New cyber security law: what does the NIS Directive mean for your business?

10 February 2016

Political agreement has been reached on a new European regime imposing cyber security requirements and incident notification obligations on banks, energy companies and other operators of essential services identified by member states, together with certain digital service providers. Implementation through national laws is expected within two years.

Political agreement at last

"The agreement constitutes a major step in improving the resilience of our network and information systems in Europe."

Günther H. Oettinger, Commissioner for the Digital Economy and Society

On 7 December 2015, the European Parliament and the Luxembourg Presidency of the Council reached informal agreement on a new cyber security law. The Directive lays down measures aimed at achieving a high common level of security of networks and information systems (NIS) within the EU. There are three main elements to the NIS Directive:

- security and notification requirements for businesses in certain 'critical' sectors. It adopts two regimes - one for operators of essential services in sectors such as energy, transport, banking and health, and a second for digital service providers (which is intended to be less stringent);
- obligations on Member States to adopt an NIS strategy and designate national competent authorities, a single point of contact and a Computer Security Incident Response Team (CSIRT) with tasks related to the security of networks and information systems; and
- establishing a European framework, with a cooperation group and CSIRTs network, to support and facilitate strategic co-operation across Europe. ENISA[1] will also play an important role - providing expertise, helping develop guidelines and facilitating the exchange of best practices.

In this briefing we focus on the requirements operators of essential services will face.

BACKGROUND

The NIS Directive was originally proposed under the EU Cyber Security Strategy published in February 2013. However, despite high profile cyber breaches across Europe and heightened media attention on the cyber terror threat, the

[1] The European Union Agency for Network and Information Security

Directive took longer than expected to agree. A number of sticking points emerged, including which organisations should be covered by the regime. The treatment of digital service providers in particular proved a contentious issue (our previous article The NIS Directive: Genesis, Status and Key Aspects provides more detail on these discussions).

Political agreement was finally reached on 7 December 2015. A draft version of the compromise text was made available by the Council of the European Union on 18 December[2], the date on which its Permanent Representatives Committee (Coreper) endorsed the informal deal. That text, which we refer to in this article, states it is subject to revision, and formal approval is still required (see Next Steps: Formal approval below).

SECURITY AND BREACH NOTIFICATION REQUIREMENTS

For businesses, the key aspects of the NIS Directive are the new requirements around the security of networks and information systems and incident notification. These apply to both operators of essential services and digital service providers, although the regimes differ slightly. They do not, however, apply to undertakings providing public communications networks or publicly available electronic communications services[3], nor to qualified and non-qualified trust service providers under the eID Regulation,[4] which have their own security regimes.

Security requirements and incident notification: operators of essential services ("OES")

Who is affected by these new requirements?

If you are identified by a Member State as an OES you may now face additional security and incident notification obligations. In practice, if you are not an OES but supply services to OES this new law may also affect you. Many OES may wish to contractually flow down these obligations, to help with their compliance.

Who are OES?

The Directive sets out a list of relevant sectors (see table over page) and criteria to help Member States identify OES with an establishment on their territory. According to the Directive, an OES is a public or private entity, meeting any of these sector/type descriptions and which meets all of the following criteria:

- an entity provides a service which is essential for the maintenance of critical societal and/or economic activities. Each Member State will establish a list of these services, and will consult with other relevant Member States before identifying any entity which provides a listed service in two or more Member States;
- the provision of that service depends on network and information systems; and
- an incident to the network and information systems of that service would have significant disruptive effects on its provision. There are a number of cross-sectoral factors which Member States should take into account when determining the significance of a disruptive effect, including the number of users relying on the relevant service and its market share. Sector-specific factors should also be taken into account where appropriate, and the recitals provide some examples of these. For example, for banking/financial market infrastructures these include their systemic importance based on total assets or the ratio of those total assets to GDP.

[2] http://www.consilium.europa.eu/en/press/press-releases/2015/12/18-cybersecurity-agreement/

[3] Article 1(3) refers to Articles 13a and 13b of the Framework Directive 2002/21/EC.

