Safeguarding Critical Infrastructure and Digital Services — recent UK and EU developments

Peter Warcup, Associate, and Nina Lazic, Partner, at Osborne Clarke LLP, consider what we can anticipate from the recently announced UK Cyber Security and Resilience Bill and the product of the European Commission's consultation on the draft NIS2 implementing regulation

It has been a busy few months for cyber-focused regulation. On 17th July 2024, in its maiden King's Speech, the new UK government introduced the Cyber Security and Resilience Bill ('the Bill'), intended to "strengthen [the UK's] defences and ensure that more essential digital services than ever before are protected". In the EU, as the implementation deadline for the revised Network and Information Systems Directive ('NIS2') inches ever closer, the European Commission ('the Commission') published a draft implementation regulation ('the draft Regulation') and held a consultation for organisations, government bodies and individuals, which closed on 25th July 2024.

Given the thin detail in the Bill, this article considers what we might expect from its later iterations and examines the draft Regulation in light of the Commission's recent consultation.

The current UK regulatory framework

At present, UK regulation concerning cybersecurity and the resilience of critical infrastructure and digital services is, largely, covered through data protection legislation and the predecessor to NIS2, the Network and Information Systems Directive ('NIS1'), which remains in force in the UK following its withdrawal from the EU. Sector level regulation and guidance may also be relevant, depending on the sector in which an organisation operates.

The UK GDPR and the Data Protection Act 2018 are, amongst other things, concerned with ensuring that personal data are processed in a manner which ensures their integrity and confidentiality. Within these confines, the legislation is applicable to cyber security and resilience, but its scope is limited and it does not apply where personal data are not involved.

NIS1, which came into force in the UK in May 2018, aimed to strengthen cybersecurity capabilities and mitigate threats to the systems used to provide services essential to the UK economy, including energy, transport, health, water, and a narrow selection of digital infrastructure and digital service providers. In-scope organisations are subject to incident reporting obligations and are required to put in place appropriate security measures (which may go beyond the standard expected under the UK GDPR). As with data protection legislation, NIS1 is largely outcome-based, setting out high-level objectives, rather than prescriptive security requirements.

Background to the Bill

The introduction of the Bill follows a series of high-profile cyber-attacks which impacted critical UK institutions, including the NHS, local government, the Ministry of Defence, the British Library, the Electoral Commission and Royal Mail. The National Cyber Security Centre has also repeatedly warned of the increasing threat to critical national infrastructure from hostile nation states and state-sponsored actors.

Despite the importance of the services affected by recent attacks, many impacted organisations fall outside the narrow scope of NIS1. Even where NIS1 applies, there are concerns that changes are not being implemented swiftly enough to address the escalating threat. The UK's second post-implementation review of NIS1, published in March 2022, found that, while the regulations had driven some improvements, progress in protecting essential services was limited. At that time, only 51% of operators of essential services had updated or strengthened their policies and processes following the introduction of NIS1.

So how was the previous government addressing these concerns?

In November 2022, the Department for Digital, Culture, Media & Sport published its response to a public consultation on proposals to enhance the UK's cyber security framework. The measures considered included expanding NIS1 to cover additional digital services providers, increasing incident reporting requirements, and allowing ministers to amend NIS1 through secondary legislation.

(Continued on page 14)

(Continued from page 13)

Following this, in December 2023, the Department for Science, Innovation and Technology launched a consultation on proposed regulations to address cyber security threats and improve the resilience of the UK's data infrastructure.

Alongside the government's efforts, the Joint Committee on the National Security Strategy conducted an extensive inquiry into ransomware, which proposed numerous measures to better understand and combat the threat of ransomware. The government provided its response to the Committee's proposals in March 2024.

On 21st May 2024, it was reported that the government would be launching a consultation to gather views on proposals for the mandatory reporting of ransomware incidents, a licensing regime for extortion payments and a complete ban on ransomware payments by operators of critical national infrastructure.

However, on 22nd May 2024, Rishi Sunak announced the snap general election, which prevented the latest consultation from progressing and meant that any proposals did not, ultimately, make their way onto the legislative agenda before the election. The Labour Party's manifesto had little to say on cybersecurity and indicated only that cyber-attacks would be considered as part of their proposed Strategic Defence review. The incoming government, nonetheless, moved swiftly to table the new Bill, with Science Secretary Peter Kyle warning, in a recent press interview, that the UK is "desperately exposed" to cyber threats, claiming that national resilience had suffered "catastrophically" under the previous government.

The Bill

Currently, there are limited details available about the specific provisions of the new Bill. However, the proposals include:

- expanding regulation — broadening the scope of the existing regulatory framework to cover more digital services and supply chains, ensuring a wider range of organisations are protected;
- strengthening regulatory powers — enhancing the authority of regulators to ensure that safety measures are being effectively implemented. This may include mechanisms for cost recovery to provide resources to regulators, and giving regulators powers to proactively investigate potential vulnerabilities; and
- mandating incident reporting — requiring organisations to report incidents, including where they have been held to ransom, to provide the government with a greater understanding of threats.

> ***"In the EU, NIS2 goes much further in expanding its scope to cover new sectors and new digital services… It would not, therefore, be surprising if future versions of the Bill are augmented to ensure NIS1 has a comparable scope."***

What might future iterations of the Bill cover?

