Cybersecurity Incidents:

Management & Reporting Framework

Jaime Calvo Alfonsin

Index

1. *What is cybersecurity all about?*
2. *Incident Management and Reporting Framework*

a. *International*

b. *Europe*

c. *Spain*

d. *Upcoming regulations*

1. What is cybersecurity all about?

Cybersecurity = Security of network and information systems

The NIS directive states that it means the ability of network and information systems **to resist**, at a given level of confidence, **any action** that **compromises** the **availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems.**

But… Whats is meant by networks and information systems for the purposes of the NIS directive?

An electronic communications network.

Any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data.

Digital data stored, processed, retrieved or transmitted by elements covered under previously points for the purposes of their operation, use, protection and maintenance.

2. Incident Management and Reporting Framework

INTERNATIONAL

USA	Deparment of Treasury's Office of Foreign Assets Control (OFAC) SEC rule 30 NYDFS Cybersecurity Regulation
UK	The Network and Information Systems Regulations 2018 (NIS Regulations)[1]
CHINA	China Cybersecurity Law (CSL)[1]
BRAZIL	National Cybersecurity Strategy Brazil

EU

Network and Information Systems Directive (NIS) 2016/114
Payment Services Directive (PSD2) 2015/2366
General Data Protection Regulation (GDPR)
EBA Outsourcing
EBA ICT risk
NIS 2 Directive[2]
Digital Operational Resilience Act (DORA)[2]

Spain

Royal-Decree 12/2018
Royal-Decree 43/2021

1. Under review. Consultation launched on January 2022.
2. Not yet in force. Regulation expected to be published during 2022.

a. International (1/1)

United States

Department of the Treasury's Office of Foreign Assets Control (OFAC)

On September 2021, OFAC updated its published advisory on **potential sanctions risk for facilitating ransomware payments** released due to a significant increase on ransom attacks *(e.g Cryptolocker on 2013 or WannaCry 2.0 in 2017 which spread to at least 150 countries)* raising awareness on potential penalties and considerations when involved on the payment of ransomware.

Civil penalties on U.S persons (*or non-US when causing U.S person to violate IEEPA-sanction*) **when enganging in transactions**, directly or indirectly, with OFAC's **Specially Designated Nationals and Blocked Persons List**, other blocked persons or those covered by comprehensive country or region embargoes (*e.g. Cuba or Iran*), **even if such person did not know or have reason to know that it was engaging in a prohibited transaction**

Mitigation of OFAC's enforcement of U.S sanctions violation based on:

a. Implementation **risk-based compliance programs** to mitigate exposure to sanctions-related violations by companies (such as finantial institutions or those involved with victims of ransomwares) and adoption of cybersecurity practices.

b. Full cooperation with law enforcement, OFAC or other relevant agencies (this cooperation would include self-initiated, appropriate, and timely reports and ongoing updates after attack).

b. Europe (1/5) NIS Directive (2016/114)

Objective (NIS, Art. 1)

This Directive lays down ***measures*** *with a view* ***to achieving a high common level of security of network and information systems within the Union*** *so as to improve the functioning of the internal market.*

It sets out: *(a) obligations for all* ***MS to adopt a national strategy on the security of network and information systems****; (b) creates a* ***Cooperation Group*** *in order to support and facilitate strategic cooperation and the exchange of information among MS and to develop trust and confidence amongst them; (c)* ***creates CSIRTs network to contribute to the development of trust and confidence between MS*** *and* ***promote swift and effective operational cooperation****; (d)* ***establishes security and notification requirements for operators of essential services and for digital service providers;*** *(e) obligations for MS to* ***designate national competent authorities****,* ***single points of contact and CSIRTs***

Subjects (NIS, Arts. 4,5 and Technical Regulations Information System Directive, Art. 1.1)

Operators of Essential Services (OES) are identified by MS based on the provision of essential services for the maintenance of critical societal and/or economic activities which are dependant on network and information systems where an incident would have significant disruptive effects on such service.

