BCLP. Client Intelligent

Insights

CYBER LAWS WILL BE UPDATED TO BOOST UK'S RESILIENCE AGAINST ONLINE ATTACKS

Dec 30, 2022

SUMMARY

Information Law analysis: Kate Brimsted, Partner and Data Privacy & Security UK Lead, and Camilla Gelson-Thomas, Associate, discuss the upcoming cyber laws to be updated (the Network and Information Systems Regulations 2018 (NIS Regulations), SI 2018/506) in an effort to boost the UK's resilience against online attacks.

This analysis was first published on Lexis®PSL on 21 December 2022 (subscription required)

The UK government confirmed on 30 November 2022 that there will be changes to the UK's cybersecurity regulations in response to a public consultation launched earlier this year. This follows recent updates relating to the EU's cybersecurity regulations, with the European Council formally adopting the second Network and Information Security Directive (NIS2 Directive) at the end of November 2022

WHAT IS THE BACKGROUND TO THE UK GOVERNMENT PROPOSALS?

In January 2022, the government launched a public consultation on proposals for legislation to improve the UK's cyber resilience, particularly in relation to organisations which play an important role in the UK economy, such as managed IT service providers (MSPs).

The proposals were to bring about these improvements through amendments to the Network and Information Systems Regulations 2018 (NIS Regulations), and included seven policy measures, split across two pillars, aimed at addressing the evolving cybersecurity threats faced by the UK.

The need for regulatory reform is demonstrated by a number of high-profile cyber attacks, including the December 2020 SolarWinds supply chain compromise, the May 2021 ransomware attack on the US Colonial Pipeline, the July 2021 attack on the managed service provider Kaseya and the attacks this year on the NHS 111 services and South Staffordshire Water. These have illustrated how

malicious actors are able to compromise a country's national security and interfere with its critical infrastructure, as well as causing significant economic harm and disruption.

WHAT ARE THE KEY PROPOSED CHANGES TO THE UK'S NIS REGULATIONS?

In summary, the proposed measures:

- 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 and 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
- strengthen existing incident reporting duties, currently limited to incidents that impact on service, to also include other significant incidents, and
- extend the existing cost recovery provisions to allow regulators (for example, Ofcom, Ofgem, and the ICO) to recover the entirety of reasonable implementation costs from the companies that they regulate.

The government's response to the consultation summarises:

- the feedback received on the proposals
- the government's responses to such feedback
- the confirmed next steps for policy development

It concludes that the government will proceed with all its original proposals and amend the NIS Regulations accordingly.

MANAGED SERVICES

Of the proposed measures, the most significant change is to broaden the scope of the NIS Regulations to catch additional digital service providers, primarily those offering managed services; these will now also be 'relevant digital service providers'(RDSPs) within the terminology of the NIS Regulations.

As a result of feedback received to the consultation and additional industry engagement, the government has tightened up the characteristics for 'managed services' to be brought in scope of the NIS Regulations. In particular, the changes clarify that in order to be within scope, the service must:

- relate to the provision of IT services—eg IT outsourcing services (ITO); Service integration and management (SIAM); Application management; Managed security operations centres (SOC); Security monitoring (SIEM); Threat and vulnerability management (TVM). This however takes non-IT services, such as business processing outsourcing (eg HR and payroll), out of scope; and
- provide regular and ongoing management support—this means that services which do not provide regular and ongoing support (eg software development or ad hoc consultancy services) will be out of scope; and
- be provided by one business to another—this takes internally-provided services out of scope (there is also no plan to include business-to-consumer services)

The government is not presently proposing to regulate data centres under this proposal. It should be noted, however, that (i) the government is keeping the inclusion of data centres in the NIS Regulations under review and (ii) some data centres may already be captured under the NIS Regulations as a result of their use by cloud service providers. Similarly, data centres may fall in scope indirectly, through forming part of the network and information systems that support the provision of a managed service or managed security service.

HOW DO THE REFORMS OF THE EU'S NIS2 DIRECTIVE COMPARE?

Expanded scope

Both the EU and UK reforms widen the scope of the existing regulation to make them applicable to a broader scope of sectors and entities including, in both cases, managed services providers. The EU's scope increases go further than the UK's proposals at present; however, the UK reforms include powers for the government to amend the NIS Regulations to add new sectors.

Incident reporting

Both the EU and UK reforms expand existing incident reporting requirements to include additional situations in which organisations have a duty to report. The EU's NIS2 Directive introduces a staged approach to incident notification. Initial notification (early warning) must be made without undue delay and within 24 hours of aware-ness of the incident at the latest, with further updates and information being provided in a second report which must be submitted without undue delay and in any event within 72 hours. There is no indication that the UK reforms will alter the existing 72-hour reporting deadline, making the EU regime more onerous as regards incident reporting.

Penalties for non-compliance

The EU's NIS2 Directive introduces uniform fine thresholds for non-compliance, with fines reaching up to (i) €10m or 2% of global annual turnover for 'essential entities'(defined in Article 3) or (ii) €7m or 1.4% of global annual turnover for 'important entities'. There is no indication that the UK reforms will increase the penalties for non-compliance above the current £17m threshold although the government has stated it will be aiming through its reforms to increase the ability of the regulators to recover their enforcement costs.

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

The timeline for implementation in the UK has not been announced, with the UK Government simply stating that the updates to the NIS regulations will be made 'as soon as parliamentary time allows'. Given current Government priorities, we would expect an updated regime to be in place no earlier than 2024.

The timing for implementation of the EU's NIS2 is somewhat clearer. NIS2 was adopted on 28 November 2022 and is expected to be published in the Official Journal of the European Union in the coming days. It will enter into force on the twentieth day following its publication and member states will have 21 months following its entry into force to transpose the directive into national law.

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Kate Brimsted

London

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