction data.

Besides that, if a firm loses personal private data, it faces a potential liability for breach of privacy laws (GDPR)[9].

In the worst-case scenario, gross negligence in managing client data could potentially constitute a criminal wrongdoing. The firm's director or head of business may see his or her liability triggered and this can be a source of important financial claims and liabilities.

The FSMA reminds all firms under its supervision that they must comply with all the legal or regulatory requirements applicable to them concerning cyber security and cyber risk management as well as with all relevant requirements or documents defined at European or at international level, such as by the European Supervisory Authorities (ESMA, EIOPA, EBA) or by IOSCO.

This is certainly the case for **firms that are legally obliged at all times to maintain an adequate organization**. It includes having an appropriate cyber risk management strategy and framework that enables the firm, amongst other things, to ensure the preservation of essential data and functions, and the maintenance of services and activities, or, where that is not possible, the timely recovery of such data and functions and the timely resumption of their services and activities.

The FSMA expects boards and senior management of such firms to fully recognize their responsibilities in respect of cyber security risk and to put this high on their agenda. They should take appropriate and state-of-the art actions to improve their cyber resilience[10] and robustly address key issues such as alignment of IT and business strategy, outsourcing risk, change management and cyber security management.

Firms required by law to maintain an "adequate organization" must have appropriate organizational and technical measures, policies and procedures to ensure cyber security and resilience. Firms that outsource activities that are subject to cyber risk should ensure that the

[9] For the sake of clarity: this document does NOT address breaches of the GDPR Regulation.

[10] **Cyber Resilience** is "the ability of an organization to continue to carry out its mission by anticipating and adapting to Cyber Threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from Cyber Incidents".

service providers have in place the measures, policies and procedures needed to ensure cyber security and resilience of the data, services and activities.

Of course, strategies, frameworks and/or policies will have no benefit against cyber incidents such as computer viruses or cyber attacks if they are not put into practice. Such firms should therefore also develop procedures to respond to and recover from cyber threats and perform adequate testing based on scenarios that cover their core business. Such firms should regard this document as a useful, but not comprehensive source of inspiration.

Other firms (not required by law to maintain an adequate organization, i.e. for example most financial intermediaries) should also adopt measures that help to protect financial consumers' data and contribute to keeping the financial system and services robust and trustworthy for the public.

The FSMA encourages **all firms** to increase their awareness, organizational and technical measures concerning cyber security and to put the matter at the top of the management agenda. All firms need to make sure that they understand and effectively manage these risks.

This includes asking themselves questions for which they seek real solutions and thoroughly testing those solutions. By way of example, it is pointless to have bought a backup system for the firm's data when backing up the data is not working in practice.

This also includes clarifying the matter towards employees. Cyber security concerns all employees and is not a technical matter that concerns only the IT specialist.

Cyber Security management - 4 key principles

In establishing effective cyber security management, four principles are key:

1. Security strategy and support – Governance

- Require management involvement and support.
- Adopt an information security strategy (safety policy) geared to the organization's strategy.
- Set up a multi-annual plan for regular training and awareness-raising for all employees.
- Create a culture of information security and risk analysis for all new projects,
- Plan for major/severe security incidents and crises.
- Keep a register of major changes in the environment.
- Have a Cyber Incident Response Plan.

2. Asset identification and risk analysis - Identification

- Identify key information systems and data.
- Adopt a policy for categorizing sensitive information systems and data.
- Manage information security risks to set priorities.

3. Implementation of measures - Protect/Detect/Respond and Recover

- Implement specific (technical/organizational/process) measures to secure the information.
- Manage resources assigned to information security and infrastructure in an effective and efficient manner, including the appointment of information security officers.

4. Evaluation of security measures

- Conduct at least an annual review of the security measures to assess the status of the security plan.
- Measure the performance of actions taken but also the evolution of threats and vulnerabilities at regular intervals to ensure that the objectives are achieved (continuous improvement cycle).
- Consider refining the risk analysis and the control measures in the light of evaluations, audits, incidents and major changes that have/had an impact on the business activities.

1. Security strategy and support - Governance

Adequately managing Cyber risk is a business problem, much more than a technical IT issue. Effective governance starts with a clear and comprehensive Information security and Cyber resilience framework. Arrangements must therefore be put in place to establish, implement and review the firm's approach to managing Cyber risks.

