CYBER|IRELAND
IRELAND'S CYBER SECURITY CLUSTER

CYBERSKILLS
BUILDING IRELAND'S CYBER SECURITY SKILLS

Perspective
Economics

2022 EDITION

State of the Cyber Security Sector in Ireland

Contents

Cyber Ireland Foreword

This inaugural "State of the Cyber Security Sector in Ireland 2022" Report, commissioned by Cyber Ireland and Cyber Skills, and funded by Enterprise Ireland under the Regional Technology Cluster Fund, is the first complete study on Ireland's cyber security sector. It assesses its economic contribution to Ireland's economy, benchmarks against other regions and explores potential sectoral opportunities.

This report has identified almost 500 companies in Ireland's cyber security sector, employing over 7,500 people. It demonstrates the economic contribution of the sector with revenues of €2.1b in 2021, generating approximately €1.1b in Gross Value Added. That's €150k per employee, signalling a productive workforce and compares favourably to strong international cyber security regions. It is positive to see the regional diversity that this sector is supporting with employment nationwide.

There is a clear cyber opportunity of 17,000 jobs and €2.1b GVA by 2030. To realise this, work must continue to ensure we strengthen our cyber security preparedness across all sectors, to support a resilient and prosperous economy and society. This can only be achieved by industry working with our partners in government and academia.

The continued growth of Ireland's cyber security cluster is one of Ireland's tech success stories. I would like to thank everyone working in cyber security for their contribution, and we will continue to do all we can to help make Ireland a safe and secure place to live and work online.

Eoin Byrne

DR EOIN BYRNE,
CLUSTER MANAGER, CYBER IRELAND

Cyber Skills Foreword

Ireland's economy, driven by key national strategies i.e. Enterprise 2025 Renewed, Ireland Industry 4.0 Strategy and Project Ireland 2040, is increasingly becoming more digital, presenting enormous opportunities for economic growth. However, cyber security is putting advancements associated with digitalisation at risk and is seen as the Linchpin in building the digital resilience necessary to future proof our businesses. Investment to support this strategically important topic, is essential to maintain Ireland's competitive advantage as a safe place for digital business and to establish the national trust needed for future inward investment and indigenous digital innovation.

This report is timely, as it is the first time Ireland has mapped and profiled Ireland's cyber security sector highlighting its importance as an industry, economic contribution and opportunities for further growth. This report in turn, will allow government agencies to inform future national policies, funding agencies to prioritise research funding in sectoral applications where Ireland is a leader and academic institutions to respond to industry skills needs.

As lead of the HEA Cyber Skills project, I was delighted to work in partnership with Cyber Ireland, in commissioning and developing this report.

I look forward to working with industry, government agencies and academic partners, to further develop and support the sector going forward, across skills, training and research.

PROF. DONNA O'SHEA,
CHAIR OF CYBER SECURITY AT MTU

Executive Summary

This report (State of the Cyber Security Sector in Ireland 2022) has been independently commissioned on behalf of Cyber Ireland and Cyber Skills, led by Perspective Economics. It outlines the size and make-up of Ireland's cyber security sector, assessing its economic contribution to Ireland's economy, in addition to benchmarking and exploring potential sectoral opportunities.

> The report is an economic baseline for the sector and will form the basis of future recommendations and policies within Cyber Ireland.

KEY FINDINGS

The following sections set out the key findings from the economic analysis. Full definitions and methodology are set out within the report.

NUMBER OF FIRMS AND EMPLOYMENT

There are 489 firms offering cyber security products or services to the market or employing staff in internal cyber security operations in Ireland.

Approximately a third of cyber security firms offer dedicated (or pure-play) cyber security services, whereas the remaining firms offer diversified services (i.e., cyber security is part of a wider company offering).

There is a relatively even split between the count of large firms and SMEs in the sector, and almost half of all cyber security firms operating in Ireland are indigenous.

The sector employs 7,351 cyber security professionals in Ireland. Teams are typically small, and nearly two-thirds of firms employ between one to nine cyber security professionals.

Foreign direct investment plays an important role in Ireland's cyber security sector, supporting c.71% of all employment in the sector. Cyber security firms headquartered in the United States have a particularly strong presence in Ireland, making up 28% of firms and supporting c.55% of all employment.

CYBER SECURITY RELATED REVENUE AND GVA ESTIMATES

It is estimated that in the most recent financial year (2021), annual cyber security-related revenue in Ireland reached approximately €2.1bn.

It is also estimated that Ireland's cyber security sector generated approximately €1.1bn in GVA[1] in 2021. GVA per employee within the cyber security sector is strong in Ireland (€150k) signalling a productive workforce. This compares favourably to the UK estimate of c. £100k (c. €120k).

