CYBER|IRELAND
IRELAND'S CYBER SECURITY CLUSTER

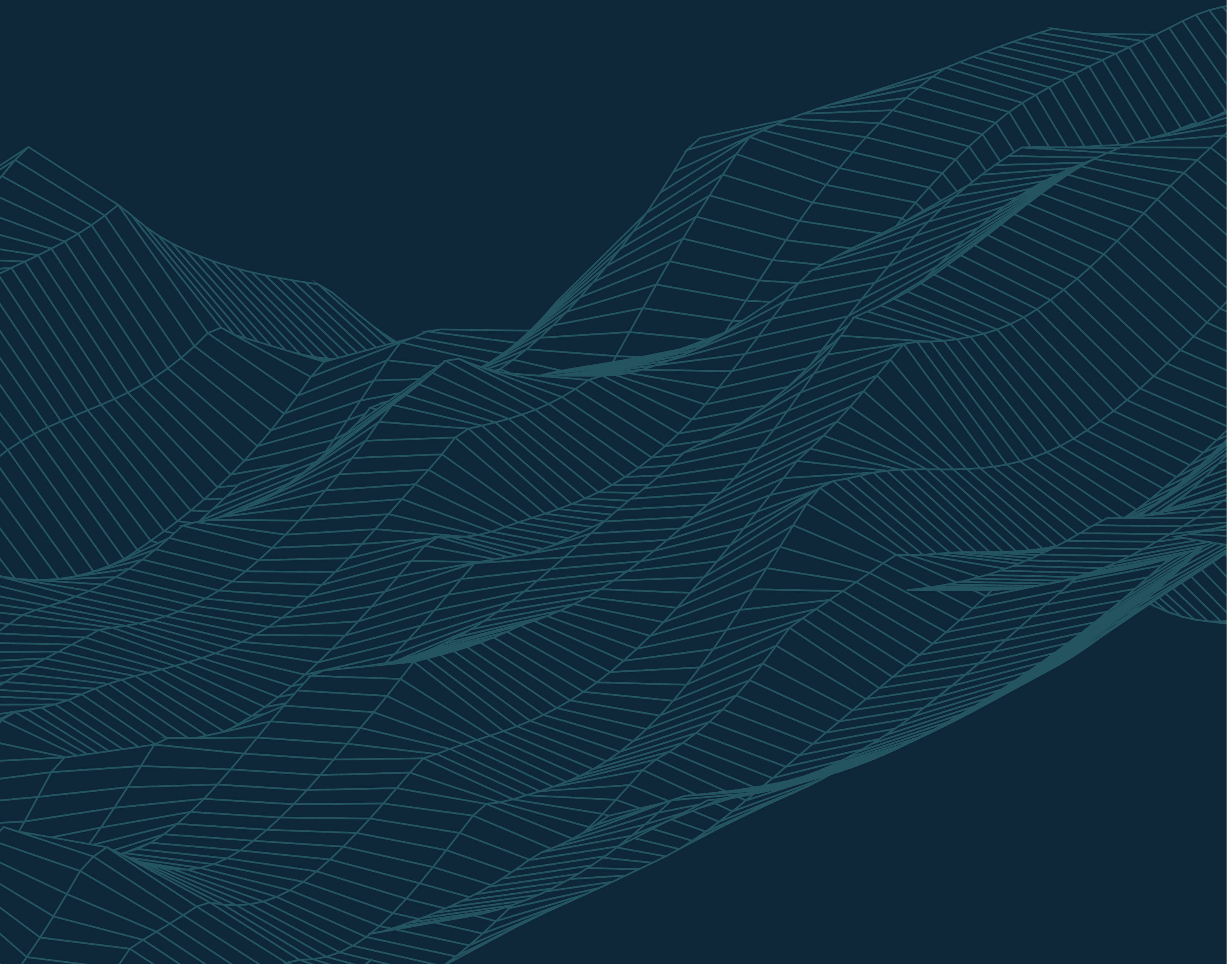
NI CYBER

Perspective Economics

2025

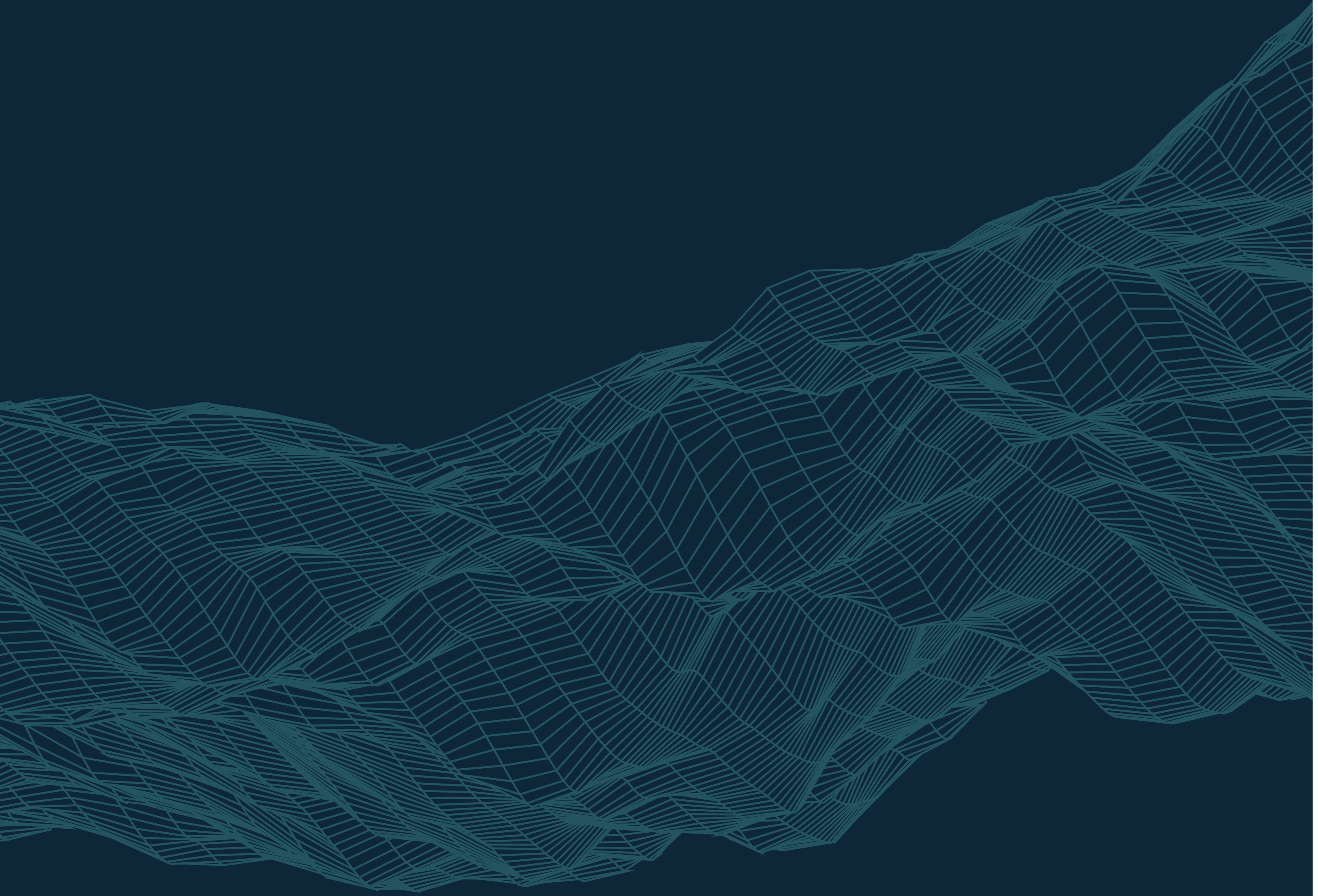
All-Island Cyber Security Sector Research Report

supported by InterTradeIreland



Contents

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.

01
Introduction

The cyber security industry has experienced significant growth in recent years, driven by the increasing reliance on digital technologies and the evolving threat landscape.

As organisations across various sectors adopt new technologies and digitise their operations, the demand for robust cyber security solutions has never been higher. In this context, understanding the dynamics and potential of the cyber security market in Ireland and Northern Ireland is crucial to support the industry's growth and competitiveness.

Cyber Ireland and NI Cyber, the island's two leading cyber cluster organisations dedicated to promoting and developing the cyber security sector, have recognised the need for a comprehensive study of the all-island cyber security market.

With support from InterTradeIreland's Synergy Programme, they have commissioned this research project led by Perspective Economics to assess the current state and future potential of the cyber security industry across the island of Ireland.

01 Map the size and scale of the all-island cyber security sector, including key metrics such as the number of companies, revenue, employment, and investment.

02 Identify the key cyber security suppliers serving the Irish and Northern Irish markets, as well as companies operating in both regions.

03 Analyse the markets, both geographic and sectoral, served by cyber security suppliers on the island of Ireland.

04 Estimate the potential growth of the all-island cyber security market based on current trends and future projections.

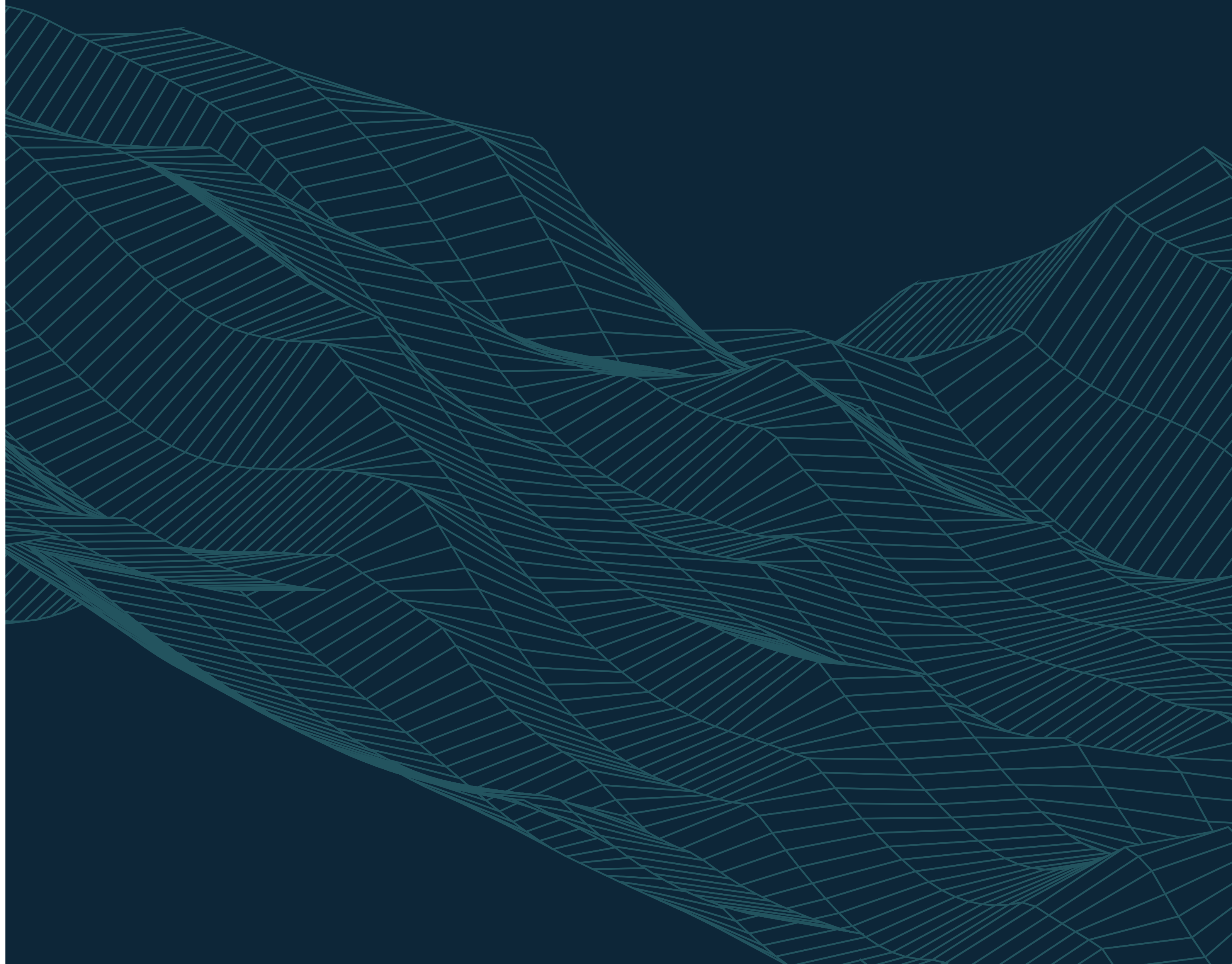
05 Examine the key buyers and sectors requiring cyber security services, as well as the factors influencing their purchasing decisions.

06 Investigate the routes to market for cyber security suppliers and the attributes impacting these routes, such as company size, ownership, and sector.

07 Identify any barriers faced by buyers in accessing cyber security solutions and propose recommendations to address these challenges.

By addressing these objectives, this research aims to provide valuable insights and actionable recommendations for Cyber Ireland, NI Cyber, and other stakeholders in the all-island cyber security sector.

The findings will support evidence-based decision-making and help shape strategies to support the growth and competitiveness of the sector, ultimately contributing to the economic development and improved cyber resilience of organisations across Ireland and Northern Ireland, and the organisations they serve globally.



02
Methodology

METHODOLOGY

This research seeks to identify firms that are active in Ireland and / or Northern Ireland and offer cyber security products or services to either domestic or international markets.

Further, in recognition of the importance of cyber security across all sectors, the research scope has also included firms that provide cyber security as a secondary, or diversified service, or those that are actively employing cyber security staff to support internal cyber security operations or for product development purposes. This ensures that the full extent of employment and expertise within the cyber security sector across the island can be fully estimated and mapped.

The cyber security sector does not have a formal NACE or SIC code, and official industrial data does not sufficiently break down sectors to identify cyber security companies. As such, the research team has reviewed active or trading companies across the island of Ireland, and reviewed trading activities and web data at scale to help identify and short-list cyber security providers. Further, the team has worked closely with Cyber Ireland and NI Cyber to identify cluster members and find evidence of similar provision across the island. The research scope includes firms that:

✓ Have a clear presence in Ireland or Northern Ireland (registered or active office location)

✓ Demonstrate an active provision of commercial activity related to cyber securit (e.g. through the presence of a website / social media / office

✓ Provide cyber security products or services to the market (i.e. sell or enable the selli of these solutions to other customers)

✓ Have identifiable revenue or employment related to cyber security within Irelan or Northern Ireland

✓ Provide recruitment support specifically for the sector; or

✓ Employ skilled cyber security professionals to work on internal products or services.

The analysis also delineates firms by two key classifications (dedicated and diversified), as defined below:

Dedicated (or pure-play)

This refers to where all, or most (75%+), of a firm's activity can be attributable to cyber security provision. These firms offer products or services specific to the cyber security sector.