The Bill proposes to expand NIS1 to "protect more digital services and supply chains", however, it is unclear what this will look like in practice. The previous government's November 2022 consultation proposed to expand NIS1 to make a wide range of managed service providers subject to the same duties as digital service providers. This would potentially have included certain providers involved with workplace services, WAN (Wide Area Network) and LAN (Local Area Network) support services, online security or technology advisory services, various IT security services, business process and IT outsourcing, service integration and management, analytics and artificial intelligence, business continuity and disaster recovery services and some software engineering providers.

The government could simply pick up where the previous government left off, but there are some indications that the Bill could go further than the earlier proposal, by expanding NIS1 to cover additional sectors. The briefing note accompanying the Bill references recent attacks affecting essential public services and infrastructure, but the entities in those sectors would not be directly covered if NIS1 was only updated to cover additional digital services. The briefing note also expresses concern that the UK regulations have been superseded in the EU and so require urgent updates to ensure that the UK's infrastructure is not comparably more vulnerable.

In the EU, NIS2 goes much further in expanding its scope to cover new sectors and new digital services. This includes, inter alia, public administration entities (as defined by individual Member States), space-based services, postal and courier services, waste management, chemical businesses, food businesses, manufacturing and research. It would not, therefore, be surprising if future versions of the Bill are augmented to ensure NIS1 has a comparable scope.

As evidenced by recent supply chain attacks affecting the NHS and Ministry of Defence, the security of supply chains remains an area of particular concern. NIS1, in its current form, does not apply directly to the supply chains of in-scope organisations and it is up to those organisations to make sure that they put in place appropriate processes and contractual controls to ensure that their suppliers' security measures are suitable. By including additional digital services within the scope of NIS1, many suppliers with an elevated cyber risk would be captured and directly subject to formal security requirements.

The Bill also seeks to address concerns that in-scope organisations are not fully implementing the requirements of NIS1. The new proposals will give regulators the teeth to be able to ensure compliance, through a combination of proactive investigation and an as-yet-unspecified power to recover costs. This does, however,

fall somewhat short of the powers granted by NIS2, which imposes direct obligations and liability on senior management of in-scope organisations. Likewise, as many UK regulators already actively monitor compliance, it will be interesting to see if later versions of the Bill strengthen regulators' powers further.

The Bill also includes a proposal to mandate the reporting of incidents, including where an organisation has been subject to a ransom. It is not yet clear what the threshold for notification would be (or how it would differ from the existing NIS1 reporting requirements), but the briefing note suggests that this will expand the type and nature of reportable incidents.

Finally, as this is a Bill nominally concerned with 'resilience', it is worth considering whether the current approach might be updated to reflect wider threats to resilience. Although NIS1 is concerned with physical and environmental factors, it remains primarily focused on cybersecurity measures. As we have seen from the recent CrowdStrike incident, non-cyber events can have a significant impact on the resilience of providers of critical services. In contrast, NIS2 takes a much more expansive 'all-hazards' approach which, as set out in the draft Regulation, considers events including natural phenomena, fire, theft, flood, power failure and human error. It is possible that the UK might emulate the approach being taken in the EU.

The draft Regulation

EU Member States have been given until 17th October 2024 to incorporate NIS2 into domestic law. As part of the implementation process, the European Commission published a draft Regulation alongside a consultation on the draft. The draft Regulation applies only to certain categories of digital infrastructure, ICT service management and digital service providers (referred to as 'relevant entities').

The draft Regulation provides both general and sector-specific thresholds for determining when an incident should be considered 'significant' for the purposes of triggering reporting obligations under NIS2. The general criteria which identify an incident as being significant include, among other things, where:

- the incident causes or has the potential to cause financial loss for the relevant entity exceeding either €100,000 or 5% of the entity's annual turnover;
- the incident causes or has the potential to cause considerable reputational damage (which includes where the incident has been reported in the media, where the incident has resulted in complaints, or where the entity is likely to lose customers with a material impact on the business);
- the incident leads to the exfiltration of trade secrets; and
- incidents that were not individually considered significant have occurred at least twice within six months and have the same apparent root cause.

The draft Regulation also sets out 26 pages of highly prescriptive risk management measures for relevant entities, which flesh out the technical and methodological requirements set out in Article 21(2) NIS2.

Consultation on the draft Regulation

The European Commission's consultation closed on 25th July 2024, having generated 154 responses. It appears from the responses that the draft Regulation is not without its critics.

Respondents are particularly concerned about the thresholds for determining whether an incident was significant (and thus, notifiable). For example, respondents consider that the measure of reputational damage and the criteria for recurring incidents lacked a de minimis threshold, which could lead to over-notification.

More generally, there is concern that it may be impractical for relevant entities to implement the detailed risk management requirements by the intended adoption date.

NIS2 requires the European Commission to adopt the final version of the implementing regulation before 17th October 2024, so it remains to be seen whether it will be amended to reflect the concerns raised in the consultation.

What can organisations do to prepare for the incoming legislation?

Organisations should carefully assess if they are likely to fall within the scope of the proposed UK and EU legislation. If they are, it would be advisable to prepare in good time to ensure that the organisation is able to meet its obligations under the relevant legislation. This continues to be a fast-moving and increasingly fragmented regulatory environment, so organisations should also continue to keep abreast of key developments in relevant sectors and jurisdictions. This journal will continue to track the developments closely.

Peter Warcup and Nina Lazic
Osborne Clarke LLP
peter.warcup@osborneclarke.com
nina.lazic@osborneclarke.com