The FSMA encourages **all firms** to have a **Cyber Incident Response Plan**[11] addressing in a comprehensive manner what measures to deploy to safeguard data and resume the business when an incident occurs.

The FSMA is of the opinion that having such a plan is indispensable for firms that are under a legal obligation to demonstrate at all times an adequate organization.

Such a Cyber Incident Response Plan should prioritize services to customers and provide for all necessary measures to enable the firm to resume operations rapidly, safely and with

[11] **Cyber Incident Response Plan**: the documentation of a predetermined set of instructions or procedures to respond to and limit consequences of a cyber incident.

accurate data. Ideally, the Plan is built around the most common disaster scenarios and around what needs most protection. It should also address communication quickly and adequately to all relevant stakeholders such as, but not limited to, the judicial authorities, the **Cyber Incident Response Teams**[12], and - if and when actionable - the Data Protection Authority, the firm's customers, etc. Such a Plan could include support from external partners.

Firms with effective cyber security programs typically require employees to participate in regular, generic and role-specific cybersecurity training and testing, for example through phishing email exercises.

Even if a firm has in place good practices, the firm's branch office or geographically dispersed sales offices deserve attention, since they may be struggling more than their head office in managing passwords, implementing patches[13] and software updates, updating anti-virus software, tracking removable storage devices (e.g. USB sticks), encrypting data and reporting incidents.

All points of sale should be trained to deal with cyber incidents affecting the firm's business: clients will put questions to the firm's sales staff and not to the IT staff (who will be busy anyway dealing with the technical problem).

2. Asset identification and risk analysis - Identification

Firms identify which of their critical operations and supporting information assets should, in order of priority, be protected against compromise. Drawing up an inventory is thus a first necessary and important step: what is worth protection as most vital asset or process? What data are the most sensitive?

Firms with effective Information/cyber security programs typically establish strong governance structures and processes (scaled to the firm) that address cyber security in a risk management context. They escalate risk acceptance decisions and problems to the appropriate levels for resolution and inform them of future program developments.

Measures these firms implement may include regular risk assessments with detailed, time-bound follow-up action plans to resolve higher-risk concerns. Firms with effective cyber

[12] **Cyber Incident Response team**: team of appropriately skilled and trusted members of the organization that handles incidents during their life cycle.

[13] **Patch management**: the systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes and service packs.

security programs typically support their risk assessments with regular vulnerability and IT penetration tests[14].

All firms should bear in mind that proportionality is key in implementing cyber security processes and procedures, and must take into account their own risk profile - keeping in mind that the staff number is neither the only, nor the most relevant risk profile indicator.

3. Implementation of measures - Protect/Detect/Respond and Recover

All firms should take adequate measures to secure their clients and transaction data against external and internal breach. Clear allocation of responsibilities within the firm thereby helps to bridge the gap between theory and practice. Early detection of breaches will enable the firms to respond swiftly and take countermeasures against a potential breach and even to contain an actual breach.

As appropriate to their scale, some firms implement security information and event management, "system usage behavior" analytics and data loss prevention tools to identify, monitor, and address potentially anomalous or suspicious activity on their networks.

Firms largely depend on IT service providers for hard and software. Having a formal process to review a prospective vendor's cyber security preparedness or to ensure new vendors have appropriate protections in place is a good practice.

For example, a firm's contract with vendors should address key questions such as the external supplier's responsibilities regarding notification to the firm in the event of a breach of customer or firm data. If the cyber security services are provided to several linked firms, the cyber security responsibilities should be sufficiently documented to the benefit of all firms, such as in a service-level agreement.

4. Evaluation of security measures

All firms should re-evaluate their security measures at least annually by measuring the performance of actions taken. Close monitoring and regular monitoring of threats and vulnerabilities are needed.

All firms should stay alert with respect to the quick evolution of threats and vulnerabilities and regularly question if the implemented measures are up to date and sufficient to meet the firm's aim and risk appetite.

Firms with an effective Cyber Incident Response Plan adopt a **continuous improvement cycle** consisting in refining the risk analysis and the control measures in the light of evaluations,

[14] **Penetration testing**: a test methodology in which assessors, using all available documentation (e.g. system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.

audits, incidents and major changes that have/had an impact on the business activities at least on a yearly basis.