Diversified

This refers to firms that offer cyber security services as part of a wider business structure e.g., finance, insurance, telecoms, or defence - or that have internal cyber security operations or product development teams.

Please note that the analysis focuses upon private registered businesses only and does not include public, academic, or charity organisations that offer cyber security products or services in Ireland. When exploring sector revenues, employment and Gross Value Added (GVA), we provide an estimate linked to the provision of cyber security products and services only.

The methodology undertaken for this research is consistent with the previous Cyber Ireland State of the Sector (2022) and NI Cyber Snapshot (2023), with some additional markers developed for this study. We summarise the methodology below:

Definition and Scoping

The research team utilised the definitions used for the prior sectoral studies, including a broad definitional approach, and the use of six taxonomy areas (set out within this report) for consideration. As the all-island sector consists of a range of market-facing, and internal cyber security functions, the study aimed to capture as many of these as possible.

Firm Identification

The research team identified relevant firms using a wide range of datasets, including previous baseline reports (with all data held by Perspective, Cyber Ireland and NI Cyber), web data (with key terms matched against over 200,000 Irish and NI active companies), company registration databases (Companies House and CRO), job vacancy data (Lightcast), investment data (Crunchbase), and procurement data (eTenders). All firms were reviewed to ensure there was a clear alignment to cyber security provision, that relevant activity (e.g., employment or office locations) could be identified and reviewed using manual and automated checks to ensure inclusion or exclusion from the dataset. This resulted in a final list of 632 unique cyber security firms across the island.

Firm Enrichment and Classification

All companies were matched against the relevant firm registration in Ireland or Northern Ireland (or UK). Firms were reviewed to match against websites, and company data was enriched using web crawling and parsing techniques (Python), extracting contextual information and enriching accurate descriptions with open source LLMs and web data.

Web Survey

A web survey was promoted by Cyber Ireland, NI Cyber, and InterTradeIreland, receiving 82 responses from 76 unique firms. The survey gathered data on performance, market sentiment, growth opportunities, routes to market, and awareness of clusters and views on growing the all-island sector.

Data Augmentation

Cleaning and augmenting the dataset with survey, web, and secondary data (e.g., accounts), estimating revenue, GVA, and employment figures related to cyber security activities.

Core Economic Modelling

The team undertook further modelling to adjust for any clear anomalies or outliers and develop estimated values (per employee) for related revenue and GVA.

Analysis and Reporting

The team built a bespoke dataset to provide insights on the size, scale, and characteristics of the all-island cyber security sector, examining cross-border activities, key products and services, target markets, and routes to market.

03
Defining and Measuring the Cyber Security Sector

Cyber security is an inherently broad domain and contains a wide range of products and services to help organisations and individuals to secure systems and data. This section sets out a working definition used to identify businesses in Ireland offering such solutions. We use a broad definition to help capture as much of the economic activity relating to cyber security as possible.

We utilise the **definition of cyber security** as set out within Ireland's National Cyber Security Strategy (2019) as:

> The means of ensuring the confidentiality, integrity, authenticity, and availability of networks, devices, and data.
>
> NATIONAL CYBER SECURITY STRATEGY (2019 – 2024)

The taxonomy developed for this study has been designed using a top-down approach, to reflect the product and service offerings across the island of Ireland. It has been used previously to map the cyber security sectors in Northern Ireland and Ireland.

We have identified six key areas of products and services offered within the all-island cyber security sector, in addition to an 'other' classification to include internal cyber security operations, product development, R&D, or recruitment.

We use this taxonomy for two key reasons, as it:

- Provides a high-level overview of the products and services offered by businesses within the all-island cyber security sector, that is easy to understand; and
- Enables comparability with other studies e.g. the NI Cyber Snapshot, allowing for an all-island, or international, comparison of the products and services typically offered.

04
The All-Island Cyber Security Sector

INTRODUCTION

The cyber security sectors in Ireland and Northern Ireland have demonstrated considerable growth and capability in recent years.

The "State of the Cyber Security Sector in Ireland 2022" revealed that the Irish cyber security industry employed over 7,300 people across more than 490 firms, generating an estimated annual revenue of €2.1 billion.

Similarly, the CSIT NI Cyber Security Snapshot 2023 highlighted the strength of the Northern Irish cyber security sector, with over 110 firms employing more than 2,900 people and generating estimated annual revenue of £150 million. The region has established itself as a hub for cyber security research and innovation, with world-leading institutions such as the Centre for Secure Information Technologies (CSIT) at Queen's University Belfast driving cutting-edge developments in the field.

The Irish and Northern Irish ecosystems share several key components, including considerable foreign direct investment, skilled pipelines, collaboration between industry, government and academia, and emergent home-grown firms seeking to compete and scale globally.

This report seeks to, for the first time, measure the size and scale of the all-island cyber security sector, capturing the joint size, scale, and value of provision across Ireland and Northern Ireland. This involves a cross-border approach, including use and standardisation of multiple company registration datasets, company accounts, web data, a shared taxonomy of product and service provision, and an all-island survey promoted by both clusters and InterTradeIreland to elicit feedback regarding cross-border and international trading activity.

Collectively, this research finds 632 companies offering cyber security products, services, or research and development across the island of Ireland, representing a significant concentration of expertise and innovation. With just over 7m people on the island of Ireland, we believe that the all-island cyber security sector is arguably one of Western Europe's leading cyber security clusters in size and scale. Further, this critical mass of companies, operating across multiple use-cases, presents a unique opportunity to further leverage the complementarities and skill-sets between Ireland and Northern Ireland – particularly where jurisdictional and practical barriers may exist and be overcome through partnerships and cross-border trade.

The benefits of an all-island approach to cyber security are significant. By working together, Ireland and Northern Ireland can:

01 Pool resources and expertise to tackle complex cyber security challenges

02 Facilitate knowledge-sharing and collaboration between industry, academia, and government

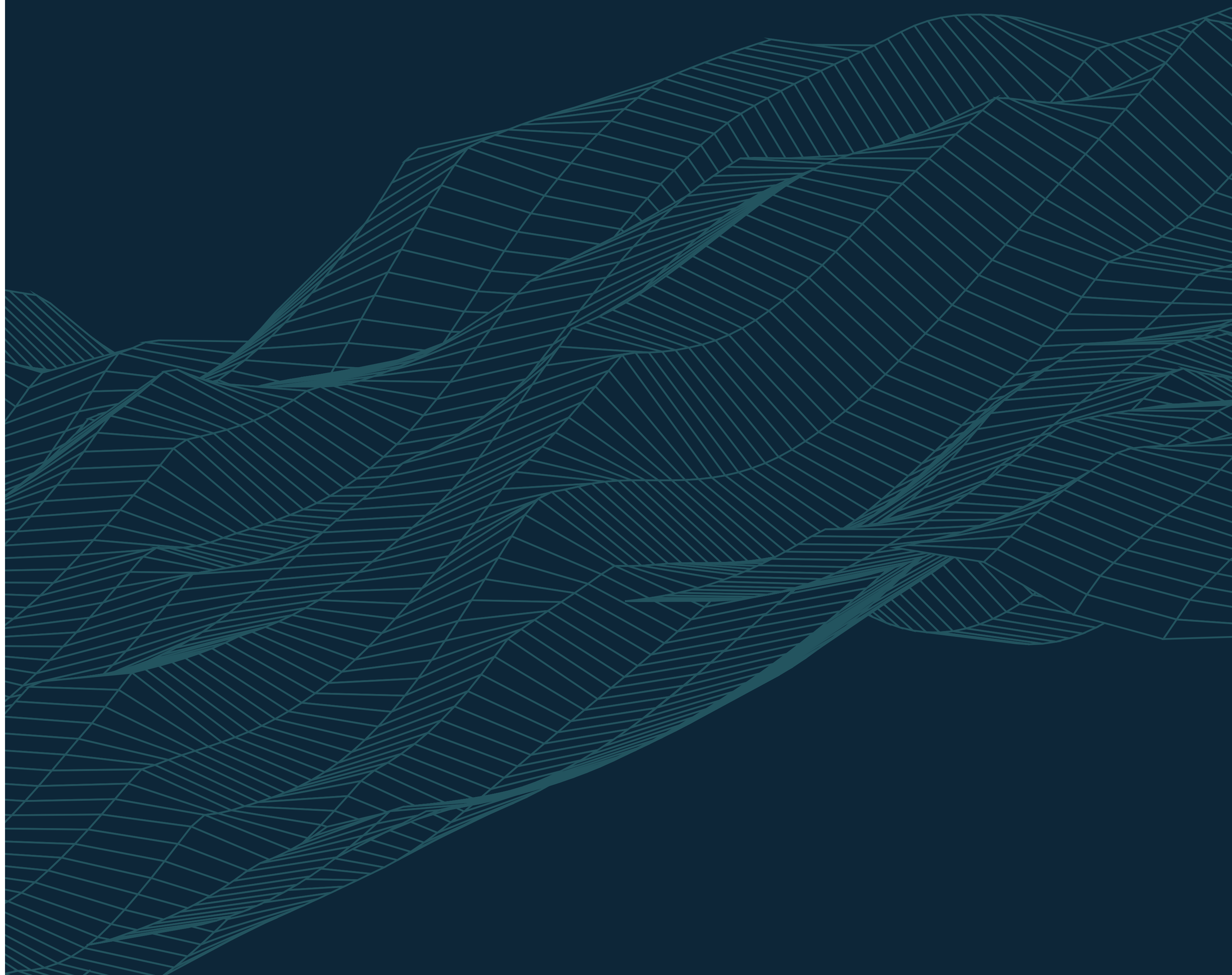
03 Enhance the global competitiveness and visibility of the all-island cyber security sector

04 Attract international investment, partnerships, and talent

05 Support the development of a more resilient and secure digital economy across the island, by increasing the supply of cyber security talent and provision across all sectors.

In the following sections, we provide a detailed analysis of the size, scale, and characteristics of the all-island cyber security sector, examining key metrics such as revenue, employment, and investment, as well as the geographic distribution and cross-border activities of firms.

This evidence-based assessment will help to inform strategies and policies to support the continued growth and success of the all-island cyber security market, and to highlight new previously untapped opportunities for further cross-border collaboration.



05
Estimating the Size of the All-Island Cyber Security Sector

We have identified 632 unique firms across the island of Ireland developing or selling cyber security products or services, or enhancing cyber security provision for their parent entity. We also note that 31 firms are registered in both Ireland (CRO) and the United Kingdom (Companies House). These are treated as singular to prevent double-counting; however, revenue and employment activity is considered across both jurisdictions.

The firms identified within this study are not homogenous. They have a wide array of market characteristics, and there is no 'one-size-fits-all' measure regarding their needs, ambitions, and routes to market. We find significant variation by factors such as size and scale, the extent of provision of cyber security products or services, whether they go to market or service an internal function within a larger firm, and the geographic and sector-based markets that they target.

As such, this section outlines key features of the identified firms that are engaged in the provision of cyber security products or services, outlining key features within the sector by:

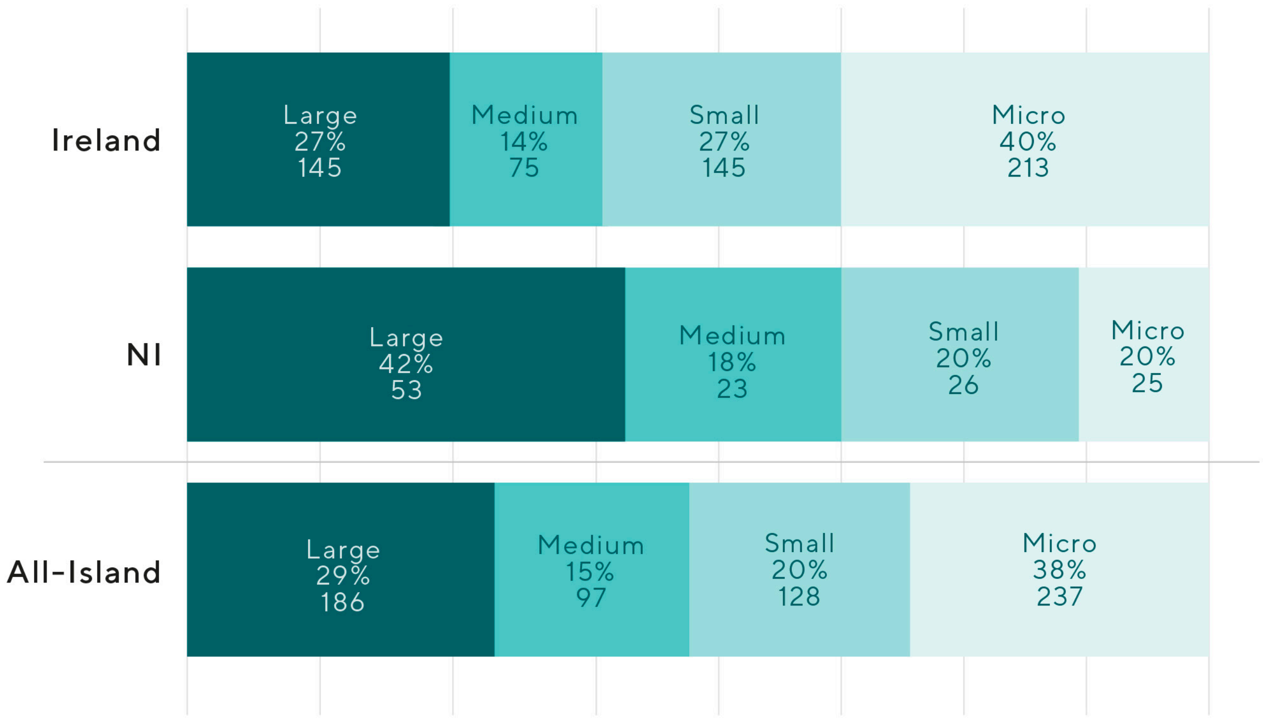
- Size (Large and SMEs)
- Dedicated and Diversified Status
- Company Background (Country of Origin)
- Products and Services Offered (Taxonomy)

These markers have been classified by the research team, with the full dataset available for use by Cyber Ireland, NI Cyber, and InterTradeIreland for further use.

SIZE AND SCALE

Across the island of Ireland, Figure 1.1 sets out the estimated size[2] of the 632 unique firms. The size variable relates to the size of the registered company active in Ireland or Northern Ireland. For example, a business with 500 staff, of which 20 work in cyber security roles, would be classified as large (typically 250+ full-time staff).

FIGURE 1.1 NUMBER OF CYBER SECURITY FIRMS BY SIZE



Source: Perspective Economics analysis of 632 identified firms

As set out in similar previous studies for Ireland and Northern Ireland respectively, the sector consists of a high proportion of large companies (29%), and the percentage of 'large' firms in the all-island cyber security sector is much higher than comparable studies. For example, the UK Cyber Security Sectoral Analysis 2024 estimates that approximately 8% of UK cyber security firms are large. However, both Ireland and Northern Ireland have historically (over the previous two decades) placed a focus upon attracting Foreign Direct Investment to respective regions, and this is a key determinant in the provenance of larger firms across the island active in cyber security.

