A new cyber order: inside the UK's Cyber Security and Resilience Bill

Pilar Arzuaga, Partner at McDermott, Will & Schulte, provides an overview of the new UK Cyber Bill and advises on what organisations need to do now in order to prepare

On 12th November 2025, the UK government introduced the Cyber Security and Resilience (Network and Information Systems) Bill ('the Bill') aimed at strengthening cyber resilience of organisations within key sectors in the UK. The Bill responds to a recent increase in cyber threats and intends to modernise and expand the existing UK cybersecurity regime under the Network and Information Systems Regulations 2018 (the 'UK NIS Regime').

The key change is that new categories of organisations, particularly managed service providers ('MSPs') and those providing data centre services, will now be brought within the scope of the UK NIS Regime. Further, the UK government will be granted the power to impose the application of the UK NIS Regime on entities it considers 'critical suppliers'.

The Bill is currently progressing through Parliament and is expected to become law in 2026. However, a number of requirements will be rolled out in phases via secondary legislation. The government has announced that consultations on these measures will also take place in 2026.

The Bill forms part of the government's broader strategy to enhance national cyber resilience, protect critical national infrastructure, and reduce systemic cyber risk across the economy. It reflects concerns expressed by UK regulators and government bodies that the current UK NIS Regime does not adequately capture the complexity of modern digital supply chains, nor the concentration of cyber risk arising from reliance on a small number of critical technology and service providers.

The Bill is also intended to bring the UK regime more closely into alignment with international standards and comparable frameworks, including the EU's NIS2 Directive, while retaining a UK-specific approach following Brexit.

What is the scope of the current UK NIS Regime?

As of today, the UK NIS Regime applies to the following types of organisation (if they meet the necessary conditions):

- organsiations operating in the energy, transport, drinking water, and healthcare sectors;
- the following digital-infrastructure providers: Domain Name System (DNS) service providers, Internet Exchange Point (IXP) operators, and Top-Level Domain (TLD) Name Registry operators; and
- organisations providing the following digital services: online marketplace, online search engines, and cloud computing services.

In practice, application of the current UK NIS Regime depends not only on the sector in which an organisation operates, but also on whether it meets certain thresholds and criteria relating to size, systemic importance, and the nature of the services provided in the UK. Where applicable, organisations may be designated as Operators of Essential Services ('OES') or as Relevant Digital Service Providers ('RDSPs'), each category carrying different but overlapping compliance and reporting obligations.

Which new entities will be covered by the UK NIS Regime once the Bill is enacted?

The Bill will expand the scope of the UK NIS Regime to include:

- data-centre operators and supporting infrastructure providers;
- MSPs that offer IT helpdesk and cybersecurity services; and
- entities referred to as 'large load controllers' managing substantial electricity demand in the context of smart infrastructure or connected systems (e.g., to support electric vehicle (EV) charging during peak times).

In addition, the Bill will grant the UK government the power to impose the application of the UK NIS Regime to other types of companies (referred to as 'critical suppliers'), to be designated by the UK government individually, if they meet the necessary conditions.

(Continued on page 4)

(Continued from page 3)

As announced in the policy papers accompanying the Bill, this power will be used to extend the application of the UK NIS Regime to those cloud suppliers operating in the UK healthcare sector that are not covered by it currently (the current UK NIS Regime excludes from its scope the smallest cloud computing services providers (i.e., those qualifying as micro or small enterprises)).

The proposed 'critical supplier' designation power is particularly significant, as it enables the UK government to respond dynamically to evolving cyber-risk landscapes and supply-chain dependencies. Rather than relying solely on sector-based classifications, regulators will be able to target individual organisations whose disruption could have a disproportionate or cascading impact on essential services, public safety, or economic stability. This may include technology vendors, software providers, infrastructure operators, or service providers that sit upstream of regulated entities and whose services are integral to the delivery of essential or digital services in the UK.

Are there any other changes?

Alongside extending the scope of the UK NIS Regime, the Bill will increase cybersecurity-related obligations, by implementing:

- a broader definition of reportable incidents (including events with potential to cause serious disruption);
- new two-stage incident-reporting obligations, with strict deadlines: initial notification within 24 hours, full report within 72 hours;
- a requirement to inform customers or users if their services/data are affected, if certain thresholds are met; and
- the UK government's ability to expand scope or update obligations over time via secondary legislation.

