Publication of the cyber security[1] directive: requirements for operators of critical infrastructures and essential services

José Miguel Lissén Arbeloa
Partner, IP-IT Practice Area, Gómez-Acebo & Pombo

Isabela Crespo Vitorique
Senior Associate, IP-IT Practice Area, Gómez-Acebo & Pombo

The Directive on security of network and information systems across the Union, a cornerstone of the EU's cyber security strategy, was published on 19 July 2016. This directive requires Member States to adopt a national security strategy and technical and organisational capabilities to prevent, detect and respond to network and information system incidents and risks. The companies and entities that operate critical infrastructures and essential services (energy, transportation, banking and financial markets, the health sector, water supply and digital infrastructure) are largely responsible for ensuring such security and must implement programmes to create a culture of risk management and measures to prevent and handle attacks when they occur.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, also known as the directive on security of network and information systems (the NIS Directive) was published in the Official Journal of the European Union on 19 July 2016 and came into force on 8 August 2016. Member States have until 9 May 2018 to transpose the directive into their national laws.

The directive is part of the European Commission's cyber security strategy, aimed at achieving an "open, safe and secure cyber space", and represents the EU's shared vision on the prevention and proper response to cyber disruptions and attacks, ensures safe growth of the digital economy and contributes to the smooth functioning of the internal market.

1. Subject matter and scope of application

The directive provides measures aimed at achieving a high common level of network and information system security across the Union and for such purpose:

a) sets out a requirement for all the member states to have a national strategy on the security of network and information systems;

b) creates a cooperation group to support and facilitate strategic cooperation and the exchange of information between the Member States as well as developing trust and confidence among them;

c) creates a network of computer security incident response teams (CSIRT);

d) lays down security and notification requirements for operators of essential services and digital service providers;

e) provides a requirement for all the Member States to designate national competent authorities, single points of contact and CSIRT.

[1] Translator's note: There is no consensus as to whether or not "cyber" should be combined with "security" as a prefix, although in the UK, and Europe at large, keeping these as two separate words is currently the convention.

2. National security strategy

Each Member State must adopt a national strategy on the security of network and information systems, defining the strategic objectives and concrete policy actions to be implemented in order to achieve and maintain a high level of security, covering, at a minimum, the sectors and services listed in annexes II and III of the directive.

The sectors identified in annex II are energy, transport, banking, financial market infrastructures, health settings, drinking water supply and distribution and digital infrastructure, while the services identified in annex III are online marketplaces, online search engines and cloud computing services.

Among other issues, the national strategy on the security of network and information systems shall address the following: *(a)* the objectives and priorities of the national strategy on the security of network and information systems; *(b)* a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors; *(c)* the identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors; *(d)* an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems; *(e)* an indication of the research and development plans relating to the national strategy on the security of network and information systems; *(f)* a risk assessment plan to identify risks; *(g)* a list of the various actors involved in the implementation of the national strategy on the security of network and information systems.

3. Identification of operators of essential services

By 9 November 2018, for each sector and subsector referred to in Annex II, Member States shall identify the operators of essential services with an establishment on their territory. Such operators are those that provide the services identified below, grouped by sectors and subsectors of activity:

- Energy/electricity: Distribution system operators and transmission system operators.
- Energy/oil: Operators of oil transmission pipelines and operators of oil production, refining and treatment facilities, storage and transmission,
- Energy/gas: supply undertakings, distribution system operators, transmission system operators, storage system operators, liquid natural gas system operators, natural gas undertakings and operators of natural gas refining and treatment facilities
- Air transport: air carriers, airport managing bodies and traffic management control operators.
- Rail transport: infrastructure managers, railway undertakings
- Water transport: inland, sea and coastal passenger and freight water transport companies, managing bodies of ports and operators of vessel traffic services.
- Road transport: Road authorities and operators of intelligent transport systems.
- Banking: credit institutions.
- Financial market infrastructures: operators of trading venues and central counterparties.
- Health settings: Healthcare providers.
- Drinking water supply and distribution: Suppliers and distributors of water intended for human consumption.
- Digital Infrastructure: IXPs, DNS service providers, TLD name registries.

