SLAUGHTER AND MAY/

JULY 2025

WHAT WILL THE CYBER SECURITY AND RESILIENCE BILL MEAN FOR YOUR ORGANISATION?

The cyber threat landscape facing the UK's public and private sectors is "diffuse and dangerous" according to the National Cyber Security Centre, with persistent attacks from both hostile states and organised crime. Recent high profile ransomware attacks on UK retailers are a reminder of how disruptive such attacks can be to business operations. However, critical national infrastructure are regularly the target, and it is easy to see how a successful attack on a nuclear power station or water supplier could have a devastating impact on the country.

In response to the current cyber threat, the UK Government is progressing a number of legislative changes, including updating its cyber legislation for critical services (which includes certain IT services). The Cyber Security and Resilience Bill (**the Bill**), was first announced in the King's speech last July. While we await its publication, a government statement published this April provides some detail on what it will cover. The Bill will draw from both the EU's recent NIS2 Directive and consultations carried out by the previous government and aims to "strengthen the UK's cyber defences and build the resilience of [its] essential services, infrastructure, and digital services."

CURRENT REGULATORY FRAMEWORK AND ROAD TO REFORM

The UK's current Network and Information Systems (**NIS**) Regulations have been in force since May 2018 and are based on the EU's original NIS Directive. As well as requiring the UK government to take certain steps (for example to publish a NIS national strategy and designate a CSIRT) they impose security and incident notification obligations on in-scope organisations. These include:

- operators of essential services (**OES**) in five key sectors: transport, energy, drinking water, health, and digital infrastructure; and
- relevant digital service providers (**RDSPs**), which include search engines, online marketplaces and cloud computing services.

The regime is enforced by relevant sector regulators, with the ICO regulating RDSPs.

Both the UK and EU have been planning to update their NIS rules for some time now. While the regimes had helped increase the level of cyber security across critical sectors, incidents were not being reported, enforcement action was limited to non-existent, and changes were needed to keep pace with an evolving threat landscape.

The EU has now updated its NIS regime – NIS2 has applied in member states since last October. However, the UK's plans had somewhat stalled. Despite the previous UK Government proposing changes in 2022 following a consultation process, no bill or other legislative proposal was ever introduced.

On coming into power, the current Labour government picked up the mantle, and proposed the Cyber Security and Resilience Bill, building on the previous work carried out in both the UK and EU.

KEY PROVISIONS EXPECTED IN THE BILL

The Bill will strengthen the existing cyber rules for essential services, infrastructure, and digital services both by bringing more entities into scope and enhancing the powers of relevant regulators. It will also align, where appropriate, with the approach taken in the EU's NIS2 Directive – a stance that organisations with operations in both the UK and EU will welcome.

EXPANDED SCOPE

MSPs:

One of the key proposals of the Bill is to bring Managed Service Providers (**MSPs**) within scope of the regime. This means that MSPs would be regulated by the ICO and subject to the same obligations as other RDSPs. With an estimate 900-1100 providers being brought into the regulatory net, this will be a significant change – and one likely to have consequences for many other organisations using these MSPs (e.g. in their contracting or risk allocation).

It is a change that makes sense: MSPs can be an attractive target for cyber criminals given the access they can provide to their customers' systems and data, as demonstrated by a number of recent attacks. For example, the ICO fined Advanced Computer Software Group in relation to a ransomware attack impacting both its direct customers and the data subjects who are its customers' customers. Media reports also suggest that IT provider TCS is investigating whether it is involved in M&S's ransomware attack, and MSPs were infamously targeted with the Cloud Hopper attack.

A MANAGED SERVICE IS A SERVICE WHICH:

1. is provided to another organisation (i.e., not in-house);
2. relies on the use of network and information systems to deliver the service;
3. relates to ongoing management support, active administration and/or monitoring of IT systems, IT infrastructure, applications, and/or IT networks, including for cyber security, and;
4. involves a network connection and/or access to the customer's systems.

Note: the exact wording will be finalised with the Bill.