This analysis suggests that the cyber security sector is growing (with respect to the workforce) in Ireland by a similar magnitude to international growth (at a rate of 10%+ per annum). This suggests that based on the current baseline estimates, Ireland's cyber security ecosystem could support up to €2.5bn in annual GVA and the employment of over 17,000 cyber security professionals in the sector by 2030.

PRIMARY LOCATIONS

- There are 734 offices identified for the 489 cyber security firms nationwide. There are four particularly notable locations for cyber security activity in Ireland (Dublin, Cork, Galway, and Limerick). These are collectively home to 73% of all cyber security offices, but cyber security activity can be seen across the country.
- While Dublin is home to more offices overall, both Cork and Galway have more firms per capita and host a range of assets that support the development of a thriving cyber security ecosystem.

PRODUCTS AND SERVICES

- Main products and services offered by firms include managed security service provision and advisory services (offered by 36% of all firms), securing applications, networks, and cloud environments services (31%), and risk, compliance, and fraud services (28%).
- Other products and services include threat intelligence, monitoring, detection and analysis (26%), operational technology security and connected devices (13%), and identification, authentication, and access control (11%).

[1] 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.

Recommendations

There are a range of recommendations that should be considered by government, industry and academia to help promote sustainable growth within the sector.

These include:

01 Developing a talent pipeline

02 Government's role in supporting the sector through awareness, procurement, and business support

03 Promoting clusters and collaboration

RECOMMENDATIONS CONTINUED OVERLEAF →

DEVELOPING A TALENT PIPELINE:

01 There should be an increased emphasis on **developing a pipeline of suitable talent to support sustainable growth within the sector.** This could involve engagement with industry to ensure existing courses offer a curriculum that prepares students for a career within the sector, teaching them the skills necessary to engage at an entry-level. There is also potential to promote cyber security to students in wider STEM or IT courses by encouraging universities to offer relevant cyber security modules to more general learning.

02 **Further initiatives such as reskilling and retraining could also promote entry into the cyber security sector.** There is a good baseline of technical talent in Ireland also, with current estimates suggesting that there are c.80k professionals engaged in technological sectors in Ireland[2]. There is potential to support firms by developing transition courses or training schemes to support entry from other industries to address skill shortages.

GOVERNMENT'S ROLE IN SUPPORTING THE SECTOR THROUGH AWARENESS, PROCUREMENT, AND BUSINESS SUPPORT:

03 Public sector commitment to supporting cyber security services has increased, which could help Ireland improve national resilience. **The recent attack on the HSE should demonstrate the importance of investment in cyber security, and the requirement for increased integration of cyber security practices across all aspects of society.** Ireland can also learn from international models undertaken in countries such as the UK, Estonia, USA and Israel.

04 Public procurement is a powerful mechanism for increasing spend on cyber security and promoting resilience across the Irish economy. Within the business survey, conducted for this research, many firms report that specifications for tenders can be restrictive and difficult to engage with. **We suggest that there is potential to engage further with cyber security SMEs to help co-create inclusive and impactful tender opportunities, which would also help cyber security SMEs to scale domestically.**

[2] An Rionn Fiontar, Trádála, agus Fostaíochta | Department of EnterpriseTrade and Employment (2022). 'Attracting Tech Talent to Ireland'. Available at: https://enterprise.gov.ie/en/What-We-Do/Workplace-and-Skills/Skills-for-Enterprise/Attracting-Tech-Talent-to-Ireland/

05 Many cyber security SME firms reported that they are experiencing a competitive labour market, in particular, competing with salaries offered by larger firms. The government could consider **supporting the development of the domestic ecosystem through the use of grants and initiatives to support employment growth within start-ups and scale-ups.**

06 The success of cyber security services hinges upon their application across different global regions. The composition of Ireland's sector suggests that foreign-owned firms have been particularly successful in developing cyber security teams in Ireland. **Ireland's expertise and attractiveness as a location for setting up cyber security teams could be used to encourage further investment from external firms seeking to further develop their cyber security capability and capacity.**

PROMOTING CLUSTERS AND COLLABORATION:

07 Sector composition indicates that domestic firms in Ireland typically have smaller teams. Therefore they are likely to benefit from increased support focused on scaling up their offering. While there are a range of services available in Ireland, **direct engagement with SME firms may increase awareness of services and uptake.** There is also wider potential to develop support informed by Enterprise Ireland's European Cybersecurity Market opportunity mapping exercise[3] which focuses on promoting engagement in European markets.

08 Firms also report difficulty engaging with larger firms. Building on the above point, **smaller firms could also be paired with larger firms to drive collaboration and increase market offering.** There is potential to leverage existing connections with organisations such as the IDA, InterTrade Ireland, and Cyber Ireland to promote business networking and collaboration between domestic SMEs and larger firms.