Interestingly, Northern Ireland has a relatively higher concentration of larger firms (42%) than Ireland (27%). This is explored in the NI Cyber Snapshot, which highlights the significance of large US FDI in particular. However, Ireland also has a much higher concentration of micro cyber security firms (40% of those identified, with 213 providers), compared to Northern Ireland (20%, with 25 providers). With almost ten micro providers in Ireland for every one identified in Northern Ireland, this may suggest an increasingly significant cyber security start-up community[3] (and increased supply of small consultancies) in Ireland. This is critical to developing the indigenous base and supporting an innovative start-up ecosystem in tandem with growing inward investment. However, it also highlights the need to support micro and smaller firms to scale accordingly.

On an all-island basis, we find similar composition of medium (typically 50-249 staff) and small (10-49) firms (15% and 20% respectively). The 225 firms across the island of Ireland may be particularly important for policy and cluster consideration, as they may have potential to grow, scale, and export (where relevant to their business models). We explore this further in sub-sectoral analysis.

[2] Full size definitions: Large: Employees >=250 and Turnover > €50m or Balance sheet total > €43m // Medium: Employees >50 and < 250 And Turnover <= €50m or Balance sheet total <= €43m // Small: Employees >10 and < 50 And Turnover <= €10m or Balance sheet total <= €43m // Micro: Employees < 10 And Turnover <= €2m or Balance sheet total <= €2m

[3] https://www.paladincapgroup.com/ireland-an-emerging-leader-in-european-cyber/

DEDICATED AND DIVERSIFIED PROVISION

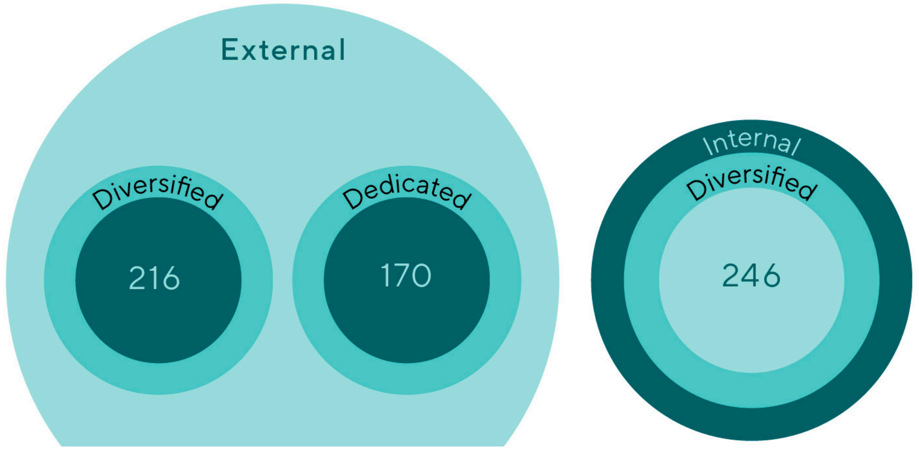
As set out previously, it is important to take a broad approach in the identification of cyber security provision across the island, to help identify the reach and scale of the ecosystem, particularly as many large IT firms and consultancies have increased their provision of cyber security in recent years. However, the research team considers that there are several markers that can be applied to each identified firm to help segment and understand the unique opportunities and challenges faced by sub-groups. Within previous Ireland and NI reports, the research team has segmented companies into two categories:

Dedicated (otherwise known as pure-play), where all or most of the firm's activity can be attributable to cyber security provision. These offer products or services specific to the cyber sector.

Diversified, where firms offer cyber security services as part of a wider business structure e.g., finance, insurance, or defence - or that have internal cyber security operations or product development teams.

Within this study, we also apply a new and additional marker: 'External' where a firm appears to be actively selling cyber security products or services to a third-party or customer, and 'Internal' where the primary role of the cyber security team (identified in Ireland) is to support the overarching business (e.g. an internal Security Operations Centre, or internal R&D for areas such as fraud detection). This provides further delineation between the strengths, capabilities, and market approach of the firms, and highlights three key market groupings, with different customers, needs, and routes to market as shown below.

FIGURE 1.2 NUMBER OF CYBER SECURITY FIRMS BY MARKET POSITIONING



Source: Perspective Economics analysis of 632 identified firms

We find that across the island of Ireland:

- The majority (61%, 386) of cyber security companies identified are external and market-facing (with respect to cyber security provision). Of these, 56% are diversified (i.e. offer cyber as part of a wider offering), and 44% are dedicated.
- The remaining firms (39%, 246) focus on internal provision, and as such are also considered diversified in scope.

This is an important distinction for policy-makers and clusters to consider, as it suggests there are three relatively distinct groups (under a broad classification), which have different approaches to market, skills requirements, and growth potential. For example:

Dedicated firms that sell cyber security products or services externally: This includes firms that are highly focused upon cyber security product and service development, research and innovation, developing and securing skills, and expanding into new markets or availing of top technical talent e.g. Rapid7, Trellix, Integrity360 etc.

Diversified firms that sell cyber security products or services externally: This typically includes firms that can sell cyber security products or services as part of a wider company offering. This can include large multinationals seeking to embed security within wider solutions e.g. Microsoft, IBM etc. It can also include consultancies and managed service providers offering cyber security e.g. Deloitte, Accenture etc.

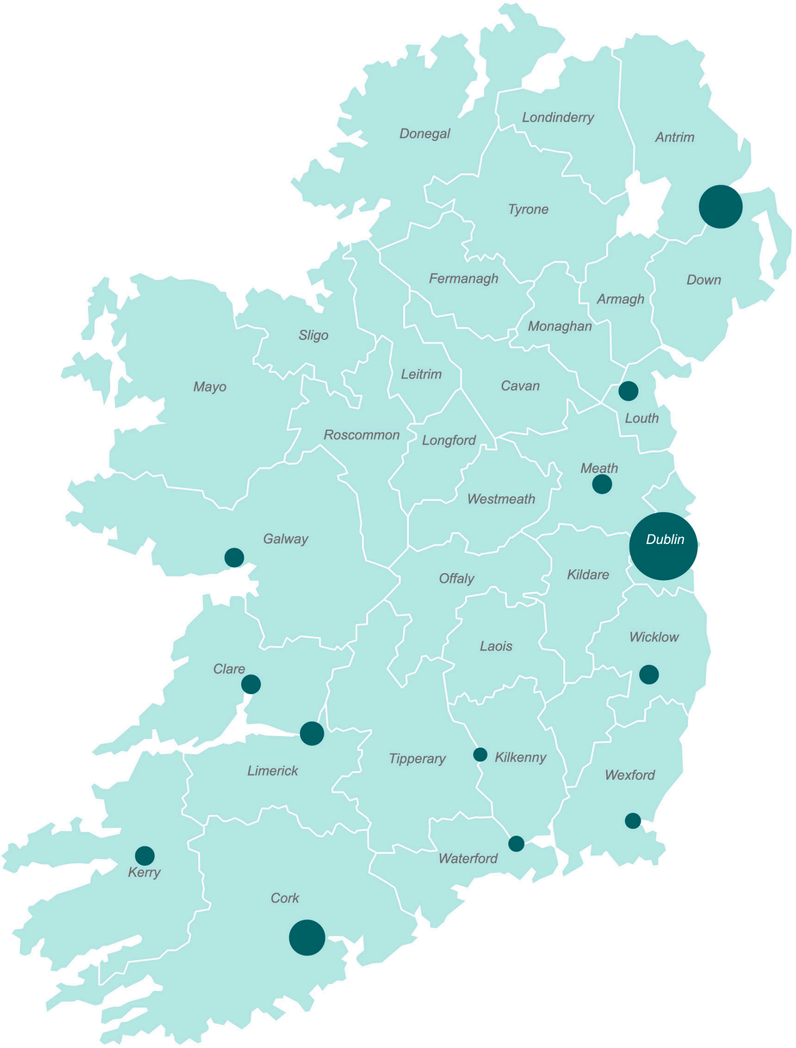
Internal approaches to cyber security: We find evidence of firms that have developed or built internal capabilities in cyber security across the island to enhance the wider company structure. This includes inward investment where large multinationals have established teams in security (and trust and safety) e.g. Google, Aflac etc. It also includes firms such as Bank of Ireland and JLR – building internal capabilities in cyber security.

[3] https://www.paladincapgroup.com/ireland-an-emerging-leader-in-european-cyber/

DEDICATED AND DIVERSIFIED PROVISION

Across the cyber security providers identified, the research team has identified 758 unique offices on the island of Ireland. The team has used web data and deduplicated multiple offices in close proximity to reduce and remove false positives. This highlights the significant clusters in areas such as Dublin (399 firms with a presence), Belfast (108), Cork (79), Galway (27), Limerick (21) and more. The respective Cyber Ireland and CSIT Northern Ireland Cyber Security Snapshot explore regional location analysis in further detail, and the 'Cross-Border and International Activity' explores all-island export and trading.

FIGURE 1.3 CYBER SECURITY OFFICES ACROSS THE ISLAND OF IRELAND

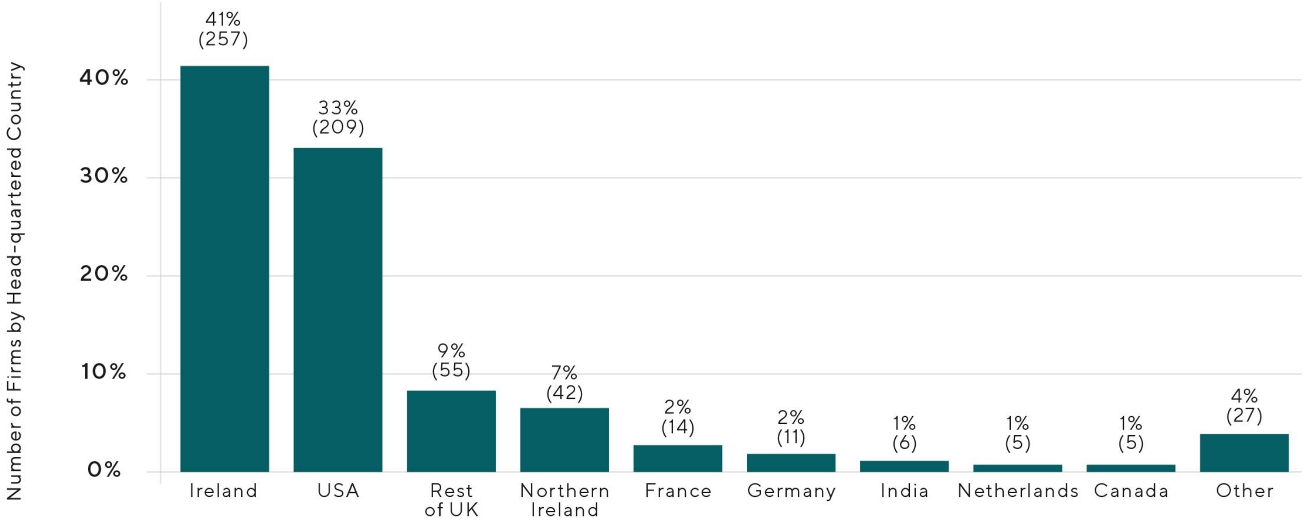


Source: Cluster analysis of 632 providers in 758 locations (dot, >10 sites)

NUMBER OF FIRMS BY HEADQUARTERED LOCATION

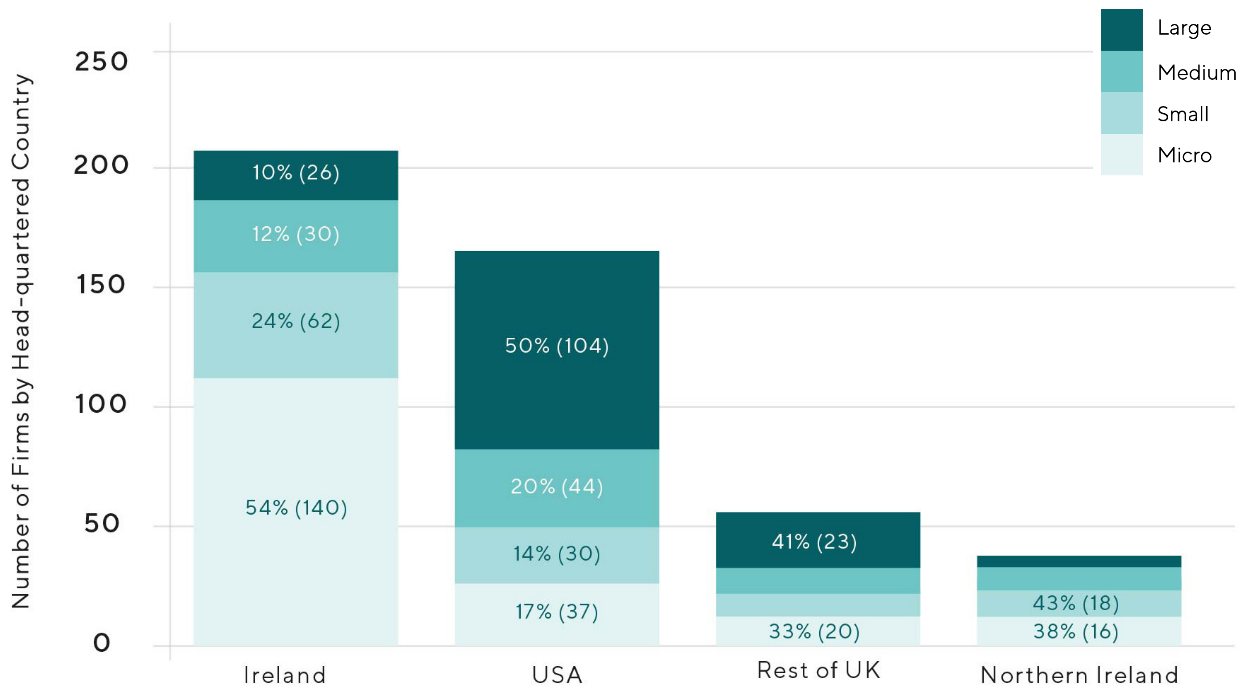
Ireland and Northern Ireland both have a recognised reputation for being an attractive investment location for foreign firms seeking to establish a European base with a well-educated, English-speaking workforce, with access to the European market and strong alignment to US markets. To understand the ownership of companies, whether they are domestic or foreign, the research explores the country location of the 'headquartered' or 'parent' firm involved in each of the cyber security businesses identified. This is also important for policy-makers, as this can provide insight into both the attractiveness of the all-island market to external investors, but also signal opportunities for growing the indigenous base, and supporting cross-border trade. As highlighted in previous studies, domestic firms (Ireland and NI headquartered) make up almost half of all firms identified (48%), with significant inward investment from large US firms in particular. This is explored in employment and revenue data within subsequent sections.

