Cybersecurity Policy

16.Dec.2020

Versions Index

16.Dec.2020
Initial version

DISCLAIMER

The English language text below is not an official translation and is provided for information purposes only. The original text of this document is in the Portuguese language (available in www.omip.eu). In the event of any discrepancies between the English translation and the Portuguese original, the Portuguese original shall prevail. Whilst every effort has been made to provide an accurate translation we are not liable for the proper and complete translation of the Portuguese original and we do not accept any liability for the use of, or reliance on, the English translation or for any errors or misunderstandings that may derive from the translation.

This document is available in www.omip.eu

Introduction

Cybersecurity is defined as the protection of confidentiality, integrity and availability of information in cyberspace, that is, the non-physical space created by computer networks, in particular by the Internet, where people can communicate and interact via softwares, platforms or other information services.

As Regulated Market as defined in article 4 (1) of Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 (MIFID II), the constant concern of OMIP is to be equipped with a number of cybersecurity management tools in order to ensure that its assets and information systems conform to international standards, references and norms, in particular:

- ISO/IEC 27032:2012;
- National Reference Framework for Cybersecurity, National Cybersecurity Centre (CNCS);
- Framework for Improving Critical Infrastructure Cybersecurity (v1.1, April 16, 2018), NIST.

and also to legal requirements, in particular Law 46/2018 (of 13 August), establishing the legal framework for cyberspace security (transposing Directive (EU) 2016/1148, of the European Parliament and of the Council, of 6 July 2016). Specifically, being a Regulated Market and pursuant to Article 29(1) of Law 46/2018, OMIP is identified by the CNCS as an Essential Service Operator in the financial market infrastructure sector (updated annually upon notification by the CNCS).

With this in mind, OMIP establishes through this Cybersecurity Policy the principles of its cybersecurity management organisation, aiming to achieve the following macro objectives: Identification, Protection, Detection, Response, Recovery, Tests, Cooperation and Information Sharing, and Continuous Improvement.

1. Scope

This policy applies to employees, trainees, service providers and other OMIP partners, and to all its technological assets in operation or inactive.

All of the OMIP areas of operation that have an impact on cybersecurity are included in the policy scope.

2. Objectives

To ensure cybersecurity, OMIP ensures the following objectives:

a) Identification
   i. Ensure compliance with applicable laws, regulations and other standards;
   ii. Comply with the requirements of confidentiality, integrity and availability appropriate to the OMIP's business objectives, in particular to the needs of its members and legal and regulatory requirements;
   iii. Identify and classify information assets according to their relevance and criticality, such that they may be adequately protected throughout their life cycle;
   iv. Ensure that suppliers and service providers meet OMIP's cybersecurity needs and requirements;
   v. Identify, evaluate and deal with the cybersecurity risks inherent to OMIP's activity and to which assets are exposed;
   vi. Establish a risk management strategy according to the organisation's risk tolerance;

vii. Implement security controls and mechanisms that aim to mitigate or limit potential damages caused by the misuse of asset vulnerabilities, in order to minimise information security incidents and ensure a level of security appropriate to the risk that OMIP is willing to undertake.

b) Protection
   i. Establish and implement controls to protect OMIP's information assets from theft, intrusion, abuse or other unlawful forms of processing;
   ii. Ensure that the equipment, infrastructures and systems that support OMIP's activity are available and reliable;
   iii. Promote a culture of awareness and commitment to cybersecurity among the members of the Board of Directors, Senior Management and Employees, motivating them to become aware and take responsibility for their intervention in order to minimise the risks of information security incidents;
   iv. Ensure the protection of personal data in accordance with the applicable legislation.

c) Detection
   i. Monitor cybersecurity anomalies and events in a timely manner, and understand the potential impact of such events;
   ii. Continuously monitor networks and information systems to identify cybersecurity events and check the effectiveness of the protection measures in place;
   iii. Implement and maintain anomalous event detection processes.

d) Response
   i. Identify, contain and resolve information security incidents and, in particular, cyber attacks;
   ii. Reduce damages to the business related to information security incidents, and minimise their impact on OMIP's stakeholders (internal and external);
   iii. Ensure that information security incidents are reported in accordance with the legislation in force and with the internal procedures defined to that end.

e) Recovery
   i. Ensure that OMIP can continue to provide its services, in particular its critical business functions, in case of serious information security incidents or cyber attacks, under the conditions laid down in the applicable regulations, norms and specific procedures;
   ii. Ensure redundancy of equipment, infrastructures and information systems that support critical business functions, thus avoiding single points of failure (SPOFs);
   iii. Minimise the negative impacts that may arise from serious security incidents, both for the reputation of the organisation and for all OMIP stakeholders.

f) Tests
   i. Assess the effectiveness of controls implemented at to mitigate the risks identified;
   ii. Ensure the maintenance of integrity, availability and confidentiality of OMIP's information systems;
   iii. Identify and mitigate vulnerabilities in OMIP's infrastructure;
   iv. Assess effectiveness and identify points of failure and potential improvements in procedures and information security incidents response and recovery plans.

g) Cooperation and information sharing

i. Promote the sharing of relevant information on cybersecurity through secure channels in a timely manner, with OMIP's and OMI Group's stakeholders and other interest groups;
ii. Contribute to the widespread awareness of cybersecurity

h) Continuous Improvement
i. Update OMIP's procedure, policies, plans and processes in the light of the updating of industry best practices and international references and norms on cybersecurity;
ii. Promote strategies to implement opportunities for improvement, including proposals resulting from audits, intrusion tests or other internal or extern cybersecurity projects;
iii. Define indicators that support cybersecurity reporting models to be presented internally to the Cybersecurity Committee and, where applicable, to other company bodies.