In order to determine the significance of a disruptive effect, Member States shall take into account the following cross-sectorial factors: *(a)* the number of users relying on that service; *(b)* the dependency of other sectors referred to in Annex II on the service provided by that entity; *(c)* the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety; *(d)* the market share of that entity; *(e)* the geographic spread

with regard to the area that could be affected by an incident; *(f)* the importance of the entity for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service..

4. Cooperation group and CSIRT network

A Cooperation Group is established in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence, and with a view to achieving a high common level of security of network and information systems. The Cooperation Group shall have the following tasks, among others: *a*) exchanging best practice on the exchange of information related to incident notification; *b*) exchanging information and best practice on research and development relating to the security of network and information systems; and *c*) collecting best practice information on risks and incidents affecting such networks and systems.

A network of the national CSIRTs is established in order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation. The network shall have the following tasks: *(a)* exchanging information on CSIRTs' services, operations and cooperation capabilities; *(b)* exchanging and discussing non-commercially sensitive information related to that incident and associated risks; *(c)* exchanging and making available non-confidential information concerning individual incidents; *(d)* discussing and, where possible, identifying a coordinated response to an incident that has been identified in a Member State; *(e)* providing Member States with support in addressing cross-border incidents; *(f)* discussing, exploring and identifying further forms of operational cooperation, issuing guidelines in order to facilitate the convergence of operational practices concerning operational cooperation.

5. Security and notification requirements

Member States shall ensure that operators of essential services: (1) take appropriate and proportional technical and organisational measures to manage the risks posed to the security of network and information systems; (2) take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services; (3) notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide. Notification shall not make the notifying party subject to increased liability

Furthermore, Member States shall ensure that digital service providers: (1) take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering their services; (2) take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services referred to in Annex III that are offered within the Union, with a view to ensuring the continuity of those services; (3) notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service. Similarly, in this case, notification shall not make the notifying party subject to increased liability.

6. Promotion of a "risk management culture"

In recitals 44 and 46 of the directive, the EU legislature emphasises that its objective is for the operators of essential services and providers of digital services to be largely responsible for ensuring the security of network and information systems. For this purpose, it underscores that "a culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced, should be promoted and developed [by the Member States] through appropriate regulatory requirements and voluntary industry practice". These risk management measures include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact.

7. Actions to put into practice

Without prejudice to the way in which the EU legislature's mandate, as contained in

the directive and the voluntary sector practices to implemented by operators of essential services, digital service providers and Member States' regulatory bodies, is incorporated into Spanish and Portuguese law, our understanding is that, in line with the recommendations and guidelines proposed last year by bodies such as the US Securities and Exchange Commission (SEC) or Office of Compliance, Inspections and Examinations (OCIE), in light of the growing proliferation of attacks, threats and risks for the security of network and information systems, operators of essential services and digital service providers must take measures aimed at creating and consolidating a culture of risk management and protection of their company's assets.

A good cyber security and defence programme rests on two fundamental pillars: regulatory compliance and cyber threat intelligence. In order to effectively achieve such a programme, companies and operators of infrastructure and critical services should take the following measures:

1) *Regulatory compliance: policies and procedures and good corporate governance.*

   a) Appointment of a CSIRT team leader within each organisation.

   b) Implementation of good general and sector practices, particularly in the most vulnerable departments.

   c) Development of cyber security programme policies and procedures that include:

   - The determination of risk maps in connection with cyber security and protection of the company's assets, especially with respect to databases and critical information.
   - The identification of the company's cyber assets (assets with exposure to the internet: databases, industrial control systems (ICS, SCADA…); financial, strategic, employee or client information; intellectual property, industrial and commercial secrets, etc.).
   - Incident response protocol.
   - Protocols for internal notifications and notifications to the competent authorities in the case of a computer security breach.
   - Employee action and liability policies regarding the use of the company's computer tools.

2) *Cyber risk intelligence: operational measures.*

   a) Implementation of a cyber threat intelligence programme to manage risks and attacks.

   b) Employee training on cyber risks in order to ensure minimum levels of preparation for adverse scenarios.

   c) Establishment of network and information system access control protocols for third parties (providers, clients, commercial partners, etc.).

   d) Implementation of physical security measures for critical cyber assets.