SLAUGHTER AND MAY

BRIEFING
JUNE 2015

The NIS Directive: Genesis, Status, and Key Aspects

WHAT IS THE NIS DIRECTIVE?

The Network and Information Security Directive is the European Commission's proposed directive concerning measures to ensure a high common level of network and information security across the EU. The scope of the Directive itself is currently the subject of ongoing discussions between the European Parliament, the Council of the EU and representatives of the national governments within the Council. Press sources have reported that the Latvian Presidency is pushing to advance the discussions as far as possible before the end of its tenure on 30 June, and it is possible that a deal on the final form of the Directive is imminent. However, the Latvian defence minister himself has accepted that negotiations around the scope of the Directive will probably stretch into the second half of this year, and the UK's Department for Business, Innovation and Skills (BIS) have commented that, while the outstanding issues could be resolved before the summer recess, it is not inconceivable that an agreement will only be reached in autumn of this year.[1]

Genesis of the proposal

The Commission's proposal for the Directive was originally published on 7 February 2013,[2] alongside the EU's Cyber Security Strategy (which contains non-legislative measures on a broad range of cyber security issues). The proposal was underpinned by the Commission's overarching desire to establish a secure EU digital single market and to ensure the smooth functioning of the internal market more generally. As the Commission stated in the text of the legislative proposal accompanying the draft Directive, "network and information systems and services play a vital role in facilitating the cross-border movement of goods, services and people. Substantial disruption of these systems in one Member State can affect other Member States and the EU as a whole".[3]

The Commission's concerns about the scale of the risks posed by cyber attacks emerged as a result of the ever-increasing digitalisation of businesses and vital services across the EU, and the acknowledgment of the fact that "there is currently no effective mechanism at EU level for effective cooperation and collaboration and for secure information sharing on NIS incidents and risks among the Member States".[4]

The current data protection regime imposes security obligations on organisations in relation to their handling of personal data. There are also a number of sector-specific regulations imposing notification requirements and obligations to take appropriate technical and organisational measures to manage breaches which would cover cyber incidents. However, the Directive will apply similar provisions to a far wider range of organisations

1 BIS update on the negotiation of the NIS Directive (5 June 2015): http://www.bankofengland.co.uk/financialstability/fsc/Documents/nisupdatejune2015.pdf

2 Commission proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (7 February 2013): http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN

3 Commission's Legislative Proposal 2013/0027 (COD) (7 February 2013): http://www.europarl.europa.eu/oeil/popups/summary.do?id=1247517&t=e&l=en

4 Ibid.

falling within the definition of "market operators", which, broadly, covers organisations which manage critical infrastructure or provide essential services. It is intended that this will encourage higher security standards from these important organisations and enable authorities to gather intelligence with which they can better combat cyber threats.

Progress of the proposal

Following the Commission's initial proposal of 7 February 2013, the Parliament adopted an amended version of the proposal on 13 March 2014.[5] The Directive will not become law until the text has been agreed between the Parliament and the Council. The Council itself has not yet reached a formal position,[6] but a document on the proposal's 'state of play', setting out the Council's proposed amendments as submitted on 7 November 2014, was published on 14 January 2015.[7]

Negotiations between the EU institutions and among national representatives within the Council commenced in autumn 2014 and remain ongoing: even if a swift deal can be reached in the coming weeks, the formal process will likely not conclude until the latter half of this year. Once the agreed text has been finalised, the Directive will then have to be implemented into domestic law by the national governments of each Member State. The Council's proposed amendments envisage a two and a half year implementation period,[8] meaning that the provisions of the Directive are unlikely to bite on organisations until at least 2018.

WHAT ARE THE KEY ASPECTS OF THE NIS DIRECTIVE?

The key aspects of the proposed Directive are: (i) the establishment of a national network information security strategy and regulatory regime in each Member State, including the establishment of a national competent authority and a Computer Emergency Response Team (CERT); (ii) the establishment of a cooperation network to encourage information exchange between Member States; and (iii) the imposition of risk management and reporting obligations on certain market operators in particular strategic sectors.

Regulatory regime

The Directive will require each Member State to establish a national network information security strategy, under which they will be obliged to designate a national competent authority (or indeed several under the Parliament and Council proposals, provided a national single point of contact remains responsible and accountable) to monitor compliance with the Directive and to receive network and information security incident notifications. It is up to each Member State to establish specific rules on the sanctions for non-compliance with the regime. The identity of the national competent authority in the UK will be an important question on implementation – it remains to be seen whether a new body will be established or whether an existing regulator (for example, the ICO) will take on these responsibilities. The UK will also need to consider how the new reporting requirements will interact with existing notification requirements and voluntary notification schemes under sector-specific regulatory frameworks.