Data Centres:

The proposals also plan to bring data centres in scope. Last year they were designated as part of the UK's critical national infrastructure (the first CNI designation in almost a decade). The suggestion now is that the Bill will classify these centres as an essential service which, again, seems a sensible addition to the in-scope list given data centres underpin "almost all economic activity and innovation" in the UK. The April statement discussed setting thresholds based on the amount of data that is processed. Data centres above 1MW capacity will be in scope, unless they are enterprise data centres (i.e., solely managing the IT needs of their own business) in which case a higher, 10MW capacity, threshold will apply.

Designated Critical Suppliers:

Recognising the importance of addressing supply chain risk, the Bill will enable regulators to bring specific, high-impact suppliers to OES' and RDSPs in scope. They can by classified as "Designated Critical Suppliers", even where that supplier is an SME who would previously have been exempt. However, that supplier's goods or services must be so critical that its disruption could cause a significant disruptive effect on the essential services or digital service provider it supports. The supplier's goods or services must also rely on networks and information services. Given these thresholds, it is expected that this will only cover a small percentage of suppliers, particularly as it will not include suppliers who are already regulated elsewhere (for example, under the Communications Act 2003).

In addition, the government may be able to use secondary legislation to bring new sectors and sub-sectors in-scope of the regime and impose duties on OES and RDSPs to manage their supply chain. Regarding the latter, it will be interesting to see what these provisions cover given it can be difficult in practice for organisations to manage their supply chain, particularly beyond the first tier of suppliers.

How does this compare to NIS2?

The EU's NIS2 also expanded the number of sectors in scope and had a focus on managing supply chain risk. While it adopts a broader scope, covering 18 critical sectors (including MSPs, as well as food distributors and postal services), the UK's approach under the Bill is more selective and adaptable.

SECURITY

While NIS2 expressly includes a set of security requirements that organisations must follow, the Bill will enable the government (subject to ongoing consultation) to make regulations to update the existing security requirements in the NIS regime. This will include placing the National Cyber Security Centre's (**NCSC**) Cyber Assessment Framework on a firmer footing, making it easier (so the government says) for organisations to know what is required of them around security and for regulators to oversee the security requirements. While the framework has already been placed on a statutory footing for RDSPs, the Bill will enable its requirements to be updated, aligning them more closely with the security obligations set out in NIS2, and applying them where appropriate to OES.

INCIDENT REPORTING

The Bill will update and enhance the current incident reporting requirements for regulated entities. This is an important development given that many significant events currently go unreported.

The Bill will introduce a two-stage reporting structure for cyber incidents. Regulated entities will be required to notify their regulator, and (at the same time) the NCSC, 24 hours after gaining awareness of an incident. A detailed report must then be provided within 72 hours. Again, this aligns more closely with the provisions in NIS2, which has a similar early warning notification system.

The reporting thresholds will also be expanded. Currently an incident has to interrupt the continuity of the essential or digital services before it is reportable. Under the Bill this will be expanded to cover incidents that are capable of having a significant impact on the provision of relevant services, and that significantly affect the confidentiality, availability, and integrity of the system. These reforms intend to provide the government with more data, and therefore more understanding, around the cyber threats organisations are facing. The Bill will also introduce transparency obligations, which will require digital services and data centres to alert affected customers.

EXPANDING ICO POWERS AND PUBLISHING REGULATORY OBJECTIVES

The Bill intends to place regulators on a stronger footing, providing them with more powers and enhanced oversight of the cyber risk. The ICO, as the regulator of RDSPs (including MSPs), will have more authority to collect information from those entities. This is consistent with the theme of enhancing the flow of information to government agencies and regulators. The stated aim is not just to enable the ICO to take a more proactive approach to enforcement, but also to allow it to mitigate risks and prevent attacks. Changes will include an expanded duty for RDSPs to share information with the ICO when they register with it, together with powers to enforce a failure to register. The criteria for the ICO to be able to serve information notices will also be expanded.