[4] Regulation 910/2014

Table listing the types of entity which may be identified as OES

SECTOR	SUBSECTOR AND TYPE OF ENTITY
Energy	Electricity: Electricity supply undertakings, distribution system operators and transmission system operators
	Oil: Operators of oil transmission pipelines and operators of oil production, refining and treatment facilities, storage and transmission
	Gas: Supply undertakings, distribution system operators, transmission system operators, storage system operators, LNG system operators, natural gas undertakings and operators of natural gas refining and treatment facilities
Transport	Air: Air carriers, airport managing bodies and entities operating ancillary installations contained within airports, and traffic management control operators providing air traffic control
	Rail: Infrastructure managers and railway undertakings including operators of service facilities
	Water: Inland, sea and coastal passenger and freight water transport companies (not including the individual vessels operated by those companies), managing bodies of ports including their port facilities and entities operating works and equipment contained within ports, and operators of vessel traffic services
	Road: Road authorities responsible for traffic management control and operators of intelligent transport systems
Banking	Credit institutions
Financial market infrastructures	Operators of trading venues and central counterparty
Health	Health care settings including hospitals and private clinics, health care providers
Drinking water	Supplier and distributor of water intended for human consumption (excluding distributors for whom distribution is only part of their general activity of distribution of goods and commodities)
Digital infrastructure	Internet exchange points, domain name system service providers and top level domain name registries

When will OES be identified?

It is not clear when Member States will choose to identify OES with an establishment on their territory. However, the Directive states that they must have done so by a date six months after the date they adopt and publish their implementing legislation. They will also receive support from the cooperation group to take a consistent approach to identifying OES, and they must regularly (and at least every two years) update their lists.

OES security measures: managing risks and minimising impacts

Member States must ensure that OES take appropriate and proportionate technical and organisational measures to "manage the risks posed to the security of networks and information systems which they use in their operations." Those measures shall, having regard to the state of the art, ensure a level of security appropriate to the risk presented – concepts familiar to many organisations from the Data Protection regime.

OES must also take appropriate measures to prevent and minimise the impact of incidents, with a view to ensuring the continuity of those services.

The recitals state that, while OES may provide both essential and non-essential services, they should only be subject to the security obligations with respect to those services which are deemed essential.

However, these are not the only security measures that may apply. The Directive prescribes minimum harmonisation, meaning Member States can adopt or maintain provisions which achieve a higher level of security of networks and information systems. Also, where sector specific Union legislation contains security or notification requirements which are at least equivalent in effect to the obligations in the NIS Directive, those provisions shall apply instead of the corresponding provisions of the NIS Directive.

Member States will also be encouraging the use of European or internationally accepted standards and specifications relevant to network and information security.

OES incident notifications requirements

Member States must ensure that OES notify the competent authority or CSIRT, without undue delay, of incidents having a significant impact on the continuity of the essential services they provide. The Directive sets out three parameters which "in particular" shall be taken into account when determining the significance of the impact:

- the number of users affected by the disruption to the essential service;
- the duration of the incident; and
- the geographical spread of the area affected by the incident.

The Directive expressly states that notification will not expose the notifying party to increased liability.

Recognising the cross-border nature of many cyber breaches, the notification must include information to enable the competent authority or CSIRT to determine any cross-border impact. It shall then inform other affected Member State(s) if the incident has a significant impact on the continuity of essential services in that Member State. However, in accordance with EU law or national legislation, the operator's security and commercial interests will be preserved, together with the confidentiality of the information provided by the operator.

Following consultation with the OES, that competent authority or CSIRT may also inform the public about individual incidents where public

awareness is necessary to prevent or deal with an incident.

Competent authorities acting together with the cooperation group may develop and adopt guidelines concerning the circumstances in which OES are required to notify incidents, including on the parameters to determine the significance of the impact of an incident.

How will this be enforced

Member State competent authorities will have the necessary powers to assess the compliance of OES with their requirements and to require OES to provide:

- information needed to assess the security of their networks and information systems, including documented security policies; and
- evidence of effective implementation of security policies – e.g. the results of a security audit carried out by the competent authority (and it will be interesting to see the powers Member States give competent authorities, especially around audit) or a qualified auditor.

Following assessment of this information or the results of these security audits, the competent authority may issue binding instructions to an OES to remedy its operations. Where an incident has occurred involving personal data, the competent authority will work closely with the data protection authorities - and respecting data protection is a theme running throughout the Directive.

There may also be penalties for breach of the national laws implementing the NIS Directive which the different Member States will lay down. These must be "effective, proportionate and dissuasive". Again, it will be interesting to see what Member States do here, particularly given the large penalties which will apply under the new General Data Protection Regulation, and the powers already held by regulators in some affected sectors, e.g. the FCA and PRA in the UK.

In terms of who will regulate, while the UK has already established its own CSIRT (CERT UK), it is not yet clear who the national competent authority will be. The ICO has publically stated that it is not seeking to take on the role.[5]

Digital service providers (DSPs): Security requirements and incident notification

While our focus here is on OES, the Directive does set out a separate regime for DSPs, which aims to be less stringent and more harmonised than the one for OES. This compromise position was reached after much debate over whether, and to what extent, providers of information society services should be covered by this regime.