FIGURE 1.4 NUMBER OF CYBER SECURITY FIRMS BY HEADQUARTERED COUNTRY



Source: Perspective Economics, n = 632

FIGURE 1.5 NUMBER OF CYBER SECURITY FIRMS BY HEADQUARTERED COUNTRY BY SIZE (KEY MARKETS)



Source: Perspective Economics, n = 632

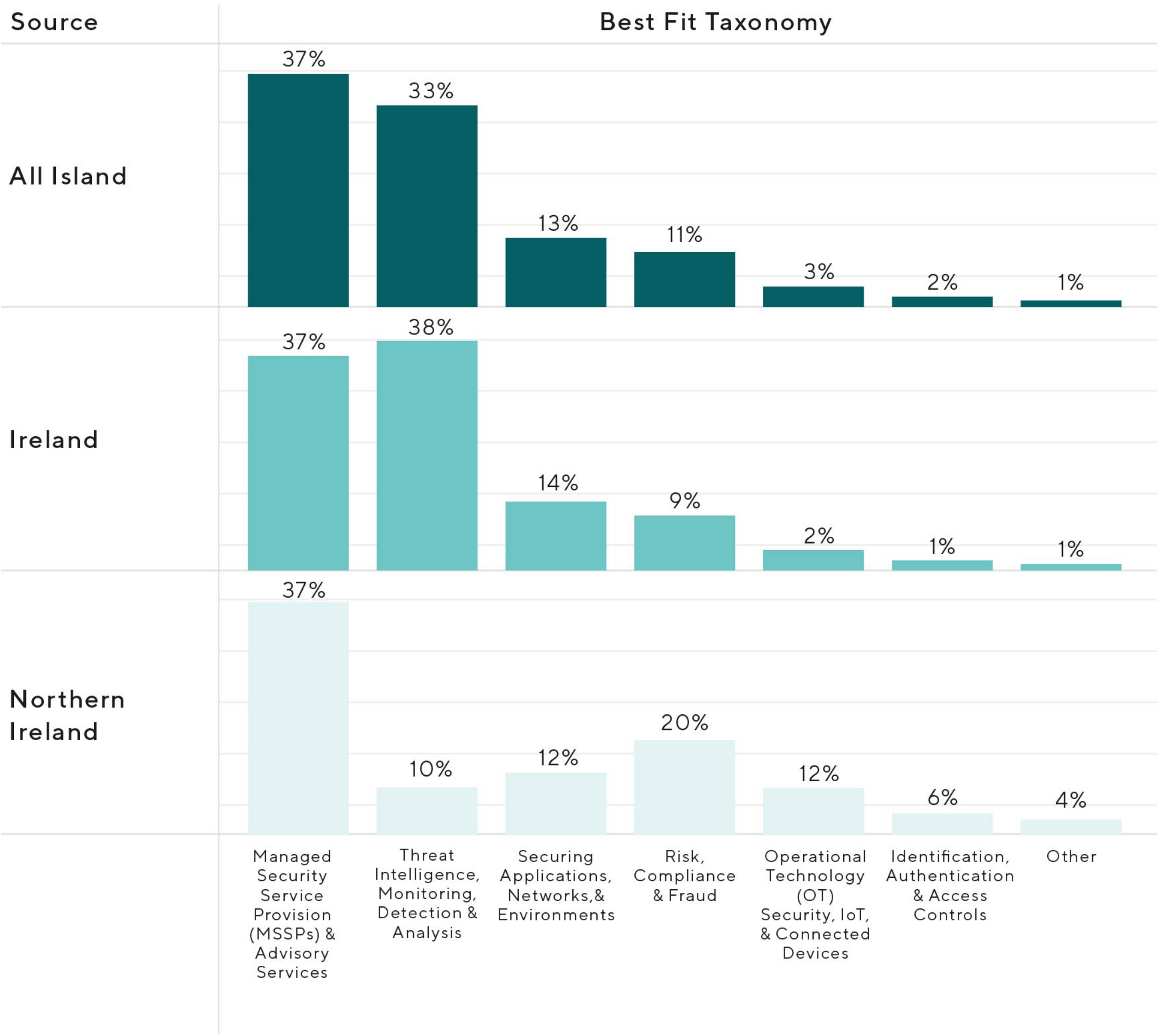
PRODUCTS AND SERVICES OFFERED (TAXONOMY)

This study uses the cyber security market taxonomy developed by Perspective Economics for both the previous Ireland (2022) research, and Northern Ireland snapshot (2023). This provides a high-level overview of the products and services offered by businesses within the cyber security sector and enables comparability allowing for an all-island assessment of the marketplace.

CATEGORY	DEFINITION
Managed security service provision (MSSP) and advisory services	Firms that typically sell cyber security services to an external party and are primarily focused on outsourced security. For example, where a business procures an MSSP to undertake monitoring, network security, patching and device management, penetration testing, and broader security and IT advice.
Risk, compliance, and fraud	Firms where the focus is on identifying risk (such as harmful actors or anomalies), ensuring compliance with cyber security standards (e.g., ISO27001 and GDPR), data management, and identifying and mitigating fraud within transactions.
Securing applications, networks, and cloud environments	Firms that develop or implement products or solutions with respect to application security, networks, or cloud infrastructure. This might include identifying and patching potential software or network exploits or applying secure parameters to network or cloud environments e.g., ensuring infrastructure is encrypted, ensures DLP, and has appropriate authentication or controls in place.
Operational technology, security, and connected devices	This refers to the manufacture and distribution of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a change through monitoring and/or control of devices, processes, and events.
Threat intelligence, monitoring, detection, and analysis	Information security products or services that focus on network administration or network engineering or identification of harmful activities, that help to counter the activities of cybercriminals such as hackers and developers of malicious software.
Identification, authentication, and access control	Firms supporting the verification of users accessing systems.
Other firms	Firms that support employment in sectors that are not market-facing. This can include cyber security recruitment firms, firms developing security solutions for internal use only, firms securing systems internally, or those with teams dedicated to trust and safety of end-user data (e.g., social media firms).

Figure 1.6 highlights the estimated 'best-fit' against the taxonomy for the all-island economy, and Ireland and Northern Ireland respectively. This focuses upon firm count and highlights how over one in three cyber security firms (37%) in both countries are typically focused on managed services provision, and that Ireland has greater proportional breadth in areas such as threat intelligence (38% vs 10% of firms), and that Northern Ireland has a high concentration of risk, compliance and fraud focused firms (20% compared to 9% in Ireland.)

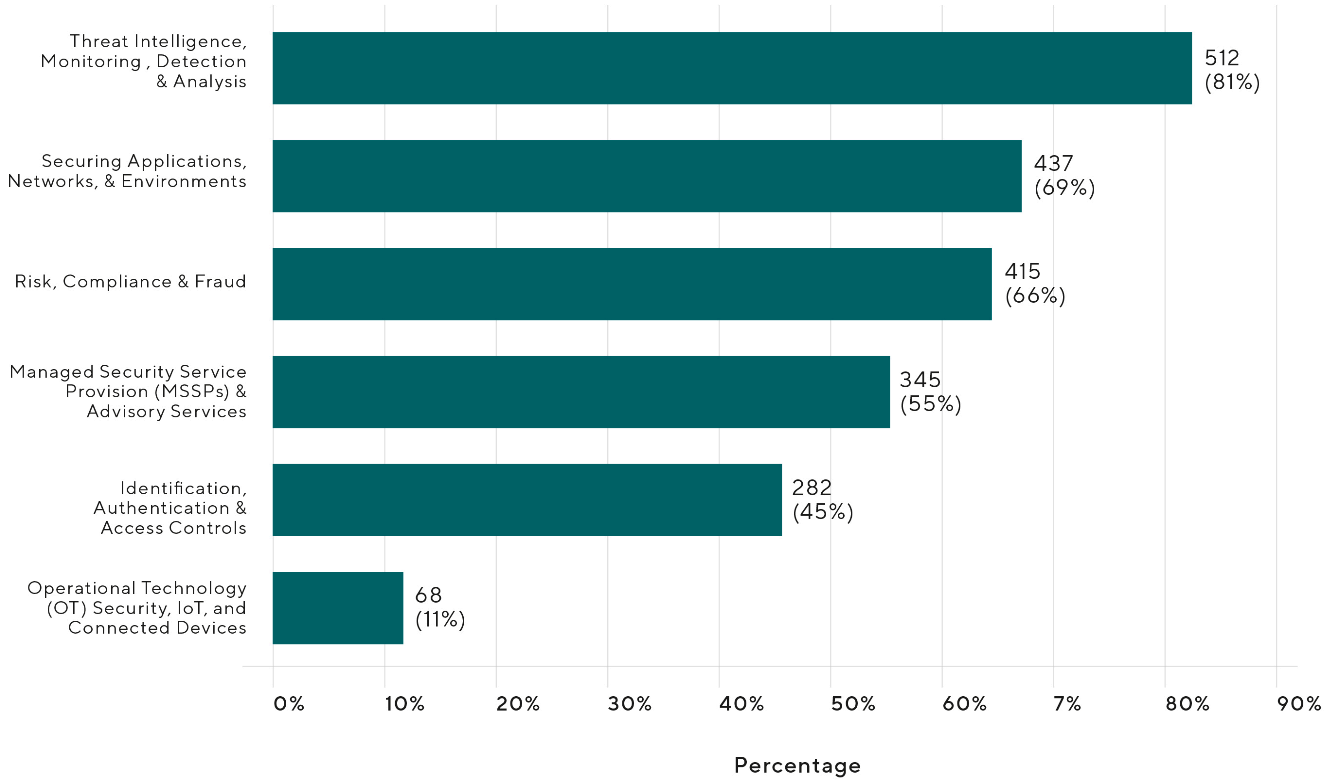
FIGURE 1.6 TAXONOMY PRODUCTS AND SERVICES (BEST-FIT BY LOCATION)



Source: Perspective Economics, n = 632

Figure 1.7 also highlights where the research team has applied multiple markers against the taxonomy, where if a firm provides any relevant products or services, they are considered in scope (i.e. many markers can be applied, not just a single best-fit). This highlights breadth across the market (explored in Routes to Market with respect to reselling and partnerships), but also highlights a more nascent market in Operational Technology (OT) and Internet of Things (IoT) security across the island.

FIGURE 1.7 TAXONOMY PRODUCTS AND SERVICES (ALL COVERAGE)



Source: Perspective Economics, n = 632

06 Economic Activity: Revenue, GVA and Employment

ECONOMIC ACTIVITY: REVENUE, GVA AND EMPLOYMENT

This section provides an overview of the economic contribution that the cyber security sector generates for the wider all-island economy. This includes an estimate of total cyber security related revenue, Gross Value Added (a measure of productivity), and employment across the island.

We estimate that in the most recent financial year, annual cyber security-related revenue across the island of Ireland reached approximately €3.2bn (£2.9bn).

This figure has been estimated using:

- Revenue figures available for dedicated (100%) cyber security firms that publish annual accounts.
- Revenue figures available for diversified cyber security firms (with revenue estimated based on the proportion of staff working in cyber security related roles.)
- Reported cyber security revenue estimated (for the most recent financial year) through the business survey undertaken in Summer 2024.

The nature, availability, and quality of company data available means this is an estimate only. However, significant outliers (e.g. very high revenue figures with multinationals registered in Ireland) have been removed from the modelling to enable a feasible and realistic estimate of cyber security activity.

- For Irish firms, we estimate cyber security related revenue is approximately €2.7bn. This compares strongly against the 2022 baseline estimate of €2.1bn, suggesting the sector has grown by approximately €600m in the previous two years, with an estimated CAGR of 13.4%.
- For Northern Ireland firms, the size of the sample means that estimating revenue data is more limited, and is undertaken on a per FTE basis (within NI). Based upon the 2023 snapshot, and data within this research, we estimate revenue of approximately £434m (€486m) for the NI cyber security sector.

ESTIMATED CYBER SECURITY GROSS VALUE ADDED

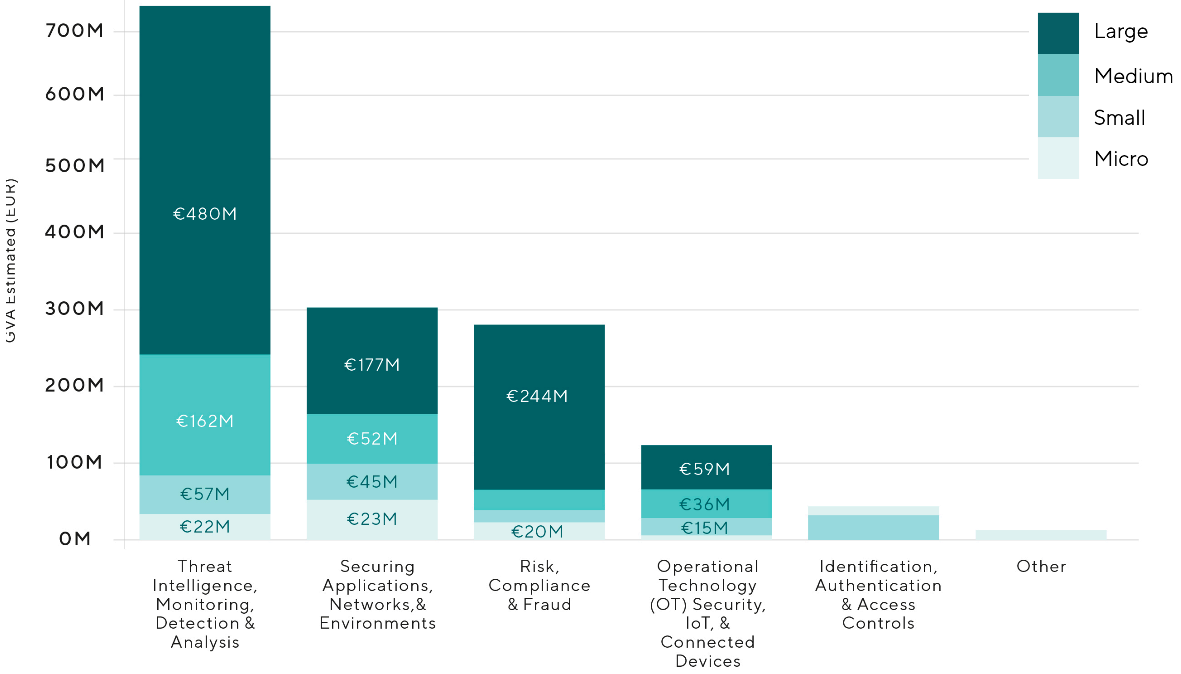
Gross Value Added (GVA) is used as a measure of productivity (at a firm level, or above). It captures the sum of a firm's Gross Profit, Employee Remuneration, Amortisation and Depreciation. In this respect, any increase in GVA can highlight an improvement in the performance of a firm or a sector, as evidenced through higher profitability or enhanced earnings. Company accounts across Ireland can often capture global or international economic activity, and we have therefore adjusted the estimates to account for this.