[3] Enterprise Ireland (2019). 'The European Cybersecurity Market Mapping The Opportunities And Route To Market For Irish SMES'. Available at: https://globalambition.ie/wp-content/uploads/2019/11/The-European-Cybersecurity-Opportunities-for-Irish-SMEs_Key-Takeouts.pdf

01
Introduction

Cyber Ireland, the national cyber security cluster organisation, was founded in 2019 to bring together industry, academia, and government to represent the needs of the cyber security ecosystem in Ireland and support its growth. The cluster is hosted at Munster Technological University and is supported by government through Enterprise Ireland, IDA Ireland and the National Cyber Security Centre. Cyber Ireland's activities support collaboration, skills development, Research, Development & Innovation, and new business development in the cyber security sector. Cyber Ireland is the industry partner to the HEA funded initiative Cyber Skills, a government-backed initiative designed to address skill shortages in the cyber security sector.

There are no comprehensive data or reports on the cyber security sector in Ireland. The cyber security sector does not have a formal NACE Code, and therefore, the industrial data published by the Central Statistics Office (CSO) does not break down sectors to identify cyber security companies. Additionally, there are many cyber security teams and employees across different industry sectors that also contribute to the cyber security cluster.

A baseline is required to understand the size, make-up and economic impact of the cyber security sector in Ireland. This is strategic as other countries have conducted regular reports of their cyber security sectors, setting ambitious targets for their growth. Examples include the UK Cyber Security Sectoral Analysis 2021 and Northern Ireland Cyber Security Sector Snapshot 2021.

1.1 RESEARCH OBJECTIVES

Cyber Ireland has commissioned Perspective Economics to conduct an economic analysis of Ireland's cyber security sector. The objectives of this study are:

01 To understand the current size and make-up of the cyber security sector in Ireland and to track its future development.

02 To assess the economic contribution of the cyber security sector in Ireland and its importance to the economy.

03 To assess the international cyber security market opportunities for Irish start-ups and SMEs, alongside foreign direct investment opportunities for Ireland.

04 Produce recommendations to support the development and economic growth of Ireland's cyber security sector, from evidence-based assessments.

As part of this research, almost five hundred (489) firms offering cyber security products or services, or firms that have built internal cyber security teams in Ireland have been identified. The report explores the products and services offered by these firms, as well as their location, cyber security related revenue, employment and Gross Value Added generated by the sector in Ireland.

This is the first study that seeks to map Ireland's cyber security sector in detail. The methodology is aligned to similar studies conducted in the United Kingdom[4], and Northern Ireland[5]. We, therefore, welcome feedback and comments on this research, as Cyber Ireland seeks to track the growth and performance of the sector in the years ahead.

1.2 TEAM AND ACKNOWLEDGEMENTS

The project team included Sam Donaldson (Study Lead) and Conor Tinnelly (Analyst) from Perspective Economics. We would particularly like to acknowledge and thank Dr Eoin Byrne, Cyber Ireland and Professor Donna O'Shea, Chair of Cyber Security at MTU for their contribution and insights, in addition to the engagement from industry and government partners throughout the study period.

Further, we would like to thank the businesses that contributed to the online sector survey. The response leading up to the publication of this study is indicative of the ambition and collaboration within the cyber security sector in Ireland.

[4] Department for Digital, Culture, Media and Sport (2021). 'UK Cyber Security Sectoral Analysis 2021'. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/962413/UK_Cyber_Security_Sectoral_Analysis__2021_.pdf]

[5] Centre for Secure Information Technologies (2021). 'Northern Ireland Cyber Security Snapshot 2021'. Available at: https://www.qub.ac.uk/ecit/CSIT/About/Filetoupload,1077295,en.pdf

1.3 SCOPE

This research seeks to identify firms that are active in Ireland and offering 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 in Ireland can be fully mapped.

The project's scope is presented below, and a full taxonomy of products and services in scope is outlined in Section 2 of this report.

RESEARCH SCOPE

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

✓ Demonstrate an active provision of commercial activity related to cyber security (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 selling of these solutions to other customers)

✓ Have identifiable revenue or employment within Ireland

✓ Provide recruitment support specifically for the sector; or

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

This analysis differentiates 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 revenue 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.

Section 2 sets out the type of companies in scope in further detail, alongside the cyber security products and services that are typically offered.

1.4 METHODOLOGY

We set out a simple overview of our methodology below and a full version is provided in the appendix of this report.