Digital Service Provider (DSP) legal person that provides a digital service, defined by as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

b. Europe (1/5) NIS Directive (2016/114)

Cybersecurity incident (Art. 4)	*Any event having an actual adverse effect on the security of network and information systems.*
Incident Reporting (NIS 15,16)	**What to notify?** ***OES and DSP shall notify the competent authority or CSIRT of incidents having a significant impact*** *on the continuity of the essential services they provide.* ***Significant impact woud be determined by*** *(a) number of users affected by disruption essential service; (b) incident duration (c) the geographical spread (d) the extent of the disruption of the functioning of the service*; (e) the extent of the impact on economic and societal activities*.* **When?** OES and DSP shall notify, without undue delay **Who?** Operators of essential services and digital service providers **To whom?** CSIRT or competent authority as determine by member states (in Spain determined by RD 43/2021, see slide 14)

** Digital Service providers.*

b. Europe (2/5) PSD2

Subject matter (PSD2,Art.1)

Sets out rules in accordance with which Member States **shall distinguish between the following categories of payment service provider:** credit institutions, electronic money institutions, post office giro institutions which are entitled under national law to provide payment services, payment institutions, ECB and national central banks when not acting in their capacity as monetary authority or other public authorities and Member States or their regional or local authorities when not acting in their capacity as public authorities. It also includes **transparency of conditions and information requirements of payment services** and develops the **rights and obligations of payment service users and payment service providers.**

Scope (PSD2, Art.2)

This Directive applies to payment services provided within the Union.

Incident reporting (PSD2, Art. 96. RD19/2018 Art. 67)

When to notify? In the case of a major operational or security incident, without undue delay.

Who must notify? Payment service providers.

To whom? To the competent authority of the home Member State. In Spain providers would notify *Banco de España* (Art. 67 RD19/2018, of 23 November, on payment services and other urgent measures in financial matters).

*The **competent authority** of the home Member State shall, without undue delay, provide the relevant **details of the incident** to **EBA and to the ECB which** shall in cooperation with the competent authority of the home Member State, assess the relevance of the incident to other relevant Union and national authorities and shall notify them accordingly. The **ECB shall notify the members of the European System of Central Banks on issues relevant to the payment system**. On the basis of that notification, the competent authorities shall, where appropriate, take all of the necessary measures to protect the immediate safety of the financial system.*

b. Europe (3/5) GDPR

Subject-matter and objectives (GDPR, Art 1)

This Regulation lays down rules relating ***to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.*** *It protects* ***fundamental rights and freedoms of natural persons*** *and their right to the protection of personal data.*
Free movement of personal data within the Union shall be neither restricted nor prohibited *for reasons connected with the protection of natural persons with regard to the processing of personal data.*

Material Scope (GDPR, Art 2)

This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Persona data breach notification (GDPR, Art.3. AEPD Guidance)

What is a data personal breach? *Any breach of security leading to the accidental or unlawful destruction, loss or alteration of, or unauthorised disclosure of or access to, personal data transmitted, stored or otherwise processed.*

A security incident that has not affected personal data or processing of personal data is not a personal data breach, as it could not result in harm to the rights and freedoms of the natural persons whose data are the subject of the processing.

When to notify? Without delay and at the latest within 72 hours.
What to notify? About the processing and the person responsible / Intentionality and origin / Typology, categories of data and profile of data subjects / Consequences / Breach Summary / Cross-border implications / Temporary information and means of detection / Preventive security measures / Actions taken and communication to those affected.
Who must notify? The data processor. In the case of large companies, this may be the data protection officer.
To whom? In Spain, in general, in the private sphere, controllers affected by the breach must notify the Spanish Data Protection Agency.

b. Europe (4/5) EBA Guidelines Outsourcing

Objective

These guidelines aim to establish *a* ***more harmonised framework for the outsourcing arrangements of financial institutions*** *(scope of application of these guidelines covers credit institutions,investment firms subject to CRD, payment and electronic money institutions. It* ***sets out which arrangements with third parties are to be considered as outsourcing and provide criteria for the identification of critical or important functions that have a strong impact on the financial institution's risk profile or on its internal control framework*** *(where stricter requirements will apply).*

