www.dlapiper.com /en-gb/insights/publications/2024/10/the-uk-cybersecurity-and-resilience-bill-a-different-approach-to-nis2-or-a-brit…

The UK Cybersecurity and Resilience Bill – a different approach to NIS2 or a British sister act?

1 October 2024

Introduction

It wouldn't be much of an exaggeration to say that NIS2 is the acronym on everyone's lips. When coupled with its European sister legislation DORA, we encounter a regulatory twosome that make GDPR feel like yesterday's news. And appropriately so. For the EU's second Network and Information Systems Directive (NIS2) and the Digital Operational Resilience Act (DORA) - respectively in force as of October 2024 and January 2025 – are rumbunctious in both their scope and ambition. Together they focus their attention on the omnipresent threat of cyber attack, significantly increasing their scope across multiple industries, increasing their fines, ramping up incident reporting and even signalling the levying of personal liability upon management bodies whose organisations fail to comply.

Yet across the channel in the UK, we remain onlookers to the storm of digital regulation erupting over Europe, with the impact of NIS2 and DORA only being felt by those UK organisations providing services into Europe. Many are nervous. As the UK limps on under the implemented version of the former NIS1 directive, we are daily witnesses to hostile cyber actors increasingly targeting our critical sectors and supply chains, including recent attacks on critical public services in the UK. These attacks highlight very publicly that the UK's core services and institutions remain painfully vulnerable to attack, with a regulatory cyber regime badly in need of updating to keep pace with growing threats.

It is perhaps with some relief then that one of the first moves of the new Labour Government was to announce its intention to legislate a new Cybersecurity and Resilience Bill in the next Parliament, a bill which looks set to increase the number of organisations falling within its scope, including supply chains, enhancing reporting obligations and placing regulators on a stronger footing to ensure essential cybersecurity measures are being implemented. So far…so EU, as the main features of NIS2 and DORA appear closely reflected in the UK's proposed Bill. Which leaves us to ask: what are the key differences and similarities between the new Bill and NIS2? Is this a new approach, or simply a British sister act?

How does the UK Cybersecurity and Resilience Bill compare to its NIS1 predecessor and the new NIS2?

In the much anticipated first King’s Speech of the new Labour Government on 17 July 2024, the monarch announced that the long anticipated Cybersecurity and Resilience Bill (CS&R Bill) would be amongst those new laws making their way onto Parliament's schedule for the next year. Six years on from the implementation of the NIS Regulations 2018 (NIS Regulations) which, in common with our fellow EU Member States of the time, was based on the EU's NIS1 Directive, the CS&R Bill recognises that the time is ripe for reform. While the NIS Regulations clearly took a step in the right direction to achieving a high level of cybersecurity across critical sectors, the new Bill recognises the need to upgrade and expand the UK's approach to keep in step with an ever-increased cyber threat.

But in the UK, we are not alone in recognising cyber as one of the most significant threats of our age. In the recitals to NIS2, the EU Commission notes that the "*number, magnitude, sophistication, frequency and impact of incidents are increasing and present a major threat to the functioning of network and information systems*" with the result that they "*impede the pursuit of economic activities in the internal market, generate financial loss, undermine user confidence and cause major damage to the Union's economy and society*". The EU's response was to enact a bolstered NIS2 which significantly expands the number of entities directly in scope; includes a focus on supply chains; enhances the powers of enforcement and supervision available to local authorities; steps up incident reporting obligations; and imposes ultimate responsibility for compliance at a senior management level. With DORA, the EU adds another layer of regulation, trumping the requirements of NIS2 for the financial services sector.

So how will the UK's new Bill compare? Although the wording of the Bill has not yet been published, this article looks at the initial indications released by Government to try and answer that question.

Expanding the Scope of Sectors Covered

One of the most critical changes introduced by the CS&R Bill is the expansion of sectors subject to cybersecurity regulation. The NIS Regulation currently applies to 5 main sectors:

(a) Energy (electricity, oil, gas);

(b) Transport (air, rail, water, and road);

(c) Health (healthcare providers and hospitals);

(d) Drinking water supply and distribution; and

(e) Digital infrastructure (internet exchange points, DNS providers, top-level domain registries)

as well as some digital services including online marketplaces, search engines and cloud computing.

This is a far more limited list than the one currently being implemented in the EU under NIS2. There, a dramatically expanded scope now includes some 18 sectors which include wastewater management, postal services, chemicals, manufacturing and food production. NIS2 even goes as far as including the space industry within its expanded remit, and importantly does not ignore ICT service management which, through broad and rather vague definitions, will include a large swathe of organisations falling within the categories of Managed Service Provider and Managed Security Service Provider. On the financial services side of the house, NIS2 applies to banking and financial infrastructure, but will largely be surpassed by DORA which will become law a few months later and applies similar cybersecurity requirements to a large number of financial services institutions together with their ICT service supply chains.

