BCLP. Client Intelligent

Insights

CLOSING GAPS IN THE CYBER ARMOUR—UK AND EU LEGAL REFORMS TO BOOST NETWORK SECURITY STANDARDS

Mar 11, 2022

This article was first published by LexisNexis UK.

Overview: Kate Brimsted, partner and Data Privacy & Security UK lead, and Anna Blest, principal knowledge development lawyer, of Bryan Cave Leighton Paisner, consider the proposed reforms to the UK Network and Information Systems Regulations 2018 (NIS Regulations) and their relationship with the EU's proposed NIS2 Directive.

BACKSTORY - UK CONSULTATION

The Department for Digital, Culture, Media & Sport (DCMS) has launched a consultation on wide-ranging proposals to reform the NIS Regulations, SI 2018/506. Views are being sought on proposals for legislative changes which would improve levels of cyber resilience. The deadline for response to the consultation is 11.45 pm on 10 April 2022.

High profile cyber attacks, such as the Solar Winds supply chain compromise (December 2020) and the attack on managed service provider, Kaseya, (July 2021) demonstrated graphically the ability of malicious actors to compromise national security and interfere with critical national infrastructure, as well as causing significant economic harm and disruption.

The current review of the UK's cybersecurity regime (in particular the NIS Regulations) comes at a time when the EU is also considering how to update its own network security regime in the face of greater cyber risk and increasingly complex digital supply chains. The UK and EU are therefore both developing regulatory reforms in this area.

WHAT IS THE BACKGROUND TO THE PROPOSED REFORMS AND WHAT ISSUES ARE THEY ATTEMPTING TO ADDRESS?

The government has confirmed that it has ambitions for the UK to become a global cyber power, with the Home Secretary announcing in May 2021 that the country is 'taking a new, comprehensive approach to strengthen our position as a democratic cyber power'.

The NIS Regulations have their root in Directive (EU) 2016/1148 (the EU-NIS Directive (NIS1)) and have already been updated in 2020 following a post-implementation review. However, it was not possible to achieve all of the intended updates at that time. The UK consultation therefore focuses on supply chain cybersecurity risks, in particular, those posed by the mass adoption of managed services. Providers of such services have the ability to access the networks of thousands of other companies. A vulnerability in one such service provider then risks exposing the networks of all its customers and potentially jeopardises the running of critical infrastructure—a classic 'weakest link' effect. At the same time, there are currently few cyber security-specific requirements applicable to these types of provider.

The UK reforms seek to cast the net wider, to bring more service providers within the remit of the NIS Regulations. Consideration is also being given to requiring mandatory adherence to the National Cyber Security Centre's (NCSC) Cyber Assessment Framework.

WHAT ARE THE KEY PROPOSED CHANGES AS COMPARED WITH THE ORIGINAL NIS REGULATIONS? ARE ANY POTENTIALLY PROBLEMATIC?

The main changes proposed are:

- expand the scope of 'digital services' to include 'managed services'
- apply a two-tier supervisory regime for all digital service providers—a new proactive supervision tier for the most critical providers, alongside the existing reactive supervision tier for everyone else
- create new delegated powers to enable the government to update the NIS Regulations, both in terms of framework but also scope, with appropriate safeguards
- create a new power to bring certain organisations, ones that entities already in scope are critically dependent on, within the remit of the NIS Regulations, and
- strengthen existing incident reporting duties, currently limited to incidents that impact on service, to also include other significant incidents

Of these, the most significant change is to broaden scope of the NIS Regulations to catch additional digital service providers, primarily those offering managed services, who will now also be 'relevant digital service providers' (RDSPs) within the terminology of the NIS Regulations. The proposals would therefore bring into scope companies offering a broad range of managed services, on an external supplier B2B basis, involving regular and ongoing service management of data, IT infrastructure, IT networks and/or IT systems and relying on network and information systems. Service providers with privileged access or connectivity to customer data, IT infrastructure, IT networks and/or IT systems or which perform essential or sensitive functions, such as the processing and/or storage of confidential or business-critical data, would then come within the NIS

Regulation for the first time. Examples of the sorts of services which proposed to be brought into scope include managed print services, WAN support services, security monitoring, BPO, application management and data analytics services.