In recognition of the fact that taking a proactive supervisory approach incurs additional costs, the government also intends to improve the regulators' cost recovery regime. This may include better enforcement related cost recovery. It may also allow regulators to set a fees regime and place a duty on regulated entities to pay the fee, all ensuring the costs of an increased regulatory burden does not fall on the tax payer.

Potentially more welcome is the suggestion that the government is considering including a new power for the Secretary of State to publish a statement of strategic priorities for regulators. This draws from existing regulatory regimes, such as those for telecoms and online safety, and will provide a unified set of objectives and expectations for the twelve sector regulators who enforce the NIS regime.

REGULATORY AGILITY AND DELEGATED POWERS

Recognising the dynamic and shifting nature of cyber threats, the Bill will build in regulatory flexibility through the use of secondary legislation (if necessary). The Secretary of State will be empowered to, for example, bring new sectors within the scope of the regulation without an Act of Parliament, subject to certain safeguards. These may include ensuring appropriate consultation is being undertaken.

The purpose of this reform is to ensure that the regulations are not stagnant, and that the government can act against any new and emerging threats without the need for new primary legislation. In comparison, NIS2, while broader in scope, is less agile procedurally.

The Bill may also grant the secretary of state a new power to issue directions directly to regulated entities and regulators (for example to take action to address a cyber threat) on national security grounds. This will enable swift action in response to a cyber threat where there is a significant threat to national security.

WHAT DOES THIS ALL MEAN FOR ORGANISATIONS?

While only certain sectors will be in scope of the updated NIS regime, this Bill is relevant to all organisations given their reliance on MSPs and other critical service providers.

For those organisations:

- previously in scope, it will be important to understand where existing processes will need to change – for example, preparing for a 24, rather than just 72, hour reporting obligations;
- new to the regime, it will be important to understand what new obligations the Bill imposes, and how these fit with existing, but similar, obligations under other regimes such as the GDPR; and
- not directly in-scope, but reliant on service providers who are regulated, it will be important to consider whether these new rules will impact their procurement practices and contractual provisions. For example, will such organisations want to be notified if their MSP suffers a reportable incident under the new rules set out in the Bill, and will this impact the due diligence they carry out on their MSPs?

COMMENT

The Bill represents a notable effort to enhance the UK's cyber security position and keep pace with changes already made by the EU. While any alignment with the EU's regime will be welcomed by organisations with operations on both sides of the channel, the Bill does not currently look like it will adopt all of NIS2's changes – for example, NIS2 introduced management body liability in certain circumstances, which was not discussed in the April statement relating to the Bill. However, like NIS2, the Bill does expand the scope of the existing regulation, focus on security and supply chain risks, and empower regulators to proactively manage cyber risk in their sectors, all of which should enhance protection for the UK's critical infrastructure and key digital services.

The Bill is also one of a number of legislative changes currently being progressed by the UK Government to increase the UK's cyber resilience, from cyber related changes to the Corporate Governance Code and guidance, to new proposals around ransomware payments. These developments, together with a number of recent ICO fines linked to cyber breaches, all reflect the commitment of both the UK government and its regulators to tackle the evolving cyber threat.

RICHARD JEENS
Partner
+44 (0)20 7090 5281
richard.jeens@slaughterandmay.com

NATALIE DONOVAN
PSL Counsel
+44 (0)20 7090 4058
natalie.donovan@slaughterandmay.com

TAYLA BYATT
Associate
+44 (0)20 7090 3123
tayla.byatt@slaughterandmay.com

GET IN TOUCH

Cyber incidents rarely respect legal or operational borders. Our team of multidisciplinary experts help our clients globally on all legal and operational issues. We advise on the full spectrum of cyber issues, from cyber preparedness to incident response. To find out more, get in touch with a member of the Cyber Hub or your usual Slaughter and May contact.

This article was written by
Richard Jeens, Natalie Donovan and Tayla Byatt.

A version of this briefing first appeared in the Privacy Laws & Business UK Report, Issue 140 July 2025.

This material is for general information only and is not intended to provide legal advice. For further information, please speak to your usual Slaughter and May contact.