STAGE	DESCRIPTION
Desk Research	The research team conducted a rapid assessment of literature relating to Ireland's cyber security sector. This was used to inform our definition of the sector, and to assist in the identification of relevant cyber security businesses in Ireland.
Definition and Market Scoping	The research team, in collaboration with Cyber Ireland, developed a sector taxonomy that maps known products and services offered within Ireland's cyber security sector. This taxonomy was also informed by previous international studies and aligns with the NI Cyber Security Snapshot to allow for all-island mapping in the future. It should be noted that the cyber security sector does not have a formal NACE Code (this is the European classification system that groups organisations according to their business activities), and therefore keyword analysis has been used to identify firms. The team subsequently used a range of market intelligence, web analytics (using over six hundred keywords), and business sources to map hundreds of potentially relevant businesses. Each business was subject to scoring and manual review, before being shortlisted as a relevant cyber security firm (where it had identifiable revenue or employment linked to cyber security activity).
Market Analysis	Following the shortlisting of relevant firms providing cyber security products or services, the team extracted relevant company trading information, such as the registered address, company number, and revenue and employment (where available). The 489 cyber security providers identified in Ireland were matched to company information using Bureau van Dijk FAME (for financial metrics) and Companies Registration Office (CRO) statistics, and through direct consultation with industry stakeholders.
Business Survey	An online business survey was also sent to these firms (where contact details were available) via Cyber Ireland and partners with the permission of included firms in August 2021. The business survey asked about the trading nature of identified firms (e.g., finance, cyber employment, and views on the perceived strengths, barriers, and opportunities within the sector).

Given the nature of company accounts of registered firms, where revenue data is unavailable or is an outlier, estimates have been used.

These estimates have been developed with bottom-up modelling and included engagement with industry. These are also benchmarked against other sectors and international comparisons.

Source: Perspective Economics

02
Defining and Measuring the Cyber Security Sector

2.1 INTRODUCTION

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. As this is the first study conducted within Ireland, we use a broad definition to help capture as much of the economic activity relating to cyber security as possible.

To identify and determine the inclusion of firms, the research team explored:

- The **response utilised by firms to address security issues online**, e.g., end-to-end encryption, threat intelligence, and identity authentication;
- The **type and extent of risk** involved, e.g., risks to a single business, or risk to national infrastructure;
- The **type of security risks addressed** by solutions within the sector such as e.g., network vulnerability, security of connected devices; and
- The **technology and approaches used to address security risks**, such as machine learning and AI capabilities to detect threats.

DEFINITION OF CYBER SECURITY:

We utilise the definition of cyber security as set out within the 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)

2.2 DEFINING CYBER SECURITY: A TAXONOMY APPROACH

The taxonomy developed for this study has been designed using a top-down approach, to reflect the core offering of services in Ireland. It has been used previously to map the cyber security sector in Northern Ireland and has been refined for this study.

Six key areas of products and services offered within Ireland's cyber security ecosystem have been identified, 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 Irish 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.

This taxonomy is an interpretation of the products and services in scope and provided by the cyber security sector. Table 2.1 provides a summary of the product and service categories typically offered by Ireland's cyber security sector.

TABLE 2.1 CYBER SECTOR TAXONOMY DEFINITIONS

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 cyber security. For example, where a business procures an MSSP to undertake cyber security monitoring, network security, patching and remote device management, penetration testing, and broader security and IT advice.
Risk, compliance, and fraud	Firms where the focus of cyber security techniques is upon identifying risk (such as harmful actors or anomalies), ensuring compliance with cyber security standards (e.g., ISO27001 and GDPR) concerning data management, and identifying and mitigating fraud within transactions. There is a strong overlap between this field with FinTech and payment processing.
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 direct change through the monitoring and/or control of devices, processes, and events.
Threat intelligence, monitoring, detection, and analysis	Information security professional 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 offering systems designed to support the verification of users accessing systems.
Other firms	Firms that support employment in the sector 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).

Source: Perspective Economics

03 Profile of Ireland’s Cyber Security Sector

3.1 INTRODUCTION

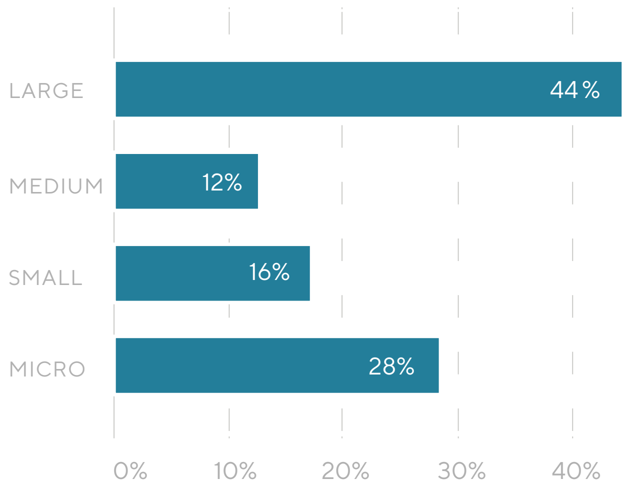
This section outlines key features of the 489 identified firms that are engaged in the provision of cyber security products or services in Ireland, outlining key features within the sector by:

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

3.2 NUMBER OF FIRMS

For the 489 firms engaged in cyber security in Ireland, Figure 3.1 sets out the breakdown by size (using EU SME definitions[6]).