Providers will have to register with the relevant competent authority (for RDSPs this is the Information Commissioner's Office (ICO)) and have appropriate and proportionate security measures in place (and potentially may be compelled to meet minimum cybersecurity standards, such as the NCSC's CAF Framework) to ensure that their own network and information systems are secure. They will also be required to report relevant incidents to their competent authority. The requirement for international companies to designate a UK representative remains in place and would therefore apply to all newly captured managed service providers.

The reforms envisage a risk-based approach (in step with UK's stated post-Brexit aims to look at risk-based regulatory strategy). Accordingly, the most critical digital service providers would be subject to a new 'proactive supervision tier' (and required to demonstrate to the ICO that they comply with the NIS Regulation) alongside the existing reactive supervision tier for other digital service providers, which will be more light touch.

Businesses may be concerned by the proposal to leave the criteria for assessing criticality of a service (and therefore the level of regulatory scrutiny which will apply) to be determined by the ICO in later guidance. While this allows for flexibility as technology develops and cybersecurity risks evolve, this could lead to significant, unanticipated investment costs for businesses previously out of scope of the NIS Regulations.

The government is also seeking new delegated powers to enable it to update the NIS Regulations more flexibly, to facilitate greater agility in responding rapidly to new technologies and threats to cybersecurity. It also wants to create an ability to reach through a supply chain, by creating a new power to designate critical suppliers or services, on which existing essential and digital services depend, bringing such suppliers directly within scope of the NIS Regulations.

The proposals increase incident reporting duties (currently limited to incidents that impact on service or affect continuity of service), to also include other significant incidents that have an impact on the security of systems underpinning the provision of an essential service. It is not yet known if the proposed reforms will increase the penalties for non-compliance above the current £17m threshold for a material contravention which 'has or could have created a significant risk to, or significant impact on, or in relation to the service provision by the OES or RDSP' (SI 2018/596, reg 18).

TO WHAT EXTENT ARE THE REFORMS PROPOSED FOR THE EU'S NIS2 DIRECTIVE SIMILAR TO THESE PROPOSALS?

The EU's reforms (which would repeal and replace NIS1 with 'NIS2') are also set to widen the scope of NIS1, to cover all medium-sized and large organisations that operate within a large number of

further sectors. However, unlike for the UK, NIS2 would:

- remove the distinction set out in NIS1 between 'operators of essential services' and 'digital service providers' so that all medium-sized and large entities active in the sectors covered by NIS2 would have to comply with the cybersecurity rules
- greatly increase the scope of the NIS2 regime beyond those sectors currently covered and managed services providers (for now the UK government is seeking a more limited scope increase, with powers to extend the UK's regime)

In common with the UK, NIS2 also addresses cybersecurity of the ICT supply chain, covering business-to-business ICT service management.

The EU's NIS2 also envisages a two-stage approach to incident reporting. Affected companies will have 24 hours from when they first become aware of an incident to submit an initial report, followed by a final report no later than one month later. NIS2 also establishes sanctions for breaches of the rules regarding cybersecurity risk management or their reporting obligations. These include national administrative fines of at least up to €10m or 2% of the entities' total turnover worldwide, whichever is higher.

Like the UK, the EU's proposals need to be viewed in the context of its other sectoral developments, such as the proposed Directive on the resilience of critical entities (CER Directive) and the proposed Regulation on digital operational resilience for the financial sector (DORA). The interplay between the UK and EU reforms looks set to lead to divergent scopes and reporting obligations, as well as the need to designate NIS representatives in both the UK and EU.

WHAT ARE THE NEXT STEPS AND LIKELY TIME FRAMES FOR THE PROPOSED UK AND EU REFORMS?

The UK Government consultation closes on 10 April 2022. The EU's proposal is now in the negotiation phase between the Council and the European Parliament. Once the final text is adopted, it is anticipated EU Member States will have two years to transpose NIS2 into national law. It is therefore likely that the UK may legislate ahead of the EU.

The UK's NIS reform proposals should also be seen in the context of the UK's ambitious cybersecurity strategy for 2022–2030 launched in January 2022. Separately, it has developed proposals on enhancing the security of connected smart devices (the Product Security and Telecommunications Infrastructure Bill—currently before Parliament) and a drive to train more cyber professionals.

MEET THE TEAM

Kate Brimsted

London

kate.brimsted@bclplaw.com
+44 (0) 20 3400 3207

Anna Blest

London

anna.blest@bclplaw.com
+44 (0) 20 3400 4475