"The proposed 'critical supplier' designation power is particularly significant, as it enables the UK government to respond dynamically to evolving cyber-risk landscapes and supply-chain dependencies. Rather than relying solely on sector-based classifications, regulators will be able to target individual organisations whose disruption could have a disproportionate or cascading impact on essential services, public safety, or economic stability."

Finally, the Bill will also make changes to the enforcement framework by introducing a possibility of:

- fines up to £17 million or 4% of global annual turnover (whichever is greater) — for serious violations (including failures to notify reportable incidents);
- fines up to £10 million or 2% of turnover (whichever is greater) — for other material non-compliance (including failure to notify the competent authority of being designated as an operator of essential services (OES)); and
- periodic charges, daily fines, or additional enforcement measures — where violations persist or where regulatory directions are ignored.

These enforcement powers represent a material increase in regulatory risk and bring the UK NIS Regime closer in severity to data-protection enforcement under the UK GDPR. In addition to financial penalties, regulators will retain the ability to issue binding directions, conduct audits, and require remedial action. Senior management may therefore face increased scrutiny in relation to cyber-risk governance, decision-making, and accountability.

Cyber-security measures under the Bill

In addition to expanding the scope of the law and strengthening enforcement, the Bill reinforces existing expectations that in-scope organisations implement cybersecurity measures that are appropriate and proportionate to the risks they face. Rather than mandating a single technical frame-work, the Bill maintains a principles-based approach under which organi-sations are expected to assess risks to their network and information sys-tems and to put in place technical and organisational measures that are suitable in light of their size, activities, and the importance of the services they provide.

Unlike the EU NIS2 framework, which provides for detailed technical and organisational requirements to be set through EU-level Implementing Acts, the Bill does not establish a single equivalent mechanism for prescribing uniform technical standards. Instead, it enables cybersecurity expectations to be clarified or updated over time through secondary legislation, codes of practice, and sector-specific guidance.

Further, the Bill reinforces the importance of managing cyber risk across supply chains and third-party relationships. Considering the role played by managed service providers, cloud services, and other suppliers in supporting essential and digital services, organisations may be expected to demonstrate how cyber risk is identified, assessed, and addressed not only within their own systems, but also in relation to key service providers.

Governance and oversight considerations

While the Bill does not introduce an explicit statutory requirement for senior management or boards to formally approve cyber-security measures, it

strengthens the ability of UK authorities to assess compliance by reference to governance and oversight arrangements. This includes consideration of how cybersecurity risks are identified, escalated, and managed within the organisation, and whether responsibilities for cyber-security decision-making are clearly defined.

This governance-focused approach is consistent with broader international regulatory developments, which increasingly treat cyber resilience as an organisational risk rather than a purely technical issue. In practice, this may lead regulators to look more closely at whether cybersecurity measures are supported by appropriate internal processes, senior-level awareness, and documented accountability.

Organisations with operations in multiple jurisdictions may therefore find it helpful to ensure that cybersecurity measures are embedded within their broader governance frameworks, and that oversight and accountability arrangements are sufficiently clear to withstand regulatory scrutiny under different but related regimes.

How should you prepare?

Given the expanded scope, stringent reporting requirements and high potential penalties, organisations should consider taking these steps now:

- undertake a scope and exposure assessment to identify whether their services, infrastructure or supply-chain profile may bring them within the new regime;
- engage in monitoring the UK government proposals for secondary legislation, take part in consultations on issues impacting your organisation or sector;
- start building or strengthening a cyber-resilience compliance programme: including incident-response capacity, vendor and supply-chain oversight, logging and monitoring, backup/recovery, and governance mechanisms;
- be ready to update contracts and SLAs to embed compliance obligations down the supply-chain where relevant;
- prepare your business continuity and incident-response frameworks to meet tight reporting deadlines (24h initial / 72h full report); and
- engage senior leadership or the board early: treat cyber-resilience as a strategic imperative, not an IT-only concern.

Organisations with operations or customers across both the UK and EU should also consider alignment between UK NIS requirements and the EU NIS2 Directive, particularly where they are already investing in NIS2 compliance programmes. A coordinated approach may help reduce duplication, ensure consistency across jurisdictions, and support more efficient governance, reporting, and assurance processes.

Pilar Arzuaga
McDermott Will & Schulte LLP
parzuaga@mwe.com