PHILIPLEE

Recent observations on the National Cyber Security Bill 2024 & NIS2

Ireland's transposition of the NIS2 Directive is taking shape through the National Cyber Security Bill 2024, which both implements core EU obligations and re casts the National Cyber Security Centre (NCSC) on a statutory footing. While much of the scheme mirrors NIS2's minimum standards on risk management, reporting, as well as supervision and enforcement, several Heads of the Bill represent policy choices that extend far beyond the Directive's baseline.

I had the pleasure of appearing before the Joint Committee on Justice, Home Affairs and Migration last week to discuss above as well as the future of cybersecurity in Ireland in the context of the General Scheme of the National Cyber Security Bill 2024.

Policy Creep

For regulated entities, the most concerning divergences lie in the breadth of the NCSC's mandate and investigatory powers, the handling of data (including personal data), and the enforcement architecture. This article highlights those areas of possible "policy creep" as well as highlighting the practical implications for boards and compliance teams.

The Bill designates the NCSC as a CSIRT, a single point of contact, and an authority for cyber crisis management, but goes further by embedding the NCSC as an executive office under ministerial authority with an express national-security mandate. Amongst the NCSC's proposed statutory functions are a number that go far beyond the strictures of the NIS2 Directive, including:

- the unilateral power to disconnect companies from the Irish network for very vague reasons including acts of foreign or domestic interference that involve a threat to any person, device or essential service; and
- monitoring foreign information manipulation and interference.

These powers exceed NIS2's internal-market-oriented scope and suggest an integrated security model in which the NCSC straddles incident response, regulation, and national security support. This model is reinforced by ministerial direction powers under which the Minister may issue binding written directions, assign additional tasks by order, and require reporting from the NCSC.

Compliance via Technical Standards

Following on from the above, there still remains uncertainty in the market as to the measures that should be adopted by companies in working towards full compliance with NIS2. The NIS2 Directive's shift away from pure organisational and non-technical approaches, toward mandatory technical standards, is sensible and the NCSC's proposal to adopt the CyFun framework provides a structured, risk-based method for assessing maturity and preparing organisations for NIS2. In addition, there is a growing consensus that ISO 27001 certification should be the foundation for achieving and evidencing NIS2 compliance. Its alignment with NIS2 has already led to formal recognition in several Member States, including Belgium, where ISO 27001 is explicitly accepted as proof that "essential" and "important" entities meet NIS2 cybersecurity requirements.

Summary

The current draft of the Bill includes policy choices that extend far beyond the Directive's baseline including particularly the breadth of the NCSC's mandate and investigatory powers. All private and public sector bodies within scope of the NIS2 Directive will be hoping that future drafts of the Bill will bring these powers into line with the wording and aims of Directive.

More generally, the NCSC's ability to take proactive security steps, to seek time-limited, court-authorised network visibility, and to process and share data within a defined, security-centric legal framework are key considerations for regulated entities. Boards should ensure their risk management, legal, and privacy functions are aligned on these features, that contractual arrangements with DNS operators and registrars and data centre providers anticipate NCSC requests and that playbooks incorporate proactive engagement with the NCSC where scanning, sensor deployment, or DNS actions arise.

Finally, as discussed in previous posts, senior management accountability is real-training oversight records, and demonstrable follow-through on audit recommendations will be critical in any supervisory review or enforcement scenario – the days of the Board firing the CISO in the event of a cyber event are over.

Key contacts:

SEAN MC ELLIGOTT
PARTNER
smcelligott@philiplee.ie
+353 1 237 3700