3. Roles and Responsibilities

3.1 Board of Directors

OMIP's Board of Directors is ultimately responsible for general cybersecurity and, in particular, for defining and reviewing this policy, in order to ensure that it is adequate and effective at all times.

3.2 Senior Management

OMIP's senior management, comprising the Chairman and Vice-chairman and the Chief Operating Officer, is responsible for supporting all measures to implement and maintain cybersecurity strategies, ensuring adequate resources to guarantee the achievement of the objectives defined in this policy.

3.3 Cybersecurity Committee

The Cybersecurity Committee of the OMI Group is an internal technical committee composed at least by the Chief Operating Officers of OMIP and OMIClear and by the Information Systems Manager of OMIE.

The Cybersecurity Committee is responsible for defining cybersecurity strategies and guidelines, promoting synergies in the implementation, compliance and monitoring of those strategies and requirements in the various companies and in the different areas of Administration, Protection, Surveillance and Resilience.

The Cybersecurity Committee shall inform the Chairman, Vice-Chairman and, if applicable, the remaining members of the respective Boards of Directors of all the relevant matters concerning cybersecurity.

3.4 Employees

OMIP's employees shall clearly understand the cybersecurity risks to which they are exposed in the performance of their duties, as well as their roles and responsibilities in mitigating those risks and the consequent protection of OMIP's assets.

In particular, OMIP's employees are responsible for:

- Complying with all cybersecurity-related norms, codes, policies and procedures;
- Information assets entrusted to them, and shall contribute proactively to properly protecting them.

3.5 Suppliers, service providers and other external entities

Suppliers, service providers and other external entities shall adopt the conduct and procedures consistent with this policy. In particular, the contracts between OMIP and the service providing companies with access to its information systems and/or technological environment shall contain security clauses and requirements that guarantee confidentiality between the parties and ensure that the professionals under their responsibility comply with this policy, with the norms, codes and other applicable procedures.

Suppliers and other external entities are also responsible for reporting to OMIP any incidents related to information security or in OMIP's information systems.

4. Cybersecurity objectives at OMIP

4.1 Identification

4.1.1 Asset Management

The assets relevant to the organisation include the information managed by OMIP, its processes and support infrastructures, employees, third parties, equipment, documents, systems, applications and networks. They are, therefore, identified accordingly, inventoried and classified according to their importance and criticality, such that they may be adequately protected throughout their life cycle (which includes their creation, handling, storage, transport and destruction).

4.1.2 Supplier and service provider management

When contracting suppliers and service providers, OMIP follows a standard procedure, which includes surveying several entities that are recognised as competent and having adequate technical knowledge for the provision of services or supply of the products.

Due to the small number of OMIP suppliers and service providers, their performance is continuously monitored. Assessment of compliance with the agreed service levels and security and cybersecurity requirements is evaluated regularly and in accordance with contracts.

4.1.3 Risk Management

One of the core areas of Information Security and Business Continuity at OMIP is continuous management – identification, assessment and treatment – of information security risks inherent to its activity and to which the organisation's assets are exposed, thus constituting a company management tool.

OMIP's risk management methodology involves:

- identification and documentation of internal and external threats that may misuse the vulnerabilities of OMIP's assets, jeopardising their integrity, confidentiality or availability;
- assessment based on risk scenarios that make up the risk level, assessing their likelihood and impact;

- risk treatment, prioritised according to the risk level defined, asset criticality, and tolerance to the organisation's risk.

As regards treatment, risk management includes the implementation of security controls and mechanisms that aim to mitigate or limit potential damages caused by the misuse of asset vulnerabilities, in order to minimise information security incidents and ensure a level of security appropriate to the risk that OMIP can undertake. These measures are defined according to the business objectives and OMIP's responsibilities, taking into account their efficiency, cost and applicability.

OMIP's risk management also includes monitoring the operational risks to which OMIP is exposed by establishing procedures for assessing the level of exposure and risk limit considered acceptable in view of the organisation's objectives, in accordance with the Operational Risk Policy.

4.2 Protection

4.2.1 Access Control

The identities and rights to access OMIP's networks and information systems are issued, managed, checked, reviewed, revoked and audited according to the principles of least privilege, of minimum functionality, and of segregation of functions. These principles apply across internal accesses (of employees), external accesses (of suppliers, service providers or clients), and remote accesses (internal or external).

The authentication mechanisms in OMIP's networks and information systems are defined and maintained according to their characteristics and access profiles, in order to maintain the integrity and confidentiality of information.

