Ibec Opening Statement to Joint Oireachtas Committee on Justice, Home Affairs and Migration in relation to the General Scheme of the National Cyber Security Bill 2024

Erik O'Donovan, Head of Digital Economy Policy, Ibec

25/11/2025

Cathaoirleach, members of the Committee, thank you for the invitation to appear today on behalf of Ibec, the group that represents Irish business. I am joined by my colleague Áine Clarke. We are both from Ibec's digital policy team.

In October 2024, we made a submission on the General Scheme of the National Cyber Security Bill, which has been shared with the Committee. We welcomed the publication of the General Scheme as a vital step in transposing the NIS2 Directive. NIS2 is an update of the first Network and Information Security Directive (NIS), which was the first European Union-wide cybersecurity law. NIS2 will introduce much stricter requirements, covering many more organisations and sectors. This reflects the changing world around us, where we see increasingly frequent and sophisticated cyber-attacks, with cybersecurity and resilience growing in importance.

Why cybersecurity matters and Ireland's opportunity

Cybersecurity is an economic and social imperative and an opportunity for Ireland, particularly given the amount of EU data we host here (over 30% according to the National Cyber Security Centre). It is fundamental to safeguarding trust in our digitalised economy and protecting our critical infrastructure. This Bill is not just an opportunity to lift the national baseline for cybersecurity; getting this right is an opportunity for Ireland to enhance our competitiveness and resilience, for the benefit of Irish society.

The impact of NIS2 on Irish business will be significant. Less than 150 organisations were in scope of the first NIS Directive. It is estimated that over 4,500 organisations will be directly in scope of NIS2, with many more indirectly affected by the requirements on in-scope organisations to manage the cybersecurity of their supply chains. For many of these businesses, NIS2 will mark a step-change in how cybersecurity is treated within the organisation. It is no longer just an IT issue but a board-level concern.

To ensure its success, we believe the Bill must be considered within the broader context of cybersecurity in Ireland. Ibec wishes to focus on four important areas: skills; developing our cyber industry; supporting business adoption; and related issues in the General Scheme.

1. Skills

First, the cybersecurity skills challenge. A lack of cybersecurity readiness, particularly among SMEs, directly impacts the ability of businesses to understand and comply with their regulatory obligations. According to Eurostat, almost one in four (24%) companies in Ireland have reported difficulties recruiting staff with the necessary cybersecurity skills**.** At the moment, we simply do not have enough skilled professionals to meet the surge in demand the National Cyber Security Bill will create. We would implore the Committee to consider directing some of the €2 billion surplus of the National Training Fund towards cybersecurity and other digital skills.

The skills question also extends to regulators. Ibec strongly supports the continued expansion and resourcing of the National Cyber Security Centre. However, the Bill also designates sectoral regulators, many of which will be supervising cybersecurity for the first time. It is critical that these bodies are sufficiently resourced, not just with funding, but with the technical expertise needed to provide guidance to businesses.

2. Developing our cyber industry

Secondly, the increase in cyber regulation in the EU – including NIS2 – presents a significant opportunity for the growth of our cybersecurity sector, as more regulated entities will mean more demand for cybersecurity products and services. Our cybersecurity sector is already a major contributor to the economy, comprising over 500 firms and generating €2.7 billion in annual revenue. NIS2 can solidify Ireland's position as a leading digital regulatory hub (a Programme for Government goal), but it will require greater prioritisation and investment in cybersecurity by Government, particularly in R&D. We urge the Government to deliver on its Programme for Government commitment to establish a dedicated, brick-and-mortar Centre of Excellence for cybersecurity, for the development of our cyber industry.

3. Supporting business adoption

Thirdly, we believe there is an urgent need to support business adoption. NIS2 requirements are far reaching, and organisations will face significant new compliance costs, including but not limited to security audits, technology upgrades, and essential training for staff. We welcome the SME cyber improvement grants that have been offered by the NCSC to date and call for additional dedicated and accessible streams of grants and vouchers to help organisations to increase their cyber resilience.

4. Matters related to the General Scheme

Lastly, I would like to raise several issues we mention in our submission. In transposing NIS2 into Irish law, we should align with the EU text and avoid gold-plating for coherence and certainty. Any costs levied on organisations should also be proportionate and take account of the financial cost of complying with the law. Many

important details necessary for complying with NIS2 have been omitted from the General Scheme, and further guidance will certainly be needed on areas such as the supply chain and the interplay between NIS2 and other laws.

As we await the enactment of the Bill, resources like the Cyber Fundamentals certification scheme and the ISO27001 standard are very important for business in plugging the gap. It is important that these standards are technical and non-discriminatory, meaning that they are based purely on objective criteria, such as performance, functionality, and security outcomes. They should also apply equally to all vendors or market participants. This concept is the bedrock of global digital trade.

Conclusion

In conclusion, we would like to stress from the outset that Ibec supports the broad aim of NIS2 to raise the common level of cybersecurity across the EU. However, we are now more than one year on from the transposition deadline, and businesses lack clarity on their regulatory obligations. We therefore urge Government to commit all the resources necessary to enacting the Bill as quickly as possible to provide certainty for businesses and regulators alike.

We look forward to working with the Committee and other stakeholders to increase Ireland's cybersecurity and resilience. Thank you.