FIGURE 3.1 NUMBER OF FIRMS BY SIZE



Ireland’s cyber security sector consists of a high proportion (44%) of large companies. This is significant when compared to the wider Irish economy where SMEs typically account for over 99% of the business population[7].

Indeed, the percentage of ‘large’ firms in Ireland’s cyber security sector is much higher than comparable studies. For example, the UK Cyber Security Sectoral Analysis 2021 estimates that approximately 10% of UK cyber security firms are large, compared to 44% in Ireland.

For the 56% of cyber security businesses that are SMEs, these are split between medium (12%), small (16%), and micro-enterprises (28%).

DEDICATED & DIVERSIFIED PROVIDERS OF CYBER SECURITY PRODUCTS & SERVICES

Within this research, firms were categorised by whether they are:

DEDICATED (PURE-PLAY)

This refers to where all, or most (75%+), of a firm’s revenue 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, or defence - or that have internal cyber security operations or product development teams.

The rationale underpinning the need to provide this distinction is attributable to seeking to understand how firms either set up to solely provide cyber security services or to provide cyber security as one product or service among others, which could impact the firm’s size, scale, growth, and market activity.

[6] 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

[7] Central Statistics Office (2021). ‘Business Demography 2019 - CSO - Central Statistics Office’. Available at: https://www.cso.ie/en/releasesandpublications/er/bd/businessdemography2019/

FIGURE 3.2 NUMBER OF FIRMS BY DEDICATED / DIVERSIFIED STATUS

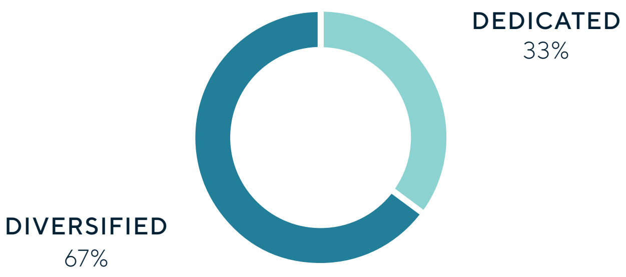


Figure 3.2 shows that 160 (33%) of total firms are dedicated (pure-play) and fully attribute their employment and revenue to activity within the cyber security sector. The other 329 (67%) firms are diversified and offer cyber security products or services as part of a wider offering or have internal cyber security operations or product development teams.

FIGURE 3.3 NUMBER OF FIRMS BY DEDICATED / DIVERSIFIED STATUS AND BY SIZE

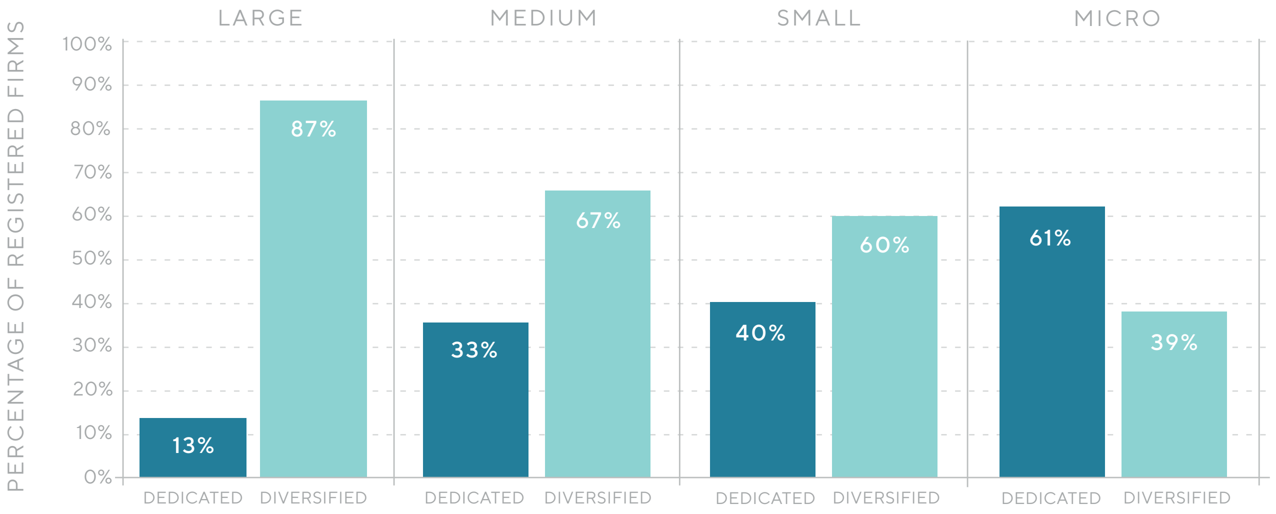


Figure 3.3 provides further detail on the company size by dedicated and diversified status. It is found that pure-play cyber security firms are typically smaller in scope (as reflected across comparable international studies), whereas diversified companies are typically larger.