What if a firm is small?

Small firms that struggle to develop a cyber risk management strategy and framework may find a good call to action in using the **Cyber Security Reference Guide,** accessible online and published by the **Centre for Cyber security Belgium** (https://cyberguide.ccb.belgium.be).

As a first step to analyzing the situation with regard to Cyber security, a small firm may wish to ask oneself the **Key Questions** attached to this document[15].

In case a smaller firm has difficulty seeing this through, it should apply for outside help by contacting consultants or specialized firms, rather than wait until harm has occurred.

Insurance companies, from whom firms might seek insurance coverage, might also help a firm by conducting a preventive screening of its cyber resilience in order to assess the firm's risk.

Sharing information

The FSMA encourages all firms to share their experience with their peers, e.g. through the web contact page of the **Cyber Security Coalition**[16] and their professional organization, since this helps to protect the financial sector and, in turn, to keep the public confident in the sector's ability to safeguard its financial interests.

The **Law of 7 April 2019**[17] requires operators of trading venues that qualify as operators of essential services to report significant incidents both to the National Computer Security Incident Response Team (or CSIRT)[18] and to the FSMA. Financial firms that have been identified as operators of essential services, other than operators of trading venues, report significant incidents to the National Bank of Belgium, which will in turn notify the CSIRT[19].

Some useful references:

The Centre for Cyber security Belgium has published a **Cyber Security Reference Guide** accessible online (https://cyberguide.ccb.belgium.be). It contains actionable advice categorized as basic or advanced measures.

Firms can find more elaborate guidance (as updated from time to time) in the following documents (such firms should take into account the principle of proportionality and the legal

---

15 These questions are extracted from the Final Report of the OICV-IOSCO Cyber Task Force (FR09/2019, June 2019) (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf).

16 www.cybersecuritycoalition.be

17 Belgian Official Gazette, 3 May 2019

18 At the date of publication of this document, the CSIRT is to be created by a future royal decree.

19 See Article 26 of the Law of 7 April 2019.

status of the firm as well as the impact of its operations on financial consumers and/or financial stability):

1. The reports, guidelines, recommendations, etc., published by international bodies (such as IOSCO or the OECD), by the European Supervisory Authorities (ESMA, EIOPA, EBA), by Central Banks or National Competent Authorities (such as the National Bank of Belgium) or by institutions having expertise in cyber security (such as the Swift Institute).

See for example the CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures (www.bis.org/cpmi/publ/d146.pdf), as well as the final report of the Cyber Task Report (June 2019) (https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf), the NIST (National Institute of Standards and Technology) Framework for Improving Critical Infrastructure Cybersecurity (https://www.nist.gov/cyberframework) and the toolkit published in July 2019 by the Swift Institute (Cyber Resilience and Financial Organizations: A Capacity-building Tool Box - https://swiftinstitute.org/research/securing-the-long-tail-of-financial-services-toolkit/).

2. The **Law of 7 April 2019** establishing a security framework of networks and information systems of general interest for public security implements, in Belgium, the European Directive on security of network and information systems (the "NIS Directive)[20], as far as sharing of information and reporting of incidents is concerned[21].

3. The **27000 family of standards on information security management systems** published from time to time by the International Organization for Standardisation (ISO) and the International Electrotechnical Commission (IEC). (See, for example, ISO, "ISO/IEC 27000:2018", February 2018, https://www.iso.org/standard/73906.html).

---

[20] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for high common level of security of network and information systems across the European Union (**NIS Directive**): https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive. The NIS Directive provides legal measures to boost the overall level of cybersecurity in the European Union by ensuring:

- Member States' preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority,
- cooperation among all the Member States, by setting up a cooperation group in order to support and facilitate strategic cooperation and the exchange of information among Member States. They will also need to set up a CSIRT Network, in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks,
- a culture of security across sectors which are vital for our economy and society and rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, health care and digital infrastructure. Businesses in these sectors that are identified by the Member States as operators of essential services will have to take appropriate security measures and notify serious incidents to the relevant national authority. Key digital service providers (search engines, cloud computing services and online marketplaces) will also have to comply with the security and notification requirements under the new Directive.

[21] See Article 4, § 3 of the Law of 7 April 2019.

4. The regularly updated information on cybercrime of the **EU Computer Emergency Response Team** (or CERT-EU for short) (https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html).