The baseline research undertaken for the Irish cyber security sector in 2022 estimated that Ireland's cyber security sector generated approximately €1.1bn in GVA in 2021. The NI Cyber Security Snapshot (2023) estimated the NI sector generated approximately £236m in GVA in 2023 (a 47% increase from the 2021 baseline of £161m).

The GVA estimates suggest that the majority is generated by the large firms (typically over 250 staff) (€976m, 67%), as expected within similar studies. However, this would also signal opportunity to grow SMEs (worth €489m), particularly in areas such as managed service provision and threat intelligence, as well as supporting nascent growth in more emergent areas such as OT security.

We estimate that the 632 cyber security firms across the island of Ireland generated approximately €1.5bn in GVA in the most recent financial year (€1.2bn in Ireland, and €264m in NI). This suggests a slightly lower CAGR of 4.5% for Irish firms (driven by a c. €100m increase over two years).

FIGURE 1.8 ESTIMATED ALL-ISLAND GVA BY MAIN TAXONOMY AND COMPANY SIZE



Source: Perspective Economics

ESTIMATED CYBER SECURITY EMPLOYMENT

The research team has used accounts and web data to review all cyber security firms across the island of Ireland and provide an estimated figure regarding the estimated number of cyber security professionals in the private sector. This has also been enhanced using cluster networks, and the use of an online survey.

Overall, we estimate that across the 632 unique cyber security firms, **there are an estimated 10,659 individuals working in cyber security related roles.** We include all employment with dedicated firms, and an individual estimate for diversified firms.

This includes an estimated 7,911 individuals in Ireland, and 2,748 individuals in Northern Ireland.

This suggests modest employment growth in cyber security roles in Ireland (+8% over the two years, CAGR of c. 4%) since the 2022 baseline study.

This is lower than the growth scenarios (10% per annum) set out in the baseline study; however, we note that labour market conditions have been more challenging in 2023 and 2024 than in previous years. Further, it is estimated that in 2023, there has been a significant increase in the number of redundancies within the tech sector and that 'Ireland accounts for the largest proportion (around 40%) of all redundancies in the tech sector in the EU[4] given the high concentration of European and EMEA headquartered firms based in Ireland[5]. The Central Bank of Ireland also estimated in early 2023, that the IT sector in Ireland had c. 2,307 layoffs in the year to February 2023, albeit this was considered likely to have been offset by wider vacancies and absorptive capacity in other firms.

[4] https://www.lavellepartners.ie/news/2023/10/02/the-impact-of-redundancies-in-the-irish-tech-sector/
[5] https://www.centralbank.ie/docs/default-source/publications/quarterly-bulletins/quarterly-bulletin-signed-articles/the-role-of-ict-services-sector-irish-economy.pdf

In Northern Ireland, we estimate that there has been more limited employment growth between 2023 to 2024 (+2% since the 2023 baseline report conducted by CSIT).

The research team has also engaged with team leads that have noted a softened labour market, and some concentrated redundancies within some cyber security teams in Northern Ireland due to wider macroeconomic pressures. Further, review of job vacancy data by Perspective Economics suggests that in 2023, there were 629 job postings relating to cyber security in Northern Ireland (an average of 52 per month).

The first five months of 2024 suggests there have been only 179 new vacancies posted (an average of 36 per month) – indicating demand appears to have fallen by almost a third coming into 2024.

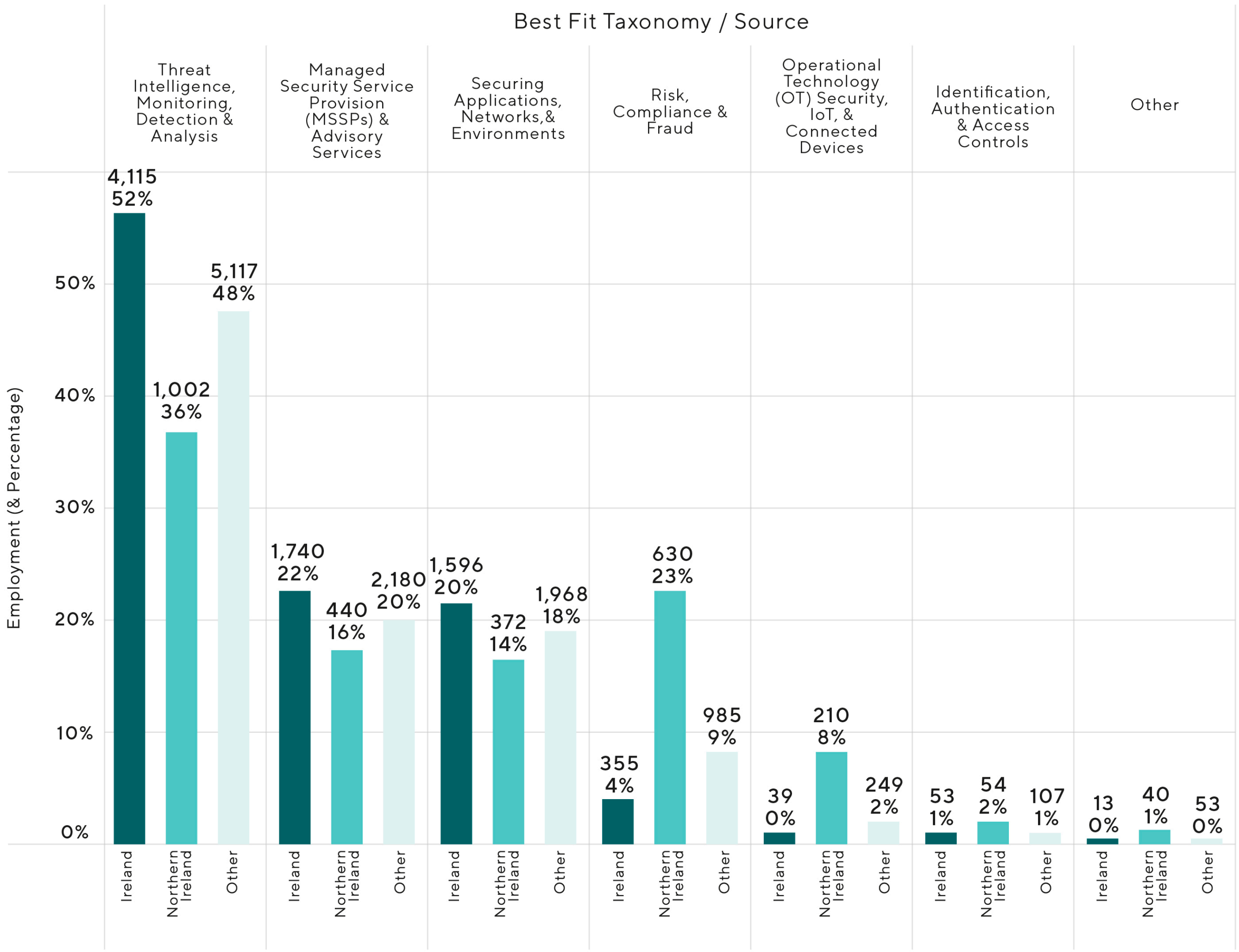
As such, whilst employment growth may have slowed in cyber security at a domestic and global level in recent years, there may be further opportunities to support indigenous firms to grow, increase access to cyber security managed service provision, or address increasing security risks in domains such as Critical National Infrastructure and the increased use of generative AI.

The employment data also provides some interesting insight into the variation between Northern Ireland and Irish employment markets in cyber security. Please note these are segmented by 'best-fit' so may omit some areas of employment activity; however, these do highlight areas of major employment activity and opportunity for respective markets.

Figure 1.9 highlights how Ireland's cyber security employment is typically driven by the presence of larger firms working in areas such as threat intelligence (4,115 FTEs, 52% of Irish cyber employment), and network and endpoint security (1,596, 20%), whereas Northern Ireland shares a similarly strong threat intelligence landscape, but also has a greater emphasis on risk, compliance and fraud (e.g. GRC roles, 630 FTEs, or 23%) and OT security.

Further, it also highlights how Ireland has stronger managed services employment (22% of roles compared to 16% in Northern Ireland), which in turn may suggest an area that could be considered by clusters and partners for growth interventions – particularly to support local and regional SMEs and public organisations further embed cyber security on a daily basis.

FIGURE 1.9 ESTIMATED ALL-ISLAND EMPLOYMENT BY MAIN TAXONOMY AND NORTH/SOUTH LOCATION



Source: Perspective Economics

Within the survey (in Summer 2024), respondents also typically reported that they expected to see moderate growth in cyber security employment within their firm in the next twelve months. 41% of respondents stated they expected moderate employment growth (c. >5%), and 32% stated they expect significant employment growth (>10%). 21% of respondents expected no change in cyber security employment, and 6% were not sure. Encouragingly, no respondents suggested that they expected their cyber security team size to decline in the next twelve months.

This may suggest a more modest landscape for employment growth in the years ahead, with firms seeking to ensure efficiency, recruit in the right areas, and invest in automation and infrastructure to enable further growth.

The survey also provided an opportunity for all-island cyber security businesses to provide feedback with respect to skills and employment. There were a number of thematic responses, summarised in the following pages:

A recognised shortage in cyber security skills, with a need for a sustainable pipeline:

Respondents recognised the wider shortage in cyber security skills across the island of Ireland, stressing the importance of industry bodies and government engaging at all levels (e.g. increasing awareness among school-leavers) to encourage increased supply and awareness.

This also suggests a role for cluster organisations and government in supporting trend analysis and workforce planning, that maintains an identifiable supply surplus to encourage sustained inward investment, without reaching 'full capacity'. One response noted that:

> "We have done really well over the past decade in building a strong cyber sector. However, we need to ensure we resource the talent pipelines, before we hit 100% utilisation, or we will hit a hard cap on growth in the sector... and either stagnate or end up in a pseudo-war with adjacent tech sectors for talent; in the time it will take to build the pipeline we always knew we needed."
>
> - IRISH CYBER SECURITY BUSINESS SITE LEAD

A need to differentiate between cyber security skills within the ecosystem

There are a wide range of cyber security career pathways and routes into the profession. There is no single homogenous route into a cyber security role; however, there are distinct areas of practice, which may overlap and work together. This is recognised within frameworks such as the European Cybersecurity Skills Framework (ECSF) which 'summarises cyber security-related roles into 12 profiles, which are analysed into the details of their corresponding responsibilities, skills, synergies and interdependencies' and the UK Cyber Security Council's Cyber Career Framework, which focuses on 16 specialisms.

The Cyber Ireland Cyber Labour Market (2023) research and CSIT Northern Ireland Cyber Security Snapshot (2023) research explored these roles in depth and found a strong demand among both ecosystems for engineering roles, SOC and security analysts, as well as wider Governance, Risk and Compliance (GRC) and project management skills. However, employers also require wider experience and backgrounds among applicants.

This is echoed by some of the qualitative feedback, which suggests a need to build the cyber ecosystem in areas such as risk and governance, and advisory skills. Further, encouraging delineation between skill-sets may also help to soften pressures on skills availability in product development in particular:

> "There are [several] apprenticeships entering the local market without the necessary background and applicable skills. The need is no longer with basic entry level roles in NI, but mid-level technical, risk and governance skills at competitive rates."
>
> - NORTHERN IRELAND CYBER SECURITY LEAD
>
> "[We need] more differentiation between cyber skills associated with product development versus cyber skills associated with provision of services"
>
> - IRISH WEB SECURITY PLATFORM

A need to create and foster a cyber security culture across the whole economy

Whilst this study identifies over 600 firms engaged in the cyber security sector, there is a sustained need to recognise the role that all organisations can play in furthering all-island development. For example, there are almost 400,000 registered businesses across the island of Ireland, in addition to thousands of public bodies, charities, and educational providers. These organisations can shape the ecosystem through behaviours, purchasing and procurement, skills development, reducing risk, and raising cyber security at board and operational levels.

Respondents have provided feedback to this extent, such as:

> “The SME sector is falling behind due to lack of resources to create a cyber secure culture. It is falling through the cracks and leaving them vulnerable to attack. An all-island cyber skills voucher or training grant scheme is essential.”

However, there is also a need to recognise commercial and operating pressures for many firms within the ecosystem. As reflected within the key headline statistics, cyber security is recognised as a ‘high-value, high-growth’ ecosystem, and as such firms also must offer attractive remuneration to staff whilst operating in a competitive labour market. There is a commercial need, particularly among managed cyber security service providers to ensure a sustainable client base, and to meet their requirements. This may mean that outsourced provision of cyber security services may be more concentrated among large and medium firms that can afford to pay, with smaller or micro firms with limited budgets or capacity ‘falling between the cracks’. As such, many smaller firms may have an IT provider for broader managed services for a monthly sum but may not be fully aware of their cyber security posture e.g. backups or incident response planning.