This is often due to large non-cyber security companies needing internal cyber security expertise or to protect the business or to support product development.

Source: Perspective Economics (n = 489)

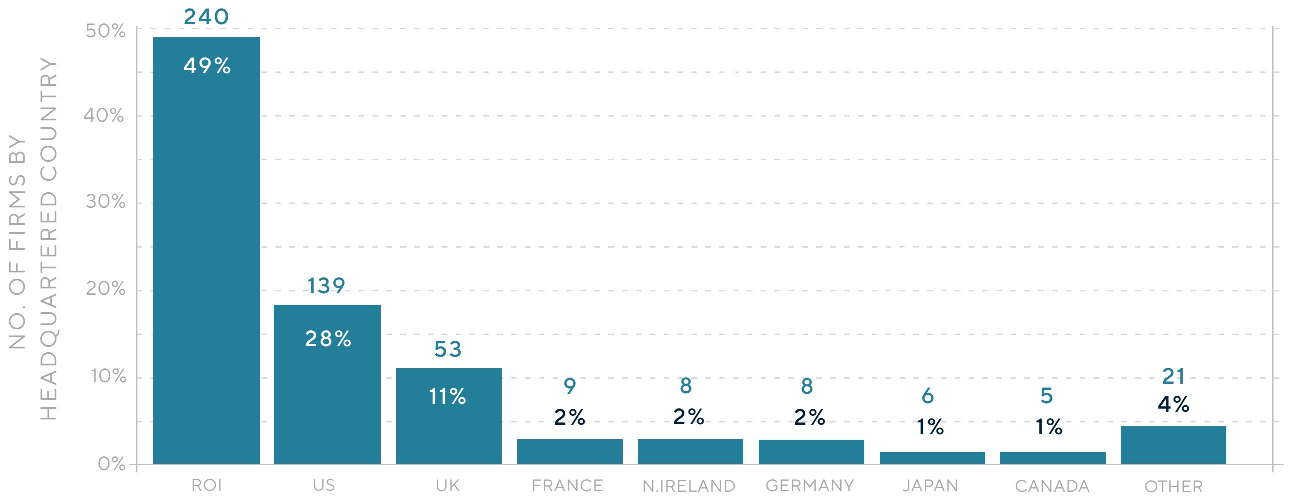
NUMBER OF FIRMS BY HEADQUARTERED LOCATION

Ireland has a 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 EU market. 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.

In total, 240 domestic, or Irish-headquartered, firms were identified, which is **almost half** (49%) **of all firms engaging in the cyber security sector in Ireland.**

As shown in Figure 3.4, firms headquartered in the United States make up the second-largest proportion (139 firms, 28%) operating in Ireland, followed by the United Kingdom[8] (53 firms, 11%), and other European countries (30 firms, 6%).

FIGURE 3.4 NUMBER OF FIRMS BY HEADQUARTERED COUNTRY



Source: Perspective Economics (n = 489)

[8] Including Northern Ireland, which is also mapped separately.

TABLE 3.1 NUMBER OF FIRMS BY LOCATION AND BY SIZE

Table 3.1 presents the size of firms by foreign-owned and domestic status. This highlights the size difference between foreign-owned and domestic companies and indicates the relative importance of large international investment into Ireland, as well as the scale of domestic Irish SMEs working in the cyber security sector.

	FOREIGN-OWNED FIRMS	DOMESTIC FIRMS	ALL FIRMS
Large (250 FTEs or more)	194 (89%)[9]	23 (11%)	217
Medium (50 - 249 FTEs)	17 (29%)	41 (71%)	58
Small (10 – 49 FTEs)	23 (30%)	54 (70%)	77
Micro (1 - 9 FTEs)	15 (11%)	122 (89%)	137
Total	**249 (51%)**	**240 (49%)**	**489**

Source: Perspective Economics (n = 489)

[9] Percentage calculated: Foreign Owned or Domestic / Number of Firms in Size Bracket.