By comparison, we also expect that the UK’s new CS&R Bill will likely extend its coverage beyond the five sectors currently regulated under NIS1. While the precise details of the Bill have not been finalized, the language of the King’s Speech emphasises a focus on "*expanding the remit of the regulation to protect more digital services and supply chains* ". This suggests that sectors involving critical digital infrastructure and B2B ICT services will be prioritised. In particular, the UK Technology Secretary recently announced the UK government's decision to class UK Data Centres as 'Critical National Infrastructure' (CNIs). This means that the data centres sector can now expect greater government support in recovering from and anticipating critical incidents and appears to be a move to bridge one of the gaps between the NIS Regulations and NIS 2, which now classifies "data centre service providers" as "essential entities". However, the extent to which this CNI designation will bring data centres into the scope of the CS&R Bill remains to be seen. Financial services are, like DORA, expected to be covered elsewhere.

Incident Reporting

The incident reporting framework is another area where the UK's CS&R Bill is expected to align with NIS2. Under NIS1, entities have 72 hours to report a cybersecurity incident. However, it appears that, in line with NIS2, the UK government plans to shorten this window, particularly for critical entities. The King's Speech points to "*mandating increased incident reporting*" which would, logically, likely lead to stricter timing requirements to encourage this. NIS2 also imposes stricter reporting timelines, requiring entities to issue an early warning report within 24 hours of detecting a "*significant*" cybersecurity incident, with a first follow-up report required within 72 hours, followed by a detailed incident analysis within a month.

Additionally, the King's Speech highlighted ransomware as a key focus area, signalling that the UK will require reports to include an indication of where a company has been held to ransom - falling short of banning ransom payments as some commentors had speculated - helping to improve the UK's overarching understanding of threats, and potentially improve the prospect of a more co-ordinated response to the ransom demands.
Regulatory Oversight and Fines

The CS&R Bill is set to bring in enhanced powers for regulators, potentially mirroring NIS2's enhanced supervisory framework. A notable component of NIS2 is its move toward a more proactive regime, granting regulators the authority to conduct ad hoc audits, investigations, and inspections (albeit only for those entities classified as "essential") to ensure compliance with cybersecurity measures.

The UK government has echoed these priorities, aiming to give regulators greater powers to ensure essential cybersecurity measures are in place. The King's Speech also hinted at cost-recovery mechanisms, ensuring regulators have the necessary resources to enforce compliance. This may imply that larger fines for non-compliance are coming, similar to the hefty new penalties in NIS2, which allows fines of up to €10 million or 2% of global annual turnover (whichever is greater) for those entities classified as "essential" and €7 million or 1.4% of global turnover for those classified as "important" (although of course the levels of fines remains a matter of national implementation and may vary widely when Member States come to implement NIS2 into national law).

This will be seen as a clear attempt to harmonise and strengthen enforcement as a key facilitator to ensure effective cybersecurity risk management is adopted by critical services across the EU. It is therefore likely that the UK, with a similar concern for effective regulation, will follow suit.

Cybersecurity Standards and Measures

The NIS2 Directive outlines several key cybersecurity measures that entities must implement, including (amongst others):

- Policies on risk analysis and security of information systems;
- Incident handling;
- Supply chain security;

- Security in system development and maintenance;
- Cyber hygiene and cybersecurity training; and
- Use of multi-factor authentication and encryption.

While the UK has not explicitly stated whether it will adopt these exact measures or perhaps be more specific, the general thrust of the CS&R Bill seems to be moving in a similar direction. The UK government's consultation on cybersecurity in 2022 stressed the importance of robust cybersecurity practices, and the themes of the King's Speech suggest that similar measures, especially concerning digital infrastructure and supply chains, will form a core part of the new regime.

Overall, it is anticipated the new legislative provisions will set the baseline for cybersecurity risk management measures, operational resilience, and reporting obligations, across all relevant sectors.

Conclusion: A Hybrid Approach to Cybersecurity

While the UK will of course not directly adopt NIS2, the CS&R Bill marks a significant evolution from the current NIS Regulations and will likely share many of NIS2's core principles as both the UK and EU unite in a shared concern to more effectively manage and mitigate one of the greatest threats of our times. The UK's Bill, while not yet seen in draft, is expected to expand the range of regulated sectors, shorten incident reporting timelines, strengthen regulatory oversight, and impose stricter cybersecurity standards. Whilst we expect obvious UK-centric focuses and adaptions, the King's Speech makes it quite clear that the UK does not want to be left behind or be seen as more vulnerable to cyber threats once NIS2 has been implemented across the channel. Accordingly, it will be hard for the CS&R Bill not to draw significant inspiration from NIS2 if it wants to achieve similar or better outcomes.

With the increasing global threat of cyberattacks, the UK will undoubtedly be aiming to close the gap with the EU's NIS2, ensuring that its cybersecurity framework is just as robust and far-reaching. In doing so, the UK hopes to maintain a competitive edge, but to get there the requirements of NIS2 will undoubtedly colour the drafting canvas of the CS&R Bill. We wait to see how that Bill manifests when it is published, later in the Parliamentary year.

Given the developing regulatory landscape, it is essential for relevant businesses to monitor these changes, and audit / review existing operations and resiliency.