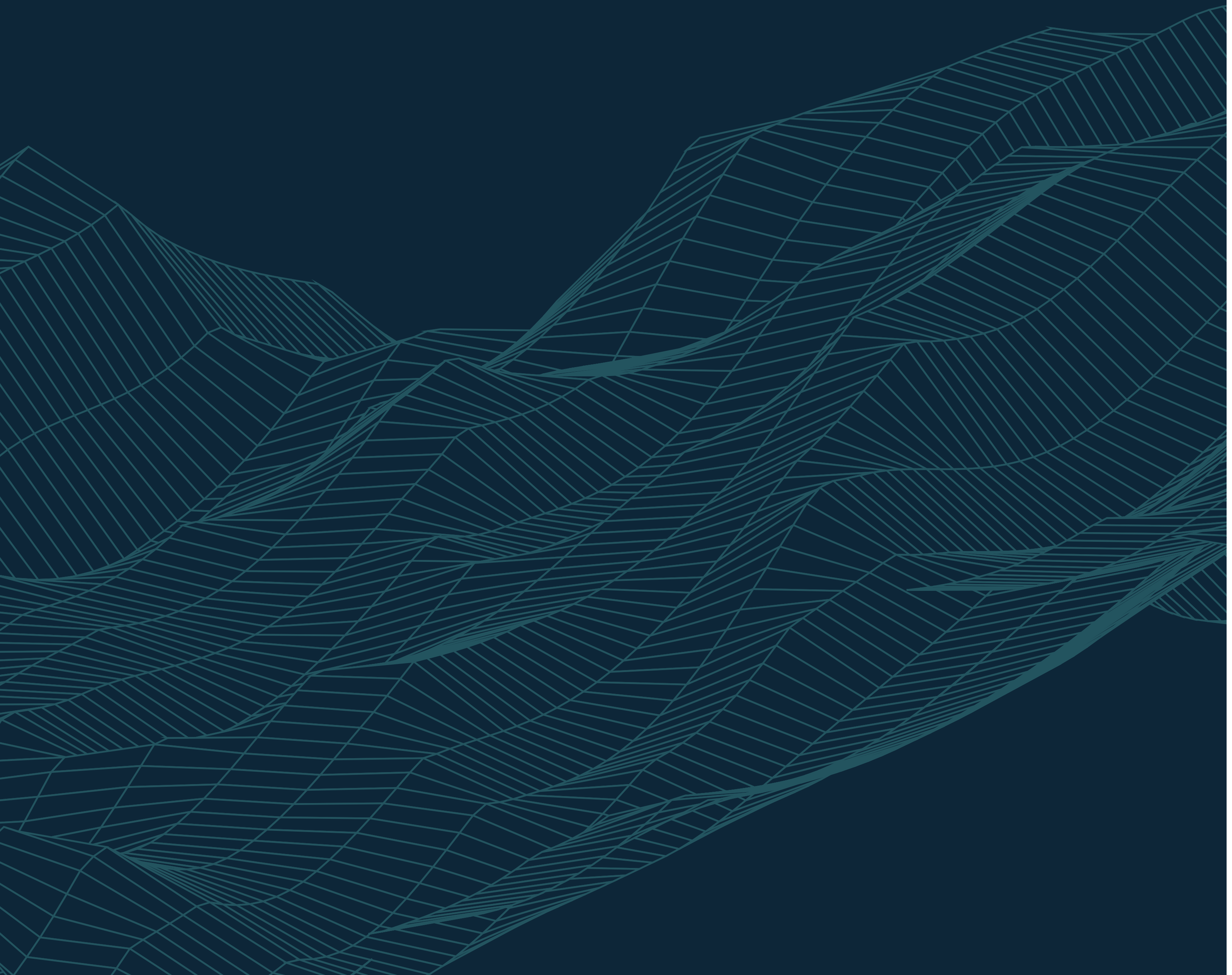
There is therefore a balancing act between increasing the potential domestic market for MSSPs and MSPs on the island of Ireland, but recognising the scale and range of potential buyers, and developing sufficient market intervention or support to enable greater market collaboration between SMEs and cyber security providers in a way that supports growth. This would require a step-change in supporting managed service providers be able to interact with the SME sector, through training and expansion support, and partnership working with government on areas such as standards. Initiatives such as the UK’s NCSC Cyber Advisor scheme may offer a template as ensuring smaller firms can access the support they need to implement a baseline standard of security.

Within the survey, many providers stressed the need for the right balance between grants provision as well as implementing standards such as ‘Cyber Essentials’ or similar within public procurement to help derisk public contracting and lift standards across SMEs. In 2023, Cyber Ireland piloted a Cyber Security Baseline Framework scheme with micro-enterprises (similar to Cyber Essentials).[6] An SME standard has been set out within the NCSC mid-term review, and is expected to be launched in 2025.

> "I often wonder if there was an opportunity to lobby government to provide grants to SMEs to have their cyber security status, at a minimum, assessed. Similar to the going online grant it would raise awareness in the sizeable SME market to the need to invest in cyber security tooling and expertise.”
>
> “The lack of Cyber Essentials in the Irish market is a gap between Ireland and the UK."

[6] https://cyberireland.ie/ci-four-pillars-cyber-security-baseline-framework/

06
Market Positioning

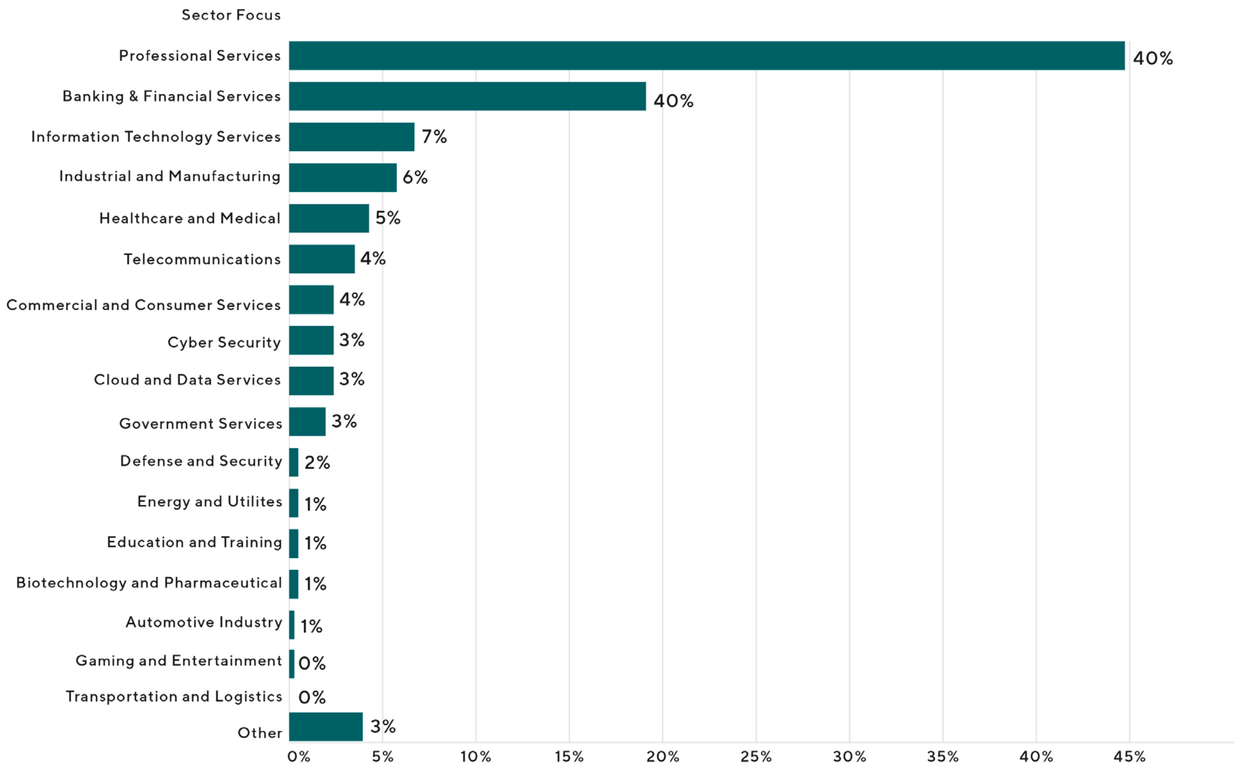


The all-island cyber security sector is home to a wide range of providers. Whilst there are areas of notable strength, such as attracting inward investment from global tech leaders, and deploying cyber security within a professional and financial services context in particular, the ecosystem's breadth is far-reaching.

Figure 1.10 highlights the primary area of sector focus among the 632 dedicated and diversified providers. These have been classified using a review of company web data and trading descriptions, to classify against a 'best-fit'. This primarily highlights the majority focus on services provision (e.g. cyber consultancy and managed services), as well as internal functions in banking and financial services (e.g. firms within which their cyber security teams are focused on mitigating user and financial risk).

However, it also highlights nascent engagement and overlap between cyber security teams working in, or with, sectors such as manufacturing (e.g. Wolfspeed, GM, JLR), healthcare and medical devices (e.g. Nova Leah, Stryker, McKesson, Boston Scientific), and wider critical sectors such as telecoms, cloud, defence, and energy (e.g. BT, IBM, Thales, Analog Devices etc). Many cyber security firms may also take a sector agnostic approach (e.g. their products or services can be deployed across a range of use cases.)

FIGURE 1.10 SECTOR FOCUS FOR ALL-ISLAND CYBER SECURITY FIRMS



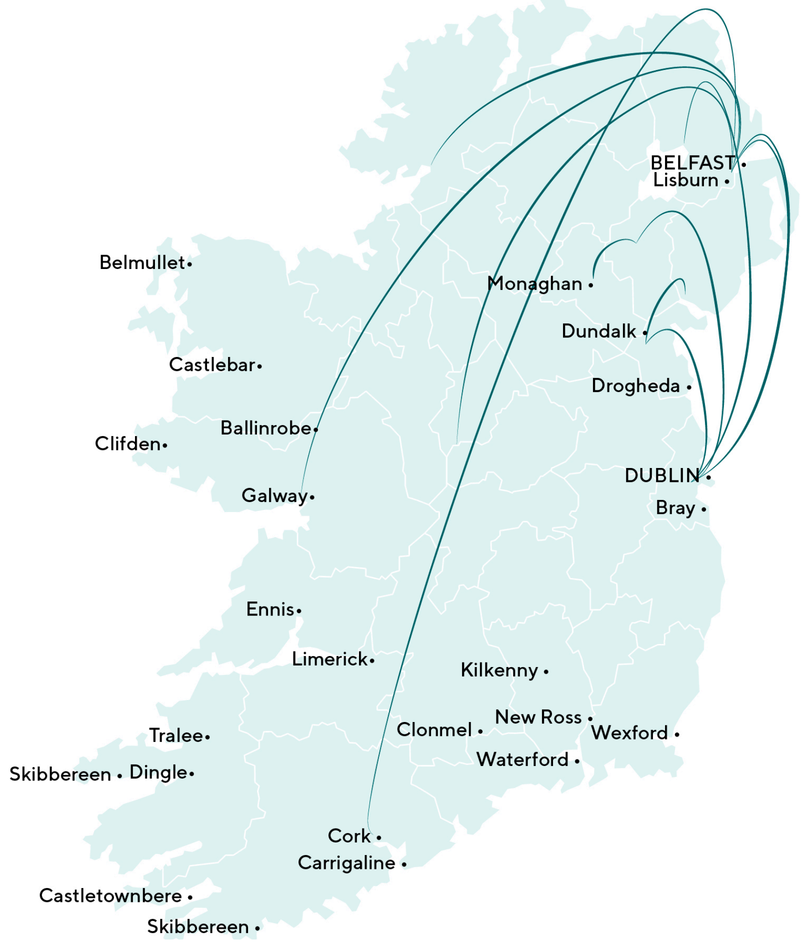
Source: Perspective Economics

07
Cross-Border and International Activity

Across the island of Ireland, there is extensive opportunity for cross-border engagement. This can take various forms, including establishing a physical presence in both jurisdictions (office-based), selling into respective markets,

Figure 1.11 highlights the estimated 42 cyber security companies with active offices in both NI and Ireland. Many of these are multinationals (e.g. large consultancies and IT firms); however, there is a small cluster of managed service providers active across both jurisdictions, particularly among those close to the border (e.g. Newry-Dundalk). Many of the larger firms may be physically present in both countries; however, may have separate and distinct teams working in cyber security serving respective markets without significant collaboration on a cross-border basis. The data and survey responses (set out in subsequent sections) suggest that whilst there is a willingness to engage in cross-border initiatives, there are practical barriers and challenges for firms, and mixed views regarding market opportunities (e.g. variations in pricing, taxation, and standards meaning that the perceived costs outweigh the benefits). This has the effect of limited evidence of cross-border activity within the secondary data to date but could suggest an opportunity to explore growth from a relatively low base.

FIGURE 1.11
CROSS-BORDER OFFICE LOCATIONS

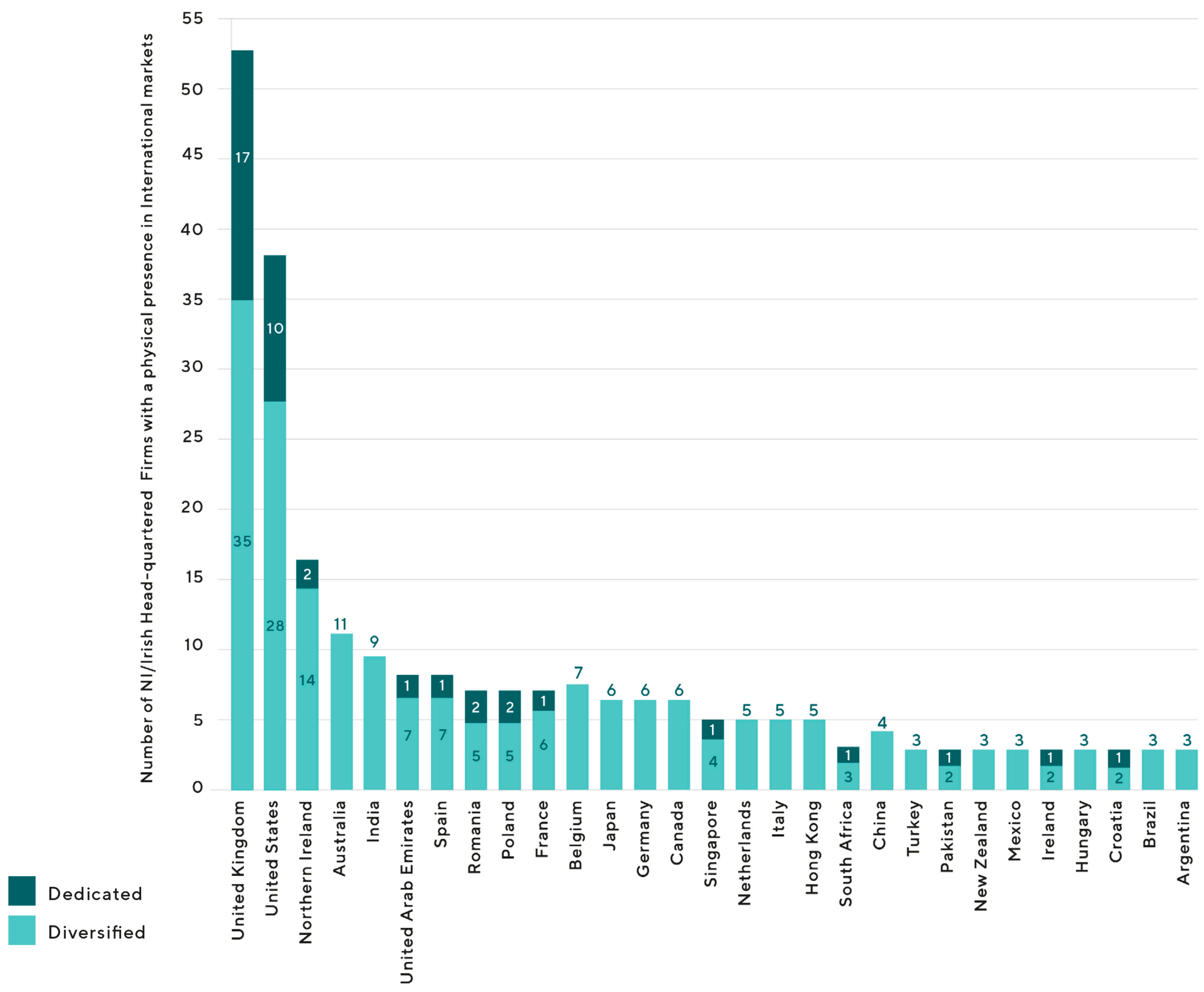


Source: Perspective Economics
N = 42 companies, 79 offices.