Member States will also be required to set up a CERT (or, as with the national competent authorities, several) as a point of contact to prevent, handle and respond to network and information security incidents and risks at national

5 European Parliament legislative resolution of 13 March 2014 on the proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (13 March 2014): http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0244

6 European Parliament procedure file for the Directive : http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2013/0027(COD)&l=en

7 Council of the European Union "state of play" document (14 January 2015): http://data.consilium.europa.eu/doc/document/ST-5257-2015-INIT/en/pdf

8 Ibid, p.128.

level. Broadly, CERTs will be engaged in monitoring and responding to incidents, providing early warnings and alerts, sharing risk and incident information with relevant stakeholders, building public awareness of the risks associated with online activities, and promoting the adoption of standardised practices for cyber security. The UK government established CERT-UK in March 2014 to fulfil a similar role, and it will be interesting to see how its roles and responsibilities develop following the implementation of the Directive, in particular with regard to its interactions with other national CERTs across the EU.

Cooperation network

The Directive will also result in the establishment of a cooperation network between Member States to facilitate information exchange and strengthen and harmonise security standards across the EU.

The makeup and responsibilities of this network have varied significantly between proposed drafts of the Directive, so it is still not entirely clear what form it will take in the final agreement. The Commission's original proposal envisaged a cooperation network between the Commission and national competent authorities, assisted by the European Network and Information Security Agency (ENISA) when necessary. The Council has proposed an alternative framework consisting of two separate networks: (i) a cooperation group between the Commission, ENISA, and representatives from each Member State; and (ii) a network composed of representatives from the national CERTs.[9] The Parliament has indicated that it may be willing to accept a solution within the framework proposed by the Council, provided there is potential for the development of more advanced forms of operational cooperation in the future.[10]

Risk management and reporting

Finally, the Directive will impose enhanced risk management and reporting obligations on "market operators". Organisations that fall within that definition will be required to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of the network and information systems which they control and use. They will also be required to notify their national competent authority of incidents which have a significant impact on the security of the core services they provide.

The nature of these obligations has been subject to significant negotiation and amendment throughout the various stages of the Directive's progress. Key issues at stake include the nature of the "technical and organisational measures" required (i.e. what standards do organisations have to comply with?) and the scope of the reporting obligations (i.e. which incidents have to be reported?). However, the crucial outstanding issue in the ongoing negotiations is the nature of the organisations which fall within the definition of "market operators" (i.e. which organisations have to comply with the regime?).

Under the Commission's original proposal, "market operators" included "operators of critical infrastructure" in five key sectors (energy, transport, banking, financial market infrastructure and health). It also included providers of key digital services which enable the provision of other digital services (including e-commerce platforms, internet payment gateways, social networks, search engines, cloud computing services and app stores) on the list. The Parliament, in its amended proposal, added a number of additional categories (including businesses forming part of the food supply chain) to the list of infrastructure sectors caught by the regime. Crucially, however, it rejected the application of the Directive to digital service providers (on the basis that inclusion of such entities would be

9 "State of play" document, pp.57ff.: http://data.consilium.europa.eu/doc/document/ST-5257-2015-INIT/en/pdf
10 Ibid. p.2.

disproportionate and could make regulation of the Directive unmanageable, although it did add Internet exchange points to the list).[11]

The treatment of digital service providers in particular has proved a sticking point in discussions between the EU institutions, but also within them: there is still no agreement on the issue between the national government representatives in the Council. Press reports have indicated that the UK is among those Member States opposed to the inclusion of digital services within the scope of the Directive, on the basis that a cyber attack on such organisations, while potentially disruptive, would not have a sufficiently significant impact on society or the economy to merit the additional regulation. Other Member States, however, have argued that digital businesses should fall within the scope of the regime. As a compromise, the Commission has recently suggested that digital businesses should be subject to a lighter touch regime than other essential services, for example that they should not be required to include information regarding the cross-border impact of any breach when they notify that incident to their national supervisory authority.

The Council and the Parliament also remain divided more generally on the approach to determining scope. The Parliament's "maximalist" proposal envisages that all relevant organisations in the sectors identified in the Directive will be subject to the regime. The Council, however, has argued that the Directive should leave Member States with the final say in determining precisely which organisations within their jurisdiction fall within the scope of the regime in order to avoid an otherwise disproportionate regulatory burden.[12]

The Directive's future impact on business within the UK and across the EU therefore remains unclear, not least because of the ongoing uncertainties regarding the nature of the organisations which will fall within the regime. However, if the disagreements among the EU institutions and national governments can be resolved over the coming weeks or months, we may soon have a much clearer picture of the shape of things to come. In our next article, which will be published once the final text of the Directive has been agreed, we will look at the implications of the Directive for businesses.

This briefing was written by Rob Sumroy (Partner), Nikhil Shah (Associate) and Natalie Donovan (Professional Support Lawyer) from Slaughter and May's Technology Group. It was first published in Cybersecuritylaw&practice, June 2015.

[11] Ibid. pp. 25-26.

[12] See "state of play" document, pp.26-27: http://data.consilium.europa.eu/doc/document/ST-5257-2015-INIT/en/pdf and BIS update document: http://www.bankofengland.co.uk/financialstability/fsc/Documents/nisupdatejune2015.pdf