4.2.2 Data and communications security

OMIP's networks and information systems shall protect the security (confidentiality, integrity and availability) of stored data, data in circulation, data in use, and information transfer flows. To this end, OMIP has implemented controls for:

- Classification, handling and destruction of information;
- Encryption;
- Data exfiltration prevention (commonly known as DLP - Data Loss Prevention);
- Secure development and restriction of software use;
- Prevention and detection of malicious activity.

4.2.3 Human Resources

OMIP promotes training and awareness activities on Information Security and transmits the necessary information so that senior management and their employees are prepared to take on their cybersecurity responsibilities. OMIP then validates the success and effectiveness of these activities through campaigns such as, for example, simulation of events.

Before taking up their duties, the employees of departments with privileged access to OMIP's networks and information systems also have specific training on access management and other operational procedures. Employees with further responsibilities in OMIP's cybersecurity also receive special training on Information Security.

4.3 Detection

OMIP and other OMI Group companies use specialised external services providers in cybersecurity for the management of network events (logs) and for the periodic assessment of vulnerabilities in information systems, namely through the use of automatic processes for detection, identification, cataloguing and monitoring of malicious activity. The results and vulnerabilities identified are then incorporated in OMIP's internal action plan in order to be examined under risk management.

4.4 Response

OMIP's response to incidents is systematised into incident and, in particular, cyber-attack management procedures, which define the tasks of identification, classification, technical intervention, registration and treatment that must be done after an incident is detected. Thus, OMIP aims to ensure a prompt and effective response to minimise potential damages to the business in terms of confidentiality, integrity and availability of information systems.

These procedures, alongside other communication and reporting procedures across all areas of the organisation, also define the communications plan for OMIP's stakeholders (internal and external), in particular relevant contents that must be shared and the appropriate channels, with the purpose of identifying, containing and resolving the incident, and also to minimise its impact on the stakeholders.

4.5 Recovery

4.5.1 Backup copies

OMIP performs backup copies of critical information stored in its information systems, keeping them in an alternative location, where possible, and ensuring the confidentiality thereof. OMIP also ensures the integrity and availability of the backup copies, putting in place procedures for their effective recovery if needed, and within the recovery time objective. These procedures are tested regularly in order to validate their adequacy and the integrity and availability of the copies made.

4.5.2 Business Continuity Plan and Activity Recovery Plans

The availability of information, of systems and of the infrastructure is ensured by the implementation of management procedures and recovery plans of information security incidents or cyber attacks. If such incidents occur, OMIP will be able to continue to provide its services, in particular its critical business functions, appropriately and as per the terms defined in the applicable regulations, norms and specific procedures, thus minimising the negative impacts they may have for the organisation's reputation and for all OMIP's stakeholders.

As regards infrastructure redundancy, OMIP's secondary data processing centre (Datacenter) is situated in a different location (with a distinct geographical risk profile) synchronised in real time with the main Datacenter so as to minimise OMIP's business disruption time.

4.6 Tests

As regards risk management, OMIP carries out tests to assess the effectiveness of controls implemented to mitigate the risks identified. Moreover, whenever OMIP's infrastructure is updated either through the integration of a new information system or due to a significant change in an existing system, a security test plan is put into place to ensure that information integrity, availability and confidentiality of information is maintained.

OMIP also carries out periodic tests of its incident and cyber-attack management procedures and of its business continuity and Datacenter recovery, based on plausible scenarios, with the aim of assessing their effectiveness and identifying points of failure and potential improvements.

4.7 Cooperation and information sharing

Relevant information on cybersecurity is shared with OMIP's stakeholders and also with the OMI Group's Cybersecurity Committee.

OMIP also collaborates with the National Cybersecurity Centre, through a shared cooperation protocol by which commitment indicators, good practices, risk indicators and experiences on threats, vulnerabilities and cyber attacks are shared through secure channels and in real time.

Additionally, OMIP collaborates with other interest groups, associations and industry organisations, in order to achieve a more comprehensive awareness of cybersecurity

4.8 Continuous Improvements

OMIP is aware not only of its dynamic situation, in terms of business processes, assets and human resources, but also of the constant developments in cyber threats and misuse of new vulnerabilities. Moreover, as cybersecurity is a cross-cutting issue in all of the organisation's activities, its continuous improvement is one of OMIP's objectives.

In this sense, OMIP updates its procedures, policies, plans and processes in the light of the latest industry's good practices and of international cybersecurity references and standards. In addition, such a review encompasses the opportunities for improvement proposed by audits, intrusion tests or other internal or external cybersecurity projects, as well as the lessons learned during the response and recovery from information security incidents.

In order to monitor continuous improvement, OMIP has access to a number of indicators that support cybersecurity reporting models, which could be presented internally to the Cybersecurity Committee and, when applicable, to other company bodies.

5. Final Provisions

This policy shall be reviewed by the Board of Directors whenever there is a change in cybersecurity, in the internal organisation of OMIP, in the legal and regulatory framework, or in the best practices of the industry.

This policy is available for consultation on the corporate website.

Approved by the Board of Directors on 16 December 2020