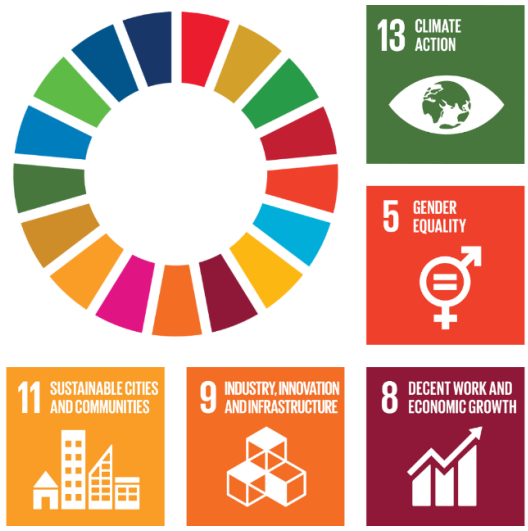
Chambers Ireland
Advancing business together



Consultation on the Third National Cybersecurity Strategy

Submission by Chambers Ireland

May 2026

Contents

About Chambers Ireland

Chambers Ireland is an all-island business organisation with a unique geographical reach. Our members are the Chambers in the cities and towns throughout the country – active in every constituency. Each of our member Chambers is central to their local business community and all seek to promote thriving local economies that can support sustainable cities and communities.

Key Points

- There is a need for the development of a strong and resilient national cybersecurity framework, aligned with protecting society and enabling innovation.
- Businesses particularly SMEs are increasingly exposed to cyber risks but often lack the resources, expertise, and clarity needed to respond effectively.
- The success of the Strategy will depend on its ability to translate national ambition into practical, accessible supports for enterprise, especially smaller firms.
- There are persistent gaps in cyber skills, coordination, and enterprise capability that must be addressed to strengthen resilience.
- Implementation of major regulatory changes (e.g. NIS2, Cyber Resilience Act) must be proportionate, coordinated, and clearly communicated to avoid unnecessary burden on business.
- A whole-of-government, risk-based approach is needed, integrating cyber security into broader enterprise, innovation, and economic policy.
- Structured public–private collaboration is critical, as businesses often identify emerging cyber risks earlier and can enhance national situational awareness.
- Improving resilience requires timely information sharing, accessible guidance, and continuous engagement between Government, regulators, and industry.

Introduction

We welcome the opportunity to contribute to the development of the third National Cyber Security Strategy. As the voice of business across the country, our network represents firms of all sizes and sectors, including a significant proportion of SMEs who are increasingly exposed to cyber risks.

We support the Government's ambition to develop a secure and resilient digital infrastructure that protects society while fostering innovation and a strong cyber ecosystem. However, the effectiveness of the next Strategy will depend on its ability to translate national-level ambition into practical supports for businesses, particularly SMEs.

It will also be important to ensure that regulatory developments such as NIS2 and the Cyber Resilience Act are implemented in a proportionate and coordinated manner. There is also a problem with persistent gaps in skills, sectoral coordination, and enterprise capability which need to be adequately addressed.

Key Priorities for Strengthening Cyber Resilience

Supporting SMEs and Enterprise Readiness

The consultation rightly identifies SMEs as a priority cohort requiring targeted support. While progress has been made under the previous Strategy, particularly in regard to the introduction of grant supports and awareness programmes, many SMEs continue to face problems. These include limited internal expertise, cost barriers to implementing cyber security measures, and uncertainty around compliance obligations under NIS2.

As a result, we would recommend expanding and simplifying financial supports for SME cyber investment, providing clear, sector-specific compliance guidance aligned with NIS2 requirements, and scaling trusted certification frameworks (e.g. Cyber Fundamentals) to create accessible baseline standards for SMEs

Strengthening National Cyber Capacity and Skills

The need to invest in national cyber capacity and skills is a central recommendation of the National Cyber Risk Assessment. Despite progress under the outgoing Strategy (e.g. education initiatives and industry engagement), gaps remain in a number of areas. There is limited availability of skilled cyber professionals, Industry–academia collaboration could be expanded, and SME's require increased access to training and upskilling.