Due to high volumen of cybersecurity risk originating from external providers, these guidelines highlighting the relevance on the performance of appropiate security assesment of such providers

When carrying out the risk assessment prior to outsourcing and during ongoing monitoring of the service provider's performance, institutions and payment institutions ***should, at least: e. define and decide on an appropriate level of protection of data confidentiality, of continuity of the activities outsourced and of the integrity and traceability of data and systems*** *in the context of the intended outsourcing.* ***[Section 12.2, Point 68]***

Institutions and payment institutions ***should ensure that service providers, where relevant, comply with appropriate IT security standards.*** *Where relevant (e.g. in the context of cloud or other ICT outsourcing), institutions and payment institutions* ***should define data and system security requirements within the outsourcing agreement and monitor compliance with these requirements on an ongoing basis.*** ***[Section 13.2 – Point 81 - 82]***

In line with the EBA Guidelines on ICT risk assessment under the SREP, ***institutions should, where relevant, ensure that they are able to carry out security penetration testing*** *to assess the effectiveness of implemented cyber and internal ICT security measures and processes.* ***[Section 13.3 – Point 94]***

d. Europe (5/5) EBA Guidelines ICT

Objective

These guidelines set out **how financial institutions should manage the ICT and security risks that they are exposed to**. In addition, this guidance aims to provide the financial institutions to which the guidelines apply with a better understanding of supervisory expectations for the management of ICT and security risks.

Failure of ICT systems can have drastic consequences for finantial institutions affecting the foundation of most banking processes and services

Cybersecurity Incident

Singular event or a series of linked events unplanned by the financial institution that has or will probably have an adverse impact on the integrity, availability, confidentiality and/or authenticity of services.

Financial institutions should establish appropriate processes and organisational structures to ensure a consistent and integrated monitoring, handling and follow-up of incidents and ensure root causes are identified and eliminated to prevent the occurrence of repeated incidents including: (a) procedures to identify, track, log, categorise and classify incidents; (b) roles and responsibilities for different incident scenarios, (c) problem management procedures to identify, analyse and solve incidents root cause (and update security measures based on experience); d) effective internal communication plans to relevant senior management (in accordance to criticality); e) incident response procedures to mitigate impacts related to the incidents and ensure that the service becomes operational and secure in a timely manner; f) external communication plans for critical business functions ensuring collaboration with relevant stakeholders to effectively respond to incident and other external parties (*e.g. customers, other market participants, the supervisory authority*) **[Section 3.5.1.60].** Financial institutions should ensure that contracts and SLA with providers include **operational and security incident handling procedures including escalation and reporting. [Section 3.2.3.8]**

c. Spain (1/2) RD 43/2021 & RD 12/2018

Objective

RD 12/2018 transposes the NIS Directive in Spanish regulation creating the **general framework for Security of Networks and Information Systems for the provision of essential services and digital services**.

On 2021, **RD 43/2021 is published building upon general framework set out by RD 21/2018 with special focus on**: Development of strategic and institutional framework for the security of networks and information system, compliance with security obligations of operators of essential services and digital service providers and security incident management.

Cybersecurity Incident (RD 12/18, Art.3)

Unexpected or undesired event with detrimental consequences to the security of networks and information systems security of networks and information systems.

Incident Reporting (RD 43/21, Arts. 3,8,10)

What to notify? OES/DSP *will notify of* ***incidents that may have disruptive effects in the services****, considering for this purpose* ***incidents with a critical, very high or high level of impact****, in accordance to national instruction for notification and management of cyber incidents.* ***They will also notify the events or incidents that, due to their risk, may affect*** *the NIS used for provision of essential services,* ***even when they have not yet had a real adverse effect on them.***

When to notify? **OES/DSP must notify authorities in accordance to notification timelines based incident criticality [*Initial Notification:*** *Immediate (critical, very high and high risk) and n/a (medium and low risk),* ***Intermediate notification:*** *24/48 hours (critical), 72 hours (very high), n/a (high, medium and low),* ***Final notification:*** *20 days (critical), 40 days (very high), n/a (high, medium, low).*

