CYBER | IRELAND
IRELAND'S CYBER SECURITY CLUSTER

NI CYBER

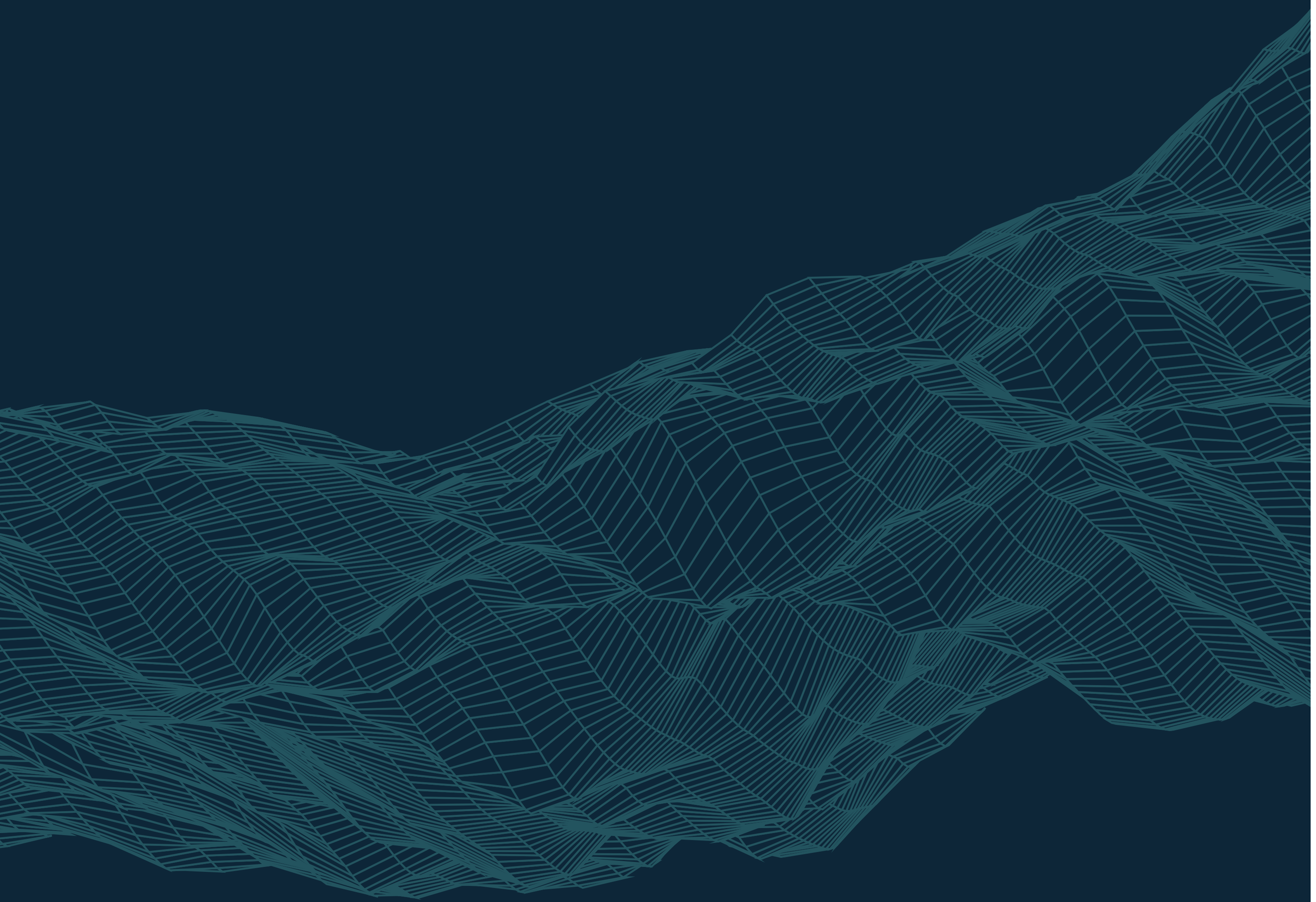
Perspective Economics

2025

All-Island Cyber Security Sector Research Report

supported by InterTradeIreland

Executive Summary



The cyber security industry has experienced significant growth in recent years, driven by the increasing reliance on digital technologies and the evolving threat landscape. Understanding the dynamics and potential of the cyber security market across Ireland and Northern Ireland on an all-island basis is crucial to support the industry's growth and competitiveness.

Cyber Ireland and NI Cyber, the island's two leading cyber cluster organisations, with support from InterTradeIreland's Synergy Programme, commissioned this research project led by Perspective Economics to assess the current state and future potential of the all-island cyber security industry.

The study employed a comprehensive approach, including analysis of company data, web analysis, a survey of 76 unique businesses, and secondary data analysis. This methodology allowed for a thorough mapping of the all-island cyber security sector, capturing both market-facing and internal cyber security functions across the island.

KEY FINDINGS

A leading ecosystem for cyber security

The research identifies 632 unique firms offering cyber security products, services, or research and development across the island of Ireland. This significant concentration of expertise and innovation positions the all-island cyber security ecosystem as one of Western Europe's leading cyber security clusters in terms of size and scale. There is a unique opportunity to leverage complementarities and skill-sets between Ireland and Northern Ireland to further promote indigenous growth and inward investment. However, further support would be welcomed by firms with respect to finding market-fit and overcoming jurisdictional and practical barriers to further enhance partnerships and cross-border trade.