3.3 PRODUCTS AND SERVICES (TAXONOMY)

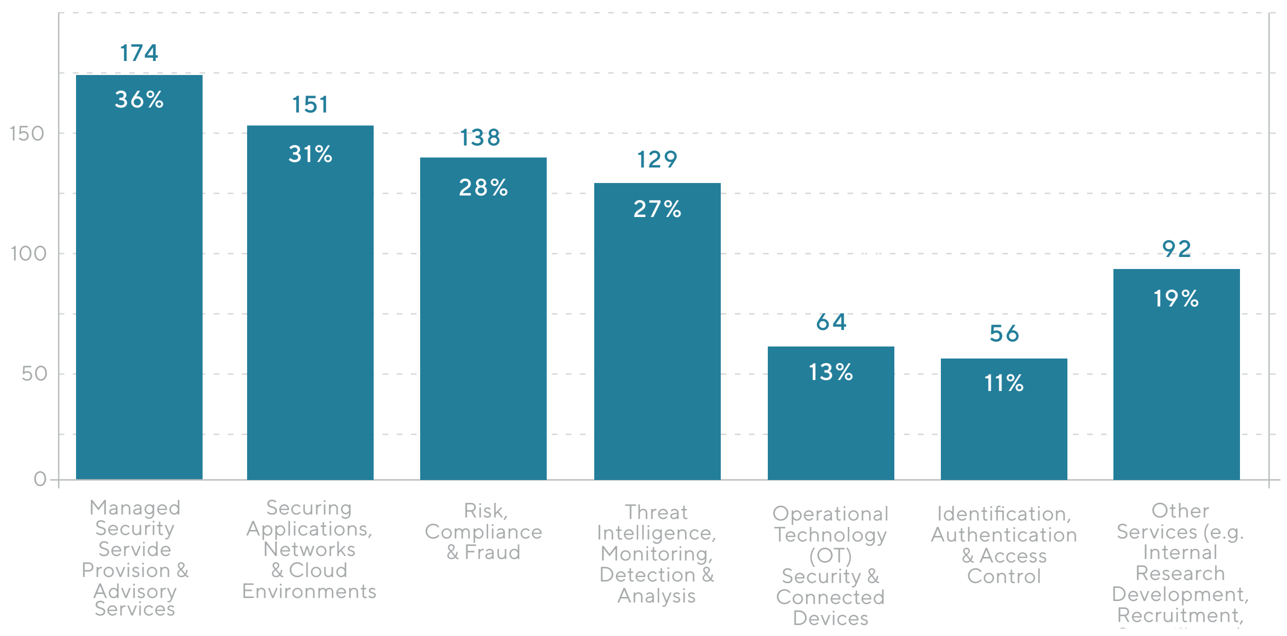
As set out in Section 2, six key areas of products and services offered within Ireland's cyber security ecosystem have been identified, in addition to an 'other' classification to include internal cyber security operations, product development, R&D, or recruitment.

An analysis of firm activity was conducted using this taxonomy [10], with firms grouped based on available company descriptions and relevant web data.

Classification of activity across taxonomy groups is presented in Figure 3.5, suggesting that c. one-third of Ireland's cyber security firms provide managed security or advisory services, or secure applications, networks, and cloud environments.

A further 28% offer risk, compliance, or fraud services. This is an area that is likely to grow with increased integration of technology, in addition to regulation, and the need for compliance with international standards with respect to payment, identity, and data protection.