Figure 1.12 (a and b) also highlight that 95 headquartered Irish and Northern Irish cyber security firms (dedicated and diversified) appear to have international offices (including Irish firms with an NI office, or vice versa). This suggests that almost a third (32%) of Irish and Northern Irish headquartered cyber security firms have at least one external office. We include NI firms with a Great Britain office in Figure 1.11 as 'external sales' is a key tenet of supporting domestic cyber security firms to growth.

This data suggests that the United Kingdom (52 firms), United States (38 firms), Northern Ireland (for Irish firms only, 16), Australia (11) and India (9) are key international markets or partnership locations for Irish and Northern Irish firms seeking to grow internationally. We also find significant diversity and room for global partnerships – with 29 countries (regions) with more than three Irish or NI cyber security firms.

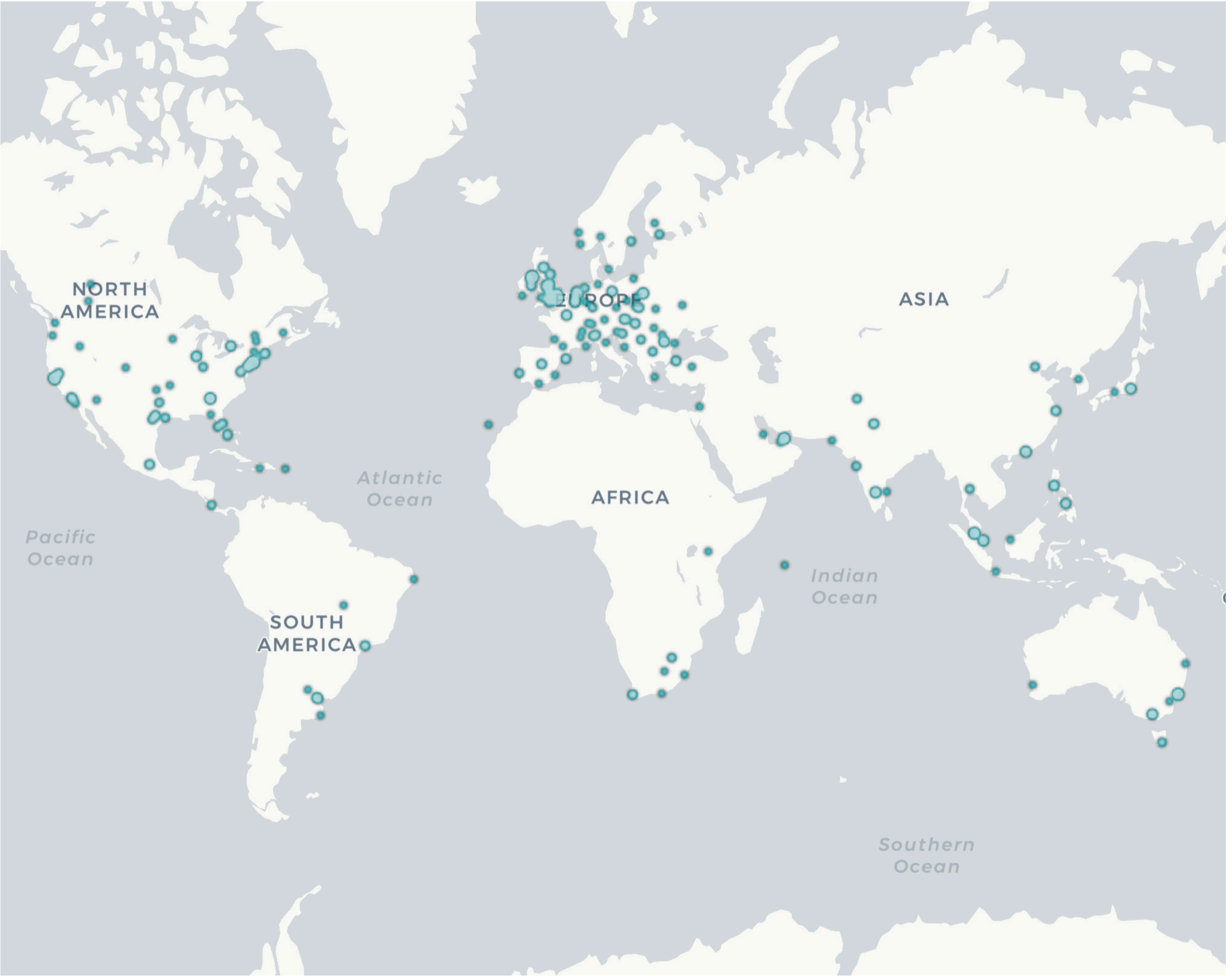
FIGURE 1.12A INTERNATIONAL LOCATIONS (FOR ALL-ISLAND HEADQUARTERED CYBER SECURITY FIRMS)



Source: Perspective Economics, n = 632

Figure 1.12b highlights the location of NI and Irish headquartered firms in other geographies, and also highlights the clustering within the US in particular, with all-island connections in areas such as New York, California, and Texas.

FIGURE 1.12B INTERNATIONAL LOCATIONS (FOR ALL-ISLAND HEADQUARTERED CYBER SECURITY FIRMS)



N = 431 offices across 95 headquartered Irish and Northern Irish cyber security firm (dedicated and diversified)

07
Routes to Market

As set out in previous sections, the all-island cyber security sector consists of a wide range of routes to market. This might include direct sales of products to other vendors (B2B), or directly to customers (B2C), or selling cyber security managed and advisory services, often working in tandem with strategic partners to resell solutions to market. Further, many cyber security teams in the all-island sector have been established to provide security support or enrichment to wider teams, and whilst they may not have to directly sell cyber security products or services, they will be critically important as buyers, collaborators, and skilled practitioners. For example, the Northern Ireland ecosystem has particularly strong expertise in fraud and risk, developed through building cyber security talent within global financial services firms.

Web data can provide some insight into routes to market, as shown in previous sections. Further, many established cyber security providers across the island have developed extensive case studies outlining their reach and indicative buyers.

Within the survey, the majority of respondents stated that their main route to market is direct sales (77% selling products or services directly to their customers). A further 40% reported that they used partnerships, and 35% undertake reselling. This will primarily include MSSPs or vendors that sell a security solution via a cloud platform. There may also be value in mapping the supply chain of these providers in future research.

The survey also suggests that 9% of respondents avail of grant or research funding. Whilst the survey is limited with respect to response rate (76 unique business responses), applying this across the wider cohort suggests there could be an extensive range of start-ups or spin-outs that may benefit from sustained sources of grant and research funding. For example, many of the businesses identified within the cyber security ecosystem have benefitted from funding through organisations and initiatives such as Innovate UK, Cyber Runway, LORCA, CSIT Labs and Enterprise Ireland support.

The MTU Cyber Innovate[7] programme, alongside CSIT's Cyber-AI Hub[8] initiative, also offer two strong examples of how universities can be a catalyst to support increased innovation and entrepreneurship, driven by world-leading research, across the island of Ireland. Collectively, these two initiatives alone represent a public investment of almost €20m in the island's cyber security ecosystem.

These initiatives and funding can also support productisation and commercialisation within academic start-ups, and encourage a pipeline of novel and innovative solutions, which can subsequently drive partnerships and export growth. Further, they can help early-stage firms unlock initial customer growth or provide a signal to investors regarding growth potential.

[7] https://www.enterprise-ireland.com/en/news/-7m-enterprise-ireland-investment-in-mtu-s-cyber-innovate-will-supercharge-ireland-s-cyber-security-innovation-ecosystem
[8] https://www.qub.ac.uk/ecit/CSIT/Cyber-AIHub/

Further, we estimate that up to 37% of providers (236) are likely to focus mainly on internal provision in cyber security only i.e. the cyber security teams on the island of Ireland are focused on areas such as R&D or securing wider product or service infrastructure. These may not have a direct 'revenue stream'; however, should be encouraged to scale and grow where possible. For example, this can support the development of highly-talented teams with a particular focus on certain cyber security domains (e.g. fraud prevention in insurance) which in turn can attract further inward investment and grow the workforce. For example, in Northern Ireland, the focus on cyber security by firms such as Allstate and Citi over recent years has arguably supported the growth and expansion of firms such as Aflac – and helped to support the development of an ecosystem that understands the application of cyber security within financial and insurance services.

EXPORT ACTIVITY

Exports are critically important to the success and growth of the all-island economy. Cross-border trade is a key component, but both Ireland and Northern Ireland have been globally recognised as attractive locations for inward investment, which in turn has supported an array of partnerships and opportunities for domestic firms to sell to international markets.

The previous sections set the reach of firms identified by office locations. This offers some insight into how cyber security firms interact with geographical markets, including an assessment of inward investment by international firms, and in turn – where Irish and Northern Irish headquartered firms are present in international markets.

We estimate that, based on web data, of the 96 'dedicated' cyber security firms headquartered in Ireland or Northern Ireland, 31% (30) have at least one physical office in another jurisdiction.

However, this is a proxy measure based on physical location. Some firms may have R&D or development teams in international markets without necessarily exporting, and other firms will have no physical presence, but could be exporting to multiple jurisdictions.

Within the online survey, 61% of respondents reported that their firm conducted some form of export activity. Of these that exported, the major market was other EU / EEA countries (89%), followed closely by Great Britain (excl. Northern Ireland) (87%), and North America (72%). 41% also exported to the Middle East, and 37% to Asia Pacific.

CROSS-BORDER TRADE

Two-thirds (67%) reported cross-border trade activity; however, this may be a high estimate given the wider secondary data and some of the feedback from stakeholders within the survey.

For example, some feedback included a range of perceived challenges faced in cross-border trading, including perceived risk of duplication or exclusion based on physical locations, as well as variation in standards, governance, and business taxation between jurisdictions:

> Government policy, while promoting an all-island approach, seems to implement a separation in practice. The existence of two cyber clusters on the island appears to contradict the stated goal of an all-island market. Many opportunities within the ROI are exclusively shared with the ROI Cyber Cluster, necessitating both a physical location and staff within the ROI to participate. This requirement effectively excludes those outside the ROI from these opportunities, which is contrary to the spirit of all-island cooperation.
>
> – SMALL NI BASED CYBER ADVISORY FIRM **(Representative Comment)**

> Many ROI opportunities are only shared among the ROI Cyber Cluster and to join you must have a staffed office in the ROI, effectively excluding small NI companies. This structure does not support the concept of an all-island market.
>
> – SMALL NI BASED CYBER ADVISORY FIRM **(Representative Comment)**

> Collectively, the cyber security industry in Ireland and NI should be more aligned - I don't feel it is so much today
>
> - LARGE MULTINATIONAL ENDPOINT SECURITY FIRM

> The SC and Baseline security requirements for all UK and NI work cause difficulty at times as the clearance requirement for criminal background checks is not something available from ROI Garda.
>
> - MEDIUM IRISH BASED MSSP

> Entry for Irish businesses into Northern Ireland has been difficult due to cost base being substantially lower in NI *[i.e. variations in pricing structures across jurisdictions].*
>
> - SMALL IRISH MANAGED SERVICE PROVIDER

However, the majority of stakeholders welcomed the opportunity for additional events and collaborative sessions to bring the community together across the island, with a focus on market engagement, skills and knowledge sharing:

> An all-island approach to the market, encouraging collaboration between Cyber NI providers and Cyber ROI providers would be welcomed - similar to Meet the Buyer formats that InterTradeIreland has run.
>
> - MEDIUM IRISH BASED MSSP

> There seems to be a strong grass roots community of security practitioners in various parts of Ireland. Key opportunity may be collaboration between different industries for more diverse learning and sharing.
>
> - MULTINATIONAL FINANCIAL SERVICES FIRM WITH AN IRISH CYBER SECURITY TEAM

> To aid developing an all-island market, more networking events on both sides of the border would help in opening up opportunities for companies based on the island.
>
> - DEDICATED IRISH CYBER SECURITY MSSP

The all-island cyber security sector may also stand to benefit from initiatives such as InterTradeIreland's First Time Exporters Accelerator scheme.

08 Growth Expectations, Barriers and Support

The online survey also asked cyber security organisations across the island of Ireland regarding their growth expectations for the next twelve months, and the wider barriers they face, and support they would most welcome from clusters and public organisations. We summarise these findings below.

GROWTH EXPECTATIONS:

As explored within the key economic estimates for the all-island sector, we estimate that revenue growth has been strong (for Irish firms) over the last two years, with an estimated CAGR of 13.4%. The UK Cyber Security Sectoral Analysis (2024) also estimates that the UK cyber security grew its revenue in the most recent financial year by 13%.

However, this revenue growth takes place within wider challenges in the market, such as inflationary pressures, increased salary costs, and disruption to the labour market. Further, for many firms, whilst revenue growth has been strong, the growth in underlying profitability and productivity has been more modest. We estimate Irish cyber security GVA CAGR of approximately 4.5% over the previous two years (5% in the UK for comparison).

Further, the employment data suggests that, whilst the all-island cyber security sector was growing employment by approximately 10% per annum between 2019 – 2022, the last couple of years (2022-2024) have seen much more modest employment growth – approximately 4% in Ireland and 2% in Northern Ireland (compared to 5% at a UK level).

This suggests that cyber security firms are exploring their commercial and market-fit and reviewing their growth strategies within the context of wider pressures faced by customers and buyers. We expect to see slightly stronger growth in underlying revenue and Gross Value Added within the all-island sector in the coming years (between 5% - 8%); however, expect employment growth may be more subdued (up to 5% per annum).

However, lower employment growth may reduce opportunities for firm expansion, and incentives or further collaboration between training providers and industry may help to catalyse further opportunities to support early-stage talent.

This is echoed within the survey findings. Within the survey, employers were optimistic about their trading conditions. 51% of firms stated they expect to see significant growth (>10%) in cyber security related revenues in the next 12 months, with 33% expecting moderate growth (>5%). Only 7% of respondents expected no change, and 9% were unsure or preferred not to say.

In comparison, when asked about their expectations for cyber security team size, only 32% stated they expected to see significant growth (>10%), with 41% expecting moderate growth (>5%), and 21% anticipating no change. This suggests that employers are three times more likely to expect their team size to remain static compared to revenue – suggesting a slower growing labour market into 2024.

We recommend that these core metrics should remain tracked by Cyber Ireland and NI Cyber, to understand the extent of trend data, and need to revise workforce planning estimates.

BARRIERS AND SUPPORT

Within the survey, respondents were asked about their particular barriers to growth (with respect to all-island activity where relevant). Key feedback included:

Perceived Policy and Implementation Gaps

Some stakeholders noted a perceived discrepancy between the promotion of an all-island cyber security market and the implementation of such policies across two jurisdictions. For example, some stakeholders raised that further collaboration between Cyber Ireland and NI Cyber, or the removal of barriers regarding business registration location may help to support a more unified market. Further, there may also be wider administrative barriers facing SMEs in this area e.g. the need for dual-checks, or additional tax planning burdens (e.g. reclaiming VAT from services sold in the other jurisdiction). Sharing knowledge about common barriers and how to mitigate these when trading on an all-island basis may be beneficial in this area.