We recommend the establishment of a coordinated national cyber skills pipeline which is properly aligned with industry demand. In addition, increased funding should be made available for applied research and industry partnerships. This should include leveraging existing workplace learning structures, such as Skillnet Ireland, to deliver flexible, employer-led cyber upskilling programmes targeted at SMEs[1].

Enhancing Coordination and Information Sharing

The expansion of coordination networks such as CORE structures has been a positive development under the previous Strategy.

However, further work is needed to extend coordination mechanisms to private sector stakeholders, particularly for SMEs. It is also important that action is taken to improve real-time information sharing on threats and vulnerabilities. In addition, we should work to strengthen collaboration across sectors facing new regulatory obligations.

We would recommend the formalisation of structured engagement channels between Government, regulators, and business representative bodies. Businesses often detect cyber risks and vulnerabilities earlier than the State, and formal engagement channels can improve

[1] https://www.skillnetireland.ie/

national situational awareness[2]. Many jurisdictions already emphasise public-private partnerships in cyber-security strategy[3]. We should also ensure SMEs, who are disproportionately vulnerable, have access to timely and actionable threat intelligence.

Regulatory Environment and Implementation

Proportionate Implementation of NIS2

The transposition of the NIS2 Directive represents a significant expansion in regulatory obligations across sectors. The objective of raising security standards is laudable and necessary, but certain strictures should be met to ensure effective implementation. Demands made on businesses should be proportionate to their size and appropriate to the level of risk. It should avoid duplication across regulatory regimes and provide clarity on responsibilities and enforcement.

As such, we recommend the early publication of detailed implementation guidance and a phased approach to compliance for smaller entities. Additionally, there should be strong alignment between NIS2 and other frameworks, including certification schemes.

Cyber Resilience Act and Supply Chain Security

The consultation highlights the importance of implementing the Cyber Resilience Act and securing supply chains. This will have implications for businesses across manufacturing, digital services, and critical infrastructure. There should be clear guidance for businesses on product-

[2] https://www.moodys.com/web/en/us/insights/public-sector/enhancing-national-security-with-public-private-partnerships.html

[3]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf?_hsenc=p2ANqtz-834pnw7jEBtoQS9F5KIgHNWU3u9BXkByfXMB2v2z3KZSLsrD16jNG13Co0Sm093Y-3VpLQ

level obligations under the Act, and support mechanisms to help firms adapt to new requirements.

Additionally, there should be an integration of supply chain security measures into broader enterprise support programmes. One of the main reasons for this is that cyber attackers increasingly target suppliers, who may be regarded as a weak link, to access larger businesses[4]. This also has the benefit of avoiding building parallel cybersecurity outreach structures.

Questions

Vision for a third national cyber-security strategy

How can we achieve our vision and how should we approach these recommendations, in your view?

We support the overall direction of these recommendations. To achieve the Strategy's vision, implementation should be guided by a clear focus on coordination, practicality, and proportionality. This means translating national objectives into actions that are accessible to businesses, particularly SMEs, supported by clear guidance, timely information sharing, and mechanisms for ongoing engagement between Government, regulators, and enterprise.

These recommendations should not be pursued in isolation. Strengthening visibility and detection, enhancing resilience, building cyber capacity, and securing supply chains are closely connected and should be delivered through a coherent whole-of-government approach. This should include sustained investment in the National Cyber Security Centre, stronger public–private collaboration, a coordinated national cyber skills pipeline, and the integration of cyber security considerations into broader enterprise and innovation supports.

The approach should also be risk-based and proportionate. For business, especially smaller firms, the success of the Strategy will depend not only on ambition at national level but on

[4] https://riskledger.com/resources/why-hackers-target-supply-chains

whether firms can access the guidance, training, financial supports, and regulatory clarity needed to improve cyber resilience in practice.

What key issues are not called out in this document or the National Cyber Risk Assessment but would be essential to raising the general level of cyber security resilience in Ireland?

In addition to the priorities identified in the consultation and the National Cyber Risk Assessment, greater emphasis should be placed on structured public–private engagement, proportionate implementation support for business, and the integration of cyber security into broader enterprise policy. These issues are essential to ensuring that cyber resilience is not treated solely as a technical or state-led issue, but as a practical business and economic priority.