Who must notify? Operators of essential services and digital service providers (through appointed Security Officer)
To whom? Based on infrastructure criticality and sector: CNPIC (all critical infrastructures), CCN (noncritical infrastructure/public sector), and Bank of Spain/ Ministerio de Asuntos Económicos y Transformación Digital, CNMV or Secretaría de Estado para el Avance Digital (noncritical infra/private sector).

c. Spain (2/2) RD 43/2021 & RD 12/2018

Should OES not comply with incident notification obligation RDL 12/2018 sets out the following fine systems based on severity of infringement

Critical infringement: *(i) no actions taken to resolve detected deficiencies after incident (ii) persistant non-notification of material incidents and (iii) lack of mitigation actions against identified incidents*

→ ***From 500.001 to 1.000.000 EUR***

Material infringement: *(i) Security incidents with significant disruptive effects,(ii) relevant unwillingness to manage security incident with significant disruptive effects when service has been materially affected*

→ ***From 100.001 to 500.000 EUR***

Non-material infringement: *(i) no notification of events that, despite not having disruptive effects on services, they must be notified under law*

→ ***Up to 100.000 EUR***

d. Upcoming regulations (1/2): DORA (Europe)

Subject matter

This Regulation lays down the following uniform requirements concerning the security of network and information systems supporting the business processes of financial entities needed to achieve a high common level of digital operational resilience.

Reporting of major ICT-related incidents (DORA, ART.17)

What to notify? Financial entities shall produce, after collecting and analysing all relevant information, an incident report using the template referred to in Article 18 and submit it to the competent authority. The report shall include all information necessary for the competent authority to determine the significance of the major ICT-related incident* and assess possible cross-border impacts.
Who must notify? Financial entities shall report major ICT-related incidents.
To whom? To the appropriate Competent Authority as provided for in Article 41DORA.
When?

- **an initial notification**, without delay, but no later than the end of the business day, or, in case of a major ICT-related incident that took place later than 2 hours before the end of the business day, not later than 4 hours from the beginning of the next business day.
- **an intermediate report,** no later than 1 week after the initial notification.
- **a final report,** when the root cause analysis has been completed, regardless of whether or not mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates, but not later than one month from the moment of sending the initial report.

Where a major ICT-related incident has or may have an impact on the financial interests of service users and clients, financial entities shall, without undue delay, inform their service users and clients

**Major ICT-related incident' means an ICT-related incident with a potentially high adverse impact on the network and information systems that support critical functions of the financial entity*

d. Upcoming regulations (2/2): NIS 2 (Europe)

On May 13th 2022, Council and the European Parliament agreed on measures for a high common level of cybersecurity across the Union, to further improve the resilience and incident response capacities of both the public and private sector and the EU as a whole. Once adopted,NIS 2 will replace the current NIS directive.

Stronger risk and incident management and cooperation

- **Removal of divergences** in cybersecurity requirements and implementation of cybersecurity measures in MS **by setting out minimum rules** and mechanisms for **effective cooperation** among relevant authorities.
- Update of sectors and activities subject to cybersecurity obligations
- **Remedies** and **sanctions** to ensure enforcement (**administrative fines** 10.000.000 EUR max or up to 2%).
- European Cyber Crises Liaison Organisation Network (**EU-CyCLONe**) which will support management of **large-scale cybersecurity incidents**.
- Entities to **notify** competent authorities/CSIRT without undue delay and in any event **within 24 hours.**

Wider applicability scope

- **Size-cap rule.** Medium-sized and large entities operating within the sectors or providing services covered by the directive will fall within its scope (**proportionality**, a higher level of **risk management** and **clear-cut criticality criteria** for determining the entities covered).
- Exclusion of entities carrying out activities in areas such as defence or national security, public security, law enforcement and the judiciary as well as parliaments and central banks but **not public administrations** (applicable at central and regional level)

Others

- Alignment with **sector-specific legislation** (DORA and CER)
- **Voluntary peer-learning mechanism** fostering mutual trust and learning from good practices and experiences
- Streamlined the **reporting** obligations to avoid over-reporting and an excessive burden on entities