Security Clearances and Background Checks

The lack of a standardised security clearance process and the difficulty in performing criminal record checks between jurisdictions pose significant barriers to many services led firms. This can limit participation in certain projects, and some firms also raised challenges in compliance regarding data handling requirements between jurisdictions.

Public Procurement and Tendering Issues

Several stakeholders noted that current public procurement processes and tendering for cyber security services are seen as inefficient and restrictive, particularly for SMEs. There is a perceived need for reforming public procurement systems to make them more accessible to both Irish and NI companies or encourage joint applications from firms on a cross-border basis. Further, public procurement is seen as a market that could be used to stimulate demand e.g. requiring tenderers in Northern Ireland to hold Cyber Essentials where servicing certain markets or contract values, or to develop similar standards in Ireland. Enabling public buyers to work with (or integrate) smaller firms within their supply chains would also increase opportunities to sell and scale among indigenous firms.

There is also a strong call for government grants and training schemes to support SMEs in enhancing their cyber security posture to stimulate demand. Some stakeholders recommended an 'all-island Cyber Skills Voucher / Certification Scheme' or similar for small businesses, promoting a secure culture and enabling participation in larger markets.

A Need to Support Commercialisation and Product Development

Some stakeholders highlighted the need for increased support in commercialising research and developing new cyber security products. This could involve providing resources, mentorship, and funding to help SMEs and startups bring their innovations to market. Establishing dedicated incubators or accelerator programs focused on cyber security could foster collaboration between academia, industry, and government, facilitating the translation of research into viable products and services. Additionally, creating opportunities for SMEs to showcase their solutions and connect with potential customers or investors could help bridge the gap between development and commercialisation.

A Need to Derisk Innovation and Encourage Further Investment

Stakeholders emphasised the importance of creating a supportive environment that encourages investment in cyber security innovation. One suggested approach is the establishment of sandboxing facilities, which provide a controlled testing environment for new cyber security solutions.

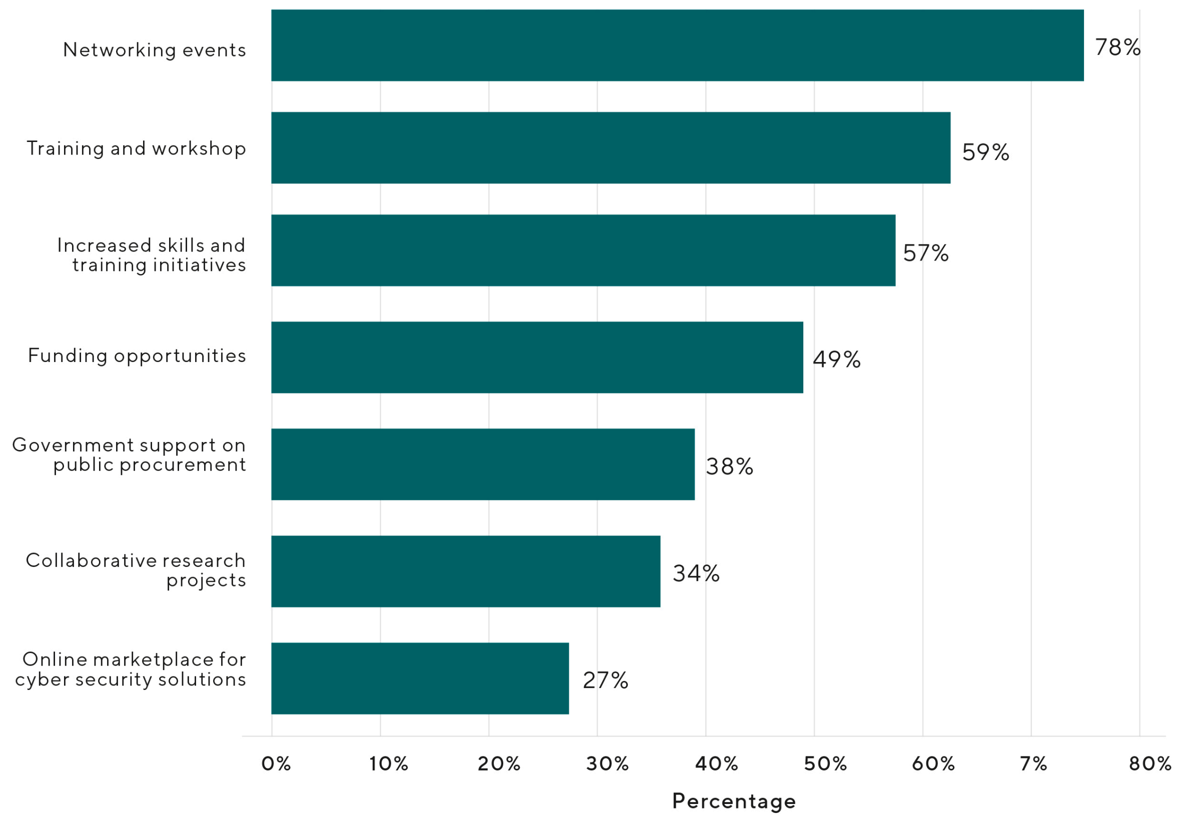
These sandboxes would allow companies to validate their products, assess their effectiveness, and identify potential vulnerabilities in a safe setting. By derisking the innovation process, sandboxing facilities can attract more investment and encourage the development of cutting-edge cyber security technologies. Furthermore, offering tax incentives, grants, or other financial support mechanisms could incentivise private sector investment in cyber security research and development.

Increasing the Understanding of Cyber Security Adoption Across the Island of Ireland

To effectively support the growth of the cyber security industry, stakeholders highlighted the need for a comprehensive understanding of the current state of cyber security adoption across the island of Ireland. This could involve conducting a survey similar to the UK Cyber Security Breaches Survey, which assesses the level of cyber security awareness, preparedness, and incidents among organisations. The survey should cover a wide range of organisations, including those in scope of the Network and Information Systems (NIS) Directive 2, those positioned for Cyber Essentials certification, and the wider market. The insights gained from such a survey would help identify areas where support and resources are most needed, inform policy decisions, and guide the development of targeted initiatives to improve cyber security posture across various sectors. Additionally, the survey results could serve as a benchmark for measuring progress and evaluating the effectiveness of cyber security interventions over time (e.g. take up of outsourced or managed services, or availability of internal skills, or engagement with NCSC resources or similar).

Within the online survey, respondents were asked to select (as many that applied) which forms of support that they would like to see to enable collaboration and growth on an all-island basis. These are summarised in Figure 1.13. below:

FIGURE 1.13 WHAT SPECIFIC SUPPORT IS REQUIRED TO SUPPORT COLLABORATION AND GROWTH IN THE CYBER SECURITY SECTOR ACROSS IRELAND AND NORTHERN IRELAND?



Source: Survey of Firms (n = 76 unique responses)

Whilst all of these are potentially valuable interventions, particularly where targeted to relevant businesses, this provides some insight into the highest priority areas for Cyber Ireland, NI Cyber and wider stakeholders to consider. The vast majority of respondents (78%) stated they would like to see more all-island networking events, with some respondents noting opportunities to bring certain geographic or sub-sectoral clusters together (e.g. a 'Cork-Belfast axis'). Networking events are also seen as relatively low-cost but high-reward where these can be organised to meet industry needs and interests. However, this requires ongoing support for administrative and networking resources for the clusters to ensure quality events are delivered.

The vast majority of respondents (78%) stated they would like to see more all-island networking events.

The survey also highlights that **59% of respondents would like to see direct support for training and workshops,** in technical and sales areas in particular.

Whilst broad, 49% of respondents would like to see additional funding resources, or a standardisation of opportunities for funding (e.g. direct cross-border funding for joint initiatives (34%), or funding to support collaboration and cross-border partnerships). Further scoping should be undertaken to gauge the extent of this demand, and reduce potential duplication across the ecosystem; however, initiatives such as CSIT's Cyber-AI Hub do suggest a significant demand for market-led innovation, where match-funding for innovative projects could help to catalyse increased market positioning for firms. The return on investment for cyber security project funding should also be tracked to make a sustained investment case for infrastructure, skills, and collaborative funding.

Respondents also stressed the importance of government reform of public procurement (38%) in both Ireland and Northern Ireland to grow the market. This has a wide range of impacts. For example, embedding standards (Cyber Essentials or ISO 27001 or similar) within procurement by all suppliers would help to increase demand for cyber security consultancies, whilst also increasing the security of public sector supply chains and reducing risk with respect to data privacy and loss. Further, government and supporting agencies can also set norms, culture, and advice to wider businesses e.g. what to do in the event of a ransomware attack. There is a sentiment within the survey responses that an increased grasp of cyber purchasing is required to understand how the domestic market can be grown in a commercially realistic way. An all-island Cyber Breaches Survey or similar may help to address some of these challenges to understand usage of managed services, average and median spend, and estimate the market opportunity for indigenous cyber security service providers.

Notably, only 27% felt that an 'online marketplace for cyber security solutions' would be a key area to help support the sector.

In principle, this would support the mapping and sharing of providers across the island, and act as a conduit between buyers and suppliers. Similar initiatives exist across the UK and Europe e.g. CyberExchange and ECSO Marketplace. However, there is mixed evidence regarding their usage, efficacy, and coverage. This should be considered significantly by the clusters or scoped to ensure maximum value for money and coverage (e.g. simple lists of providers and contact details).

09
Key Findings and Recommendations

KEY FINDINGS

01 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 sector 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.

02 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 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.

03 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.

04 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.

05 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.

06 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.

07 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 (and wider innovation programmes such as CSIT Labs and Cyber Runway) 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.

08 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.

09 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. However, the reported 67% cross-border trade activity in the survey may be a high estimate given the broader secondary data and stakeholder feedback on challenges faced in cross-border trading. Supporting firms in navigating these challenges and expanding their international presence will be crucial in enhancing the sector's global competitiveness.

RECOMMENDATIONS

01

IMPROVING ALL-ISLAND COLLABORATION:

- **Review and address direct barriers to collaboration, such as business location requirements,** to ensure that all companies across the island can avail of collaborative support, and access cluster organisations.
- **Explore practical mechanisms to facilitate equitable access** to opportunities and resources (e.g. how NI firms can access Cyber Ireland initiatives and vice versa) (e.g. virtual registrations).
- **Collaborate with wider public bodies to understand and mitigate perceived policy gaps** (e.g. North South economic collaboration), **security clearance** issues (PSNI / An Garda Síochána), and **public procurement** processes - which were highlighted by survey respondents as hindering cross-border collaboration.

02

INCREASING KNOWLEDGE-SHARING AND NETWORKING EVENTS:

- **Review and address direct barriers to collaboration, such as business location requirements,** such as "Meet the Buyer" sessions, to foster connections, share insights, and create opportunities for firms to engage with potential clients and partners across the island.
- **Leverage the diverse range of product and service offerings** to facilitate knowledge exchange and collaboration across different areas of expertise in unique targeted events.
- **Respondents placed a stronger emphasis upon supporting network building and collaboration events compared to an 'online marketplace for cyber security solutions:** The evidence regarding the efficacy of online marketplaces is limited, and the clusters should consider this prior to any significant investment in an online marketplace initiative.

03

LEVERAGE PUBLIC PROCUREMENT TO DRIVE GROWTH AND INNOVATION:

- **Advocate to national and local government in both jurisdictions to recognise the power of procurement** in supporting small cyber security providers to attract initial revenue, secure external investment, and de-risk early-stage technologies – which also growing the market and enhancing public sector security. This could also include brokering relationships between cyber start-ups and innovation initiatives
- **Streamline procurement processes** to make it easier for vendors to bid, view opportunities, and engage with buyers, addressing the concerns raised by several stakeholders about current processes being inefficient and restrictive, particularly for SMEs.
- **Enable buyers to identify gaps more effectively in their cyber security posture and invest in appropriate solutions** e.g. funding for local government and public body cyber security organisational reviews to stimulate local demand. Monitor local and SME engagement with public contracting.
- **Mandate minimum cyber security standards for all government suppliers to stimulate demand and raise the bar for security across the island,** as highlighted by survey respondents who noted the lack of such necessary standards in the Irish and Northern Irish market compared to the UK.

04

SUPPORT SME ADOPTION AND PRO-ACTIVELY TARGET MSSP GROWTH:

- **Undertake research to assess the current state of cyber security adoption among SMEs and inform targeted interventions,** as highlighted by stakeholders who emphasised the need for a comprehensive understanding of the current state of adoption across the island (e.g. by size, sectors, locations).

- **Assist MSSPs in planning for growth,** ensuring that Irish SMEs have access to high-quality, specialised cyber security services beyond general IT support - and that any regulation or requirement for minimum standards can be adequately met and planned by industry.

- **Collaborate with industry to design appropriate grant schemes that incentivise SME adoption of cyber security measures and make it more attractive for MSSPs to serve smaller clients,** as survey respondents stressed the need for the right balance between grants provision and implementing standards to help de-risk engagement and lift standards across SMEs.

05

FOSTER INNOVATION THROUGH CROSS-BORDER AND INTERNATIONAL INCUBATORS:

- **Establish cyber security incubators and accelerator programs that span both jurisdictions and have an international outlook,** building on the success of initiatives such as the MTU Cyber Innovate program and CSIT's Cyber AI Hub, which collectively represent a public investment of almost €20m in the island's cyber security ecosystem.

- **Organise and promote all-island visits to key global markets, such as the USA, to expose startups to new opportunities, investors, and potential partners,** leveraging the existing international presence of Irish and Northern Irish firms.

- **Provide tailored support to help innovative firms scale, access funding, and bring new products and services to market,** as the survey findings suggest that 9% of respondents avail of grant or research funding, indicating a potentially extensive range of start-ups or spin-outs that could benefit from **sustained sources of support, or be encouraged to participate in cluster initiatives.**

06

DEVELOP AND IMPLEMENT AN ALL-ISLAND CYBER SECURITY STRATEGY:

- **Create a comprehensive all-island cyber security cluster strategy** to build on the newly mapped sector, and further explore strengths, opportunities, and barriers. This strategy could include:

  - Promotion initiatives to showcase the sector's capabilities, including an online presence (e.g., dedicated webpage) featuring an interactive All-Island Sector Map or Dashboard.

  - A biennial update of the sector mapping to track progress and identify emerging trends.

  - An annual all-island cyber security event or conference to foster networking, knowledge-sharing, and collaboration.

  - Dedicated funding and resourcing to support the strategy's implementation, drawing inspiration from successful cross-border initiatives in other sectors (e.g. InterTradeIreland's cross-border trade roadshows).

  - Collaborate with key stakeholders across both jurisdictions, including government agencies, industry representatives, and academic institutions, to ensure the strategy aligns with broader economic and security objectives.

- Establish clear metrics and milestones to measure the strategy's impact on sector growth, cross-border collaboration, and international competitiveness.

CYBER | IRELAND
IRELAND'S CYBER SECURITY CLUSTER

NI CYBER

Perspective
Economics