5. The documents and information published by the **Centre for Cyber security Belgium** (https://www.ccb.belgium.be/en) and the **Belgian Cyber Security Coalition** (https://www.cybersecuritycoalition.be).

6. The **G-7** fundamental elements of cybersecurity for the financial sector (https://fin.gc.ca/activty/G7/pdf/G7-cyber-risk-management-gestion-risques-cybernetiques-eng.pdf) and the G-7 Fundamental Elements for Threat-Led Penetration Testing (https://www.fin.gc.ca/activty/G7/pdf/G7-penetration-testing-tests-penetration-eng.pdf).

Terminology

There is limited standardization of terms regarding cyber and hence alternative definitions can be found in different sources.

Most of the definitions included in this document find their source in the **Cyber Lexicon** published by the **Financial Stability Board** dated 12 November 2018 ; likewise, all words used and linked to "cyber" in this document have the meaning given in the Cyber Lexicon unless expressly stated otherwise (https://www.fsb.org/2018/11/cyber-lexicon).

The principal terms used in this document:

Cyber Risk	the combination of the probability of Cyber Incidents occurring and their impact
Cyber Incidents	are defined as "a Cyber event that either i) jeopardizes the Cyber Security of an Information System or the information the system processes, stores, or transmits; or ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not
Cyber Incidence Response Plan	The documentation of a predetermined set of instructions or procedures to respond to and limit consequences of a cyber incident.
Incidence Response Team	A team of appropriately skilled and trusted members of the organization that handles incidents during their life cycle.
Cyber Resilience	The ability of an organization to continue to carry out its mission by anticipating and adapting to Cyber Threats and other relevant changes in the environment and by

	withstanding, containing and rapidly recovering from Cyber Incidents.
Cyber Incident Response Team	Team of appropriately skilled and trusted members of the organization that handles incidents during their life cycle.
Ransomware or Malware	Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems.
Patch management	The systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes and service packs.
Penetration testing	A test methodology in which assessors, using all available documentation (e.g. system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.

KEY QUESTIONS

Source: Cyber Task Force Final Report OICV-IOSCO June 2019
(https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf)

As a first step toward analyzing its situation with regard to cyber security, a firm may wish to ask itself the following questions:

A. INDUSTRY STANDARD FRAMEWORK:

1. *Does the organization use an industry standard to develop a Cyber Risk management strategy and framework (e.g., ISO, NIST Cyber Security Framework, and/or others)? Please identify the standard(s).*

B. IDENTIFY AND PROTECT:

2. *Does the organization maintain an inventory of its software, hardware, applications, and vendors?*
3. *Does the organization identify Cyber Risks and Vulnerabilities that may impact business operations?*
4. *Does the organization have an Identify and access management program designed to limit access to and remove access from its users in a timely manner?*

5. *Does the organization have a Security Awareness and Training Program that allows for individuals to understand their roles within Cyber Security and learn more about emerging threats?*
6. *Does the organization employ a Patch Management program to address known software vulnerabilities? Does the organization employ hardware (e.g., firewalls, network intrusion detection systems) and software (e.g., anti-malware, host intrusion detection systems) to protect its information systems?*
7. *Does the organization have written procedures to ensure that backups of information are conducted, maintained, and tested periodically?*

C. DETECT:

8. *Does the organization detect and analyze potential Cyber Events to understand the nature, scope and methods of a Threat Actor?*
9. *Does the organization implement email protection mechanisms to automatically scan, detect, and block malware or malicious links in email?*
10. *Does the organization have a testing program to validate the effectiveness of the organization's incident detection processes and controls?*

D. RESPOND/RECOVER:

11. *Does the organization have an incident response plan to contain Cyber Incidents and applications and processes to ensure the alert and activation of the plan?*
12. *Does the organization's incident response plan address information sharing, including managing vulnerability disclosures and other communication, and reporting about Cyber Incidents to internal and external stakeholders, third parties, regulators, and law enforcement, as appropriate?*
13. *Does the organization test its incident response plan regularly and update it as needed based on Cyber Incidents that have occurred and on Threat Intelligence?*
14. *Does the organization have a recovery plan to ensure timely recovery from Cyber Incidents?*
15. *Does the organization periodically review and update your recovery plan?*