There should also be a stronger focus on supply chain resilience, particularly for SMEs, and on ensuring that smaller firms can access timely, actionable threat intelligence and practical compliance guidance. Finally, while specialist cyber skills are important, wider workforce awareness and cyber hygiene across businesses and the public should be recognised as a foundational part of national resilience.

National Cyber-security Strategy 2019-2024

What are your views on the below propositions as priorities in relation to strengthening Ireland's cyber security resilience? Are key priorities missing?

We broadly supports the priorities identified, particularly those that strengthen SME readiness, cyber skills, public awareness, and national coordination capacity. These are important foundations for improving cyber resilience across the economy and society. We would like to see a strong emphasis on how these priorities will be implemented in practice. As mentioned above we consider structured public–private engagement, proportionate regulatory implementation, and stronger support for supply chain resilience to be of high importance.

How should these goals be approached to maximise the chances of success?

These goals should be approached through a coordinated, practical, and risk-based implementation framework. Success will depend on clear ownership across Government,

sustained engagement with business and other stakeholders, and the provision of accessible guidance and support to help organisations translate strategic objectives into action. Progress should also be supported by regular review, measurable outcomes, and sufficient investment in national cyber capacity. As we have mentioned above SMEs have a particular vulnerability to cyber security threats and we think it's important that the Strategy strengthens resilience across the wider economy rather than only among the largest or most resourced actors.

Where do you see opportunities for collaboration with industry, academia and other stakeholders in delivering on these priorities?

The Strategy emphasises the importance of collaboration between Government, business, and academia.

There are significant opportunities to leverage the Chamber network to disseminate information and promote best practice. And to support consultation and feedback loops between policymakers and industry. There is also the opportunity to facilitate SME engagement with training, certification, and funding programmes.

We encourage the Government to formalise engagement with representative bodies in the implementation phase, co-design supports with industry stakeholders, to utilise existing business networks to maximise reach and impact.

Developments in the Regulatory Environment

What are your views on the below priorities in relation to strengthening Ireland's cyber security resilience? Are key priorities missing?

We broadly support these priorities, particularly the focus on coordinated implementation of NIS2, effective recognition of certification schemes, and measures to strengthen supply chain security. These are important steps in strengthening Ireland's cyber resilience and in providing greater clarity within the evolving regulatory environment.

As mentioned above, implementation is key. In particular, public bodies and regulators should be supported to ensure consistent, proportionate, and well-communicated enforcement, while businesses must have access to clear guidance, realistic transition periods, and practical compliance supports.

We also believe that structured engagement with business representative bodies should be more explicitly recognised as a priority, particularly in relation to implementation, procurement, vulnerability disclosure, and voluntary information-sharing. In addition, supply chain security should be addressed not only in relation to critical national infrastructure, but across the wider business ecosystem, including SMEs that may be affected indirectly through customer and supplier requirements.

How should these goals be approached to maximise the chances of success?

Success will depend on consistent enforcement, practical compliance supports, and structured engagement with industry to identify implementation challenges early.

A risk-based approach should also underpin delivery, particularly in areas such as procurement, vulnerability disclosure, certification, and supply chain security. To maximise impact, these measures should be accompanied by sufficient regulatory capacity, realistic transition periods, and mechanisms to ensure that SMEs and smaller suppliers are not disproportionately burdened.

Where do you see opportunities for collaboration with industry, academia and other stakeholders in delivering on these priorities?

There are clear opportunities for collaboration with industry, academia, and representative bodies in supporting the practical implementation of the evolving cyber regulatory framework. Industry can provide feedback on how obligations under NIS2, the Cyber Resilience Act, procurement requirements, and vulnerability disclosure policies operate in practice, while academia can support regulatory readiness through research, skills development, and technical expertise.

Representative organisations can help communicate regulatory requirements, identify implementation challenges faced by SMEs, and support awareness of certification, compliance, and supply chain obligations. To maximise effectiveness, Government should formalise these engagement channels so that regulatory measures are informed by real-world business experience and can be refined over time where necessary.

Conclusion

We support the development of an ambitious and forward-looking National Cyber Security Strategy that reflects the evolving threat landscape and regulatory environment. To be effective, the Strategy must deliver practical, accessible supports for businesses, particularly SMEs.

We look forward to continued engagement with the Department as the Strategy is developed and implemented.