A substantial economic contribution

The all-island cyber security sector generated an estimated €3.2bn in revenue and €1.5bn in Gross Value Added (GVA) in the most recent financial year, demonstrating substantial economic impact. Revenue growth has been strong, with an estimated Compound Annual Growth Rate (CAGR) of 13.4% for Irish firms over the last two years. However, growth in underlying profitability and productivity has been more modest, with an estimated cyber security GVA CAGR of approximately 4.5% over the same period.

Robust employment but slower growth

The research estimates that the 632 unique cyber security firms employ approximately 10,659 individuals in cyber security related roles across the island. While the all-island cyber security sector experienced employment growth of around 10% per annum between 2019-2022, the last couple of years (2022-2024) have seen more modest growth – approximately 4% in Ireland and 2% in Northern Ireland. This suggests a need to support indigenous firms' growth, increase access to managed service provision, and address increasing security risks in critical domains.

Diverse firm composition driven by FDI

The all-island cyber security sector consists of a mix of dedicated (pure-play) and diversified firms, with a high proportion of large companies (29%) compared to other regions, driven by significant inward investment, particularly from large US firms. Northern Ireland has a relatively higher concentration of larger firms (42%) than Ireland (27%), while Ireland has a much higher concentration of micro cyber security firms (40% compared to 20% in NI), suggesting an opportunity for partners to further enhance and scale the island's start-up ecosystem. Leveraging the strengths of both FDI and indigenous firms will be crucial in driving innovation and growth across the sector, and developing initiatives that are relevant to both types of firms (e.g., Meet the Buyer, or collaborative research projects) may be a key component in supporting both types of firms to grow and meet their client needs.

Sectoral strengths and opportunities for diversification

The all-island cyber security sector demonstrates notable strengths in attracting inward investment from global tech leaders and deploying cyber security within professional and financial services contexts. However, the research also highlights nascent engagement and overlap between cyber security teams working in sectors such as manufacturing, healthcare and medical devices, and critical sectors like telecoms, cloud, defence, and energy. Supporting collaboration and knowledge-sharing across these domains can help diversify the sector's offerings and widen new growth opportunities.

Potential for increased cross-border collaboration

While cross-border trade and collaboration exists within the all-island cyber security market, there is considerable potential for further growth and integration. The research identified 42 cyber security companies with active offices in both NI and Ireland, primarily multinationals and a small cluster of managed service providers near the border. Survey responses suggest a willingness to engage in cross-border initiatives, but practical barriers and challenges persist, such as perceived policy gaps, security clearance issues, and frustrations with areas such as public procurement processes.

Importance of grant funding and research support

The survey findings suggest that 9% of respondents avail of grant or research funding. While the survey response rate is limited (76 unique business responses), applying this percentage across the wider cohort indicates a potentially extensive range of start-ups or spin-outs that could benefit from sustained sources of grant and research funding. Initiatives such as the MTU Cyber Innovate program and CSIT's Cyber-AI Hub highlight the role of universities in catalysing innovation and entrepreneurship across the island. Strengthening the links between academia, industry, and government can help translate cutting-edge research into commercially viable solutions and drive the sector's growth.

Internal cyber security functions as growth drivers

The research estimates that up to 37% of providers (236) focus mainly on internal cyber security provision, such as R&D or securing wider product or service infrastructure. While these functions may not have direct revenue streams, they support the development of highly-skilled teams and can attract further inward investment, as demonstrated by the growth of the cyber security ecosystem in Northern Ireland's financial and insurance services sector. Recognising and nurturing these internal functions can contribute to the overall growth and resilience of the all-island cyber security ecosystem.

Export activity and international presence

Based on web data, the research estimates that 31% of the 96 'dedicated' cyber security firms headquartered in Ireland or Northern Ireland have at least one physical office in another jurisdiction. The survey findings indicate that 61% of respondents reported some form of export activity, with key markets including other EU/EEA countries, Great Britain, and North America. Supporting firms in navigating these challenges and expanding their international presence will be crucial in enhancing the sector's global competitiveness.

The report sets out six recommendation areas for the ecosystem, summarised below, and set out in full in the Key Findings and Recommendations section:

01 **Improving All-Island Collaboration**

Address barriers to cross-border collaboration, facilitate equitable access to opportunities, and work with public bodies to mitigate policy gaps and security clearance issues.

02 **Increase Knowledge-Sharing and Networking Events**

Organise targeted cross-border events like "Meet the Buyer" sessions, leverage diverse expertise for knowledge exchange, and prioritise networking support.

03 **Leverage Public Procurement**

Advocate for procurement practices that support small cyber security providers, streamline processes for SMEs, enable buyers to identify security gaps, and mandate minimum cyber security standards for government suppliers.

04 **Support SME Adoption and Pro-actively Target MSSP Growth**

Undertake additional research into all-island cyber security breaches, assist MSSPs in growth planning, and design grant schemes to incentivise SME adoption of cyber security measures.

05 **Foster Innovation through Cross-Border and International Incubators**

Establish access to cross-jurisdictional incubators and accelerators, organise visits to global markets, and provide tailored support for innovative firms to scale and access funding.

06 **Explore the potential for an All-Island Cyber Security Cluster Strategy**

Create a comprehensive strategy with promotion initiatives, regular sector mapping updates, annual events, and dedicated funding. Collaborate with stakeholders to align with broader objectives and establish clear metrics for measuring impact.

CYBER|IRELAND
IRELAND'S CYBER SECURITY CLUSTER

NI CYBER

Perspective
Economics