DSPs are any legal persons who provide a digital service which is of a type listed below:

- an online marketplace - a digital service that allows consumers and/or traders to conclude online sales and service contracts with traders either on its website or on a trader's website using computing services it provides (e.g. Amazon);
- an online search engine - a digital service that allows users to perform searches of all websites or websites in a particular language on the basis of a query on any subject (e.g. Google);
- a cloud computing service – a digital service that enables access to a scalable and elastic pool of shareable computing resources.

[5] https://ico.org.uk/

A Digital Service is:

- "any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" (as defined in Directive 2015/1535); and
- which is of a type listed in Annex III – i.e. an online marketplace, search engine or cloud computing service.

Micro and small enterprises are excluded from the requirements.

The cross border nature of DSPs means their regime imposes a higher level of uniformity across the EU - for example Member States do not have the same flexibility to identify DSPs as they do for OES, and are prevented from imposing higher security obligations on them.

Many of the security and notification requirements are similar to those for OES. However, there are some key differences, particularly around incident notification and enforcement, which aim to provide a lighter touch regime. There is also one key difference that directly impacts on OES – if an OES relies on a DSP for the provision of a service which is essential for the maintenance of critical societal and economic activities then it, rather than the DSP, must notify any significant impact on the continuity of the essential service due to an incident affecting that DSP.

Voluntary notification

Organisations which have not been identified as OES and are not DSPs may still notify incidents having a significant impact on the continuity of the services they provide on a voluntary basis.

NEXT STEPS: FORMAL APPROVAL

Once the agreed text has undergone technical finalisation, it still needs to be formally approved first by the Council and then by the Parliament.

The procedure is expected to be concluded in spring 2016.

After the directive has entered into force, Member States will have 21 months to adopt the necessary national provisions, and a further 6 months to identify OES in their territory. It will be interesting to see: (i) whether Member States will use this additional time period for identifying OES; and (ii) if they do use it, how they will bring the security and notification requirements into force for both DSPs and OES.

NEXT STEPS: HOW DO ORGANISATION PREPARE

If you are a bank, energy distributor, water company, transport operator or other organisation which may be covered by the new regime, this period before you have a formal legal obligation to comply with the new measures will be a busy one. You will need to:

- assess if you could fall within the definition of an OES – potential OES may not know definitively for some time if they have been identified by a Member State as falling within the regime. However, the Directive does provide criteria and guidance for the Member States, which potential OES can also use to help see if they fit the criteria;
- ensure that your technical and organisational measures are sufficiently robust to withstand an evolving threat and increased regulation – while many organisations already strive to review your existing policies and procedures around risks to your business and incident

response to ensure they are sufficiently broad to cover 'cyber' – many organisations will already have some breach notification procedures and policies in place, for example where personal data is involved or where a sector regulator (such as the FCA/PRA) already requires it. However, a cyber breach may take many forms, and it is therefore important to ensure that your focus is not narrowly directed, for example towards personal data;

- consider whether to contractually flow down any obligations to your supply chain. Many of your key suppliers - particularly technology providers, outsource suppliers and their sub-contractors - will hold your data, have access to your systems and/or help you implement appropriate technical and organisational measures. You should therefore check what security obligations, notification requirements and flow-down obligations are contained in your contracts with them, and ensure that these obligations are detailed enough and sufficiently broad to enable you to comply with your new cyber requirements; and

- consider whether you have access to the necessary legal and technical expertise to effectively manage this high profile business risk. You will need to understand how relevant Member States are implementing the Directive, and how this will sit with any existing regulation you face. Will you face dual obligations, or will the existing EU law specific to your sector apply instead of the corresponding provisions in the NIS Directive (see OES Security above)? For example, the financial sector is one where prudential regulators already place great importance on managing operational risk, including security – a fact recognised in the recitals of the NIS Directive.

CYBER SECURITY AT SLAUGHTER AND MAY

Through the joint working of its Technology, Corporate, Dispute Resolution and Financial Regulation Groups, Slaughter and May helps its clients manage their cyber risks within their corporate governance and regulatory structures.

This article was written by Rob Sumroy (Partner) and Natalie Donovan (PSL) from Slaughter and May's Technology team. It is based on an article which appeared in Cyber Security Law & Policy (January 2016). For further information, please contact Rob, Natalie or your usual Slaughter and May contact.