FIGURE 3.5 NUMBER OF FIRMS PER TAXONOMY GROUP



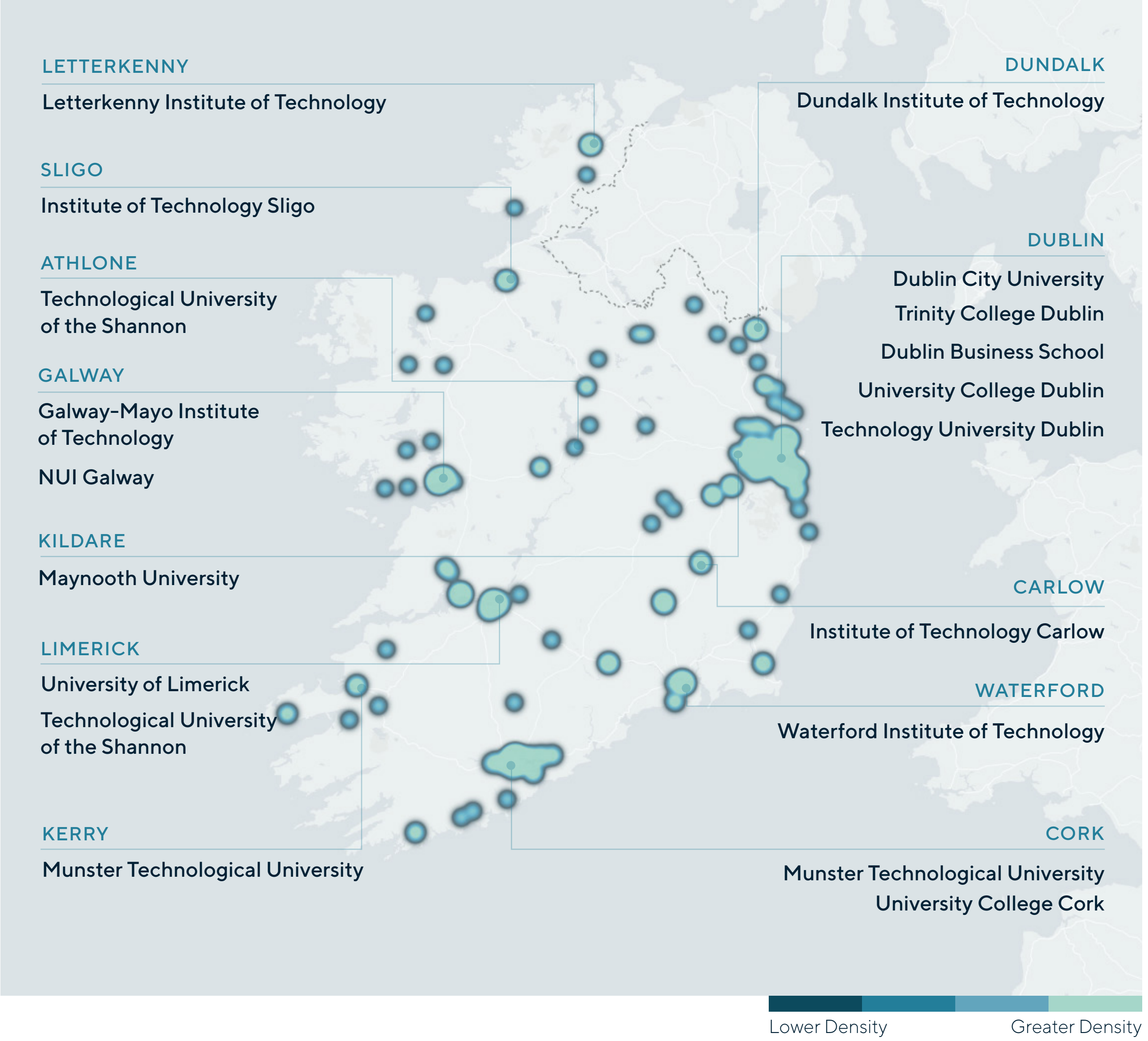
Source: Perspective Economics (n = 489)

[10] Note that firms can appear in multiple taxonomy groups, and employment estimates are provided at firm-level, as service-level data was unavailable.

3.4 LOCATION OF CYBER SECURITY FIRMS

This section explores the location of cyber security businesses in Ireland. Across the 489 businesses identified, we have identified 734 offices in Ireland, which are mapped in Figure 3.6 below. This also includes a number of research assets as identified by Cyber Ireland.

FIGURE 3.6: HEAT MAP OF OFFICE LOCATIONS AND ACADEMIC INSTITUTES


LETTERKENNY
Letterkenny Institute of Technology
SLIGO
Institute of Technology Sligo
ATHLONE
Technological University of the Shannon
GALWAY
Galway-Mayo Institute of Technology
NUI Galway
KILDARE
Maynooth University
LIMERICK
University of Limerick
Technological University of the Shannon
KERRY
Munster Technological University
DUNDALK
Dundalk Institute of Technology
DUBLIN
Dublin City University
Trinity College Dublin
Dublin Business School
University College Dublin
Technology University Dublin
CARLOW
Institute of Technology Carlow
WATERFORD
Waterford Institute of Technology
CORK
Munster Technological University
University College Cork
Lower Density
Greater Density

Source: Cyber Ireland, Perspective Economics

While some of Ireland's largest cities are home to the highest count of cyber security offices, this is somewhat reflective of their populations. As such, we have also identified the number of cyber security offices per 10,000 capita, to further identify the relative strengths and importance of cyber security to each location.

Please note this is only on an office, rather than an employment, basis (which is not modelled at a city level), but still demonstrates the proportional strength of cyber security in areas such as Cork, Galway, and Limerick relative to their population.

For example, Cork has the highest concentration of cyber security multinationals and is home to the top five cyber security employers in Ireland.

TABLE 3.2 NUMBER OF OFFICES BY COUNTY

REGION	NO. OF CYBER SECURITY OFFICES	NO. OF OFFICES (DEDICATED FIRMS)	NO. OF OFFICES (DIVERSIFIED FIRMS)	BUSINESSES PER 10K POPULATION
Cork	129	37	92	7
Galway	39	8	31	5
Dublin	397	100	297	4
Limerick	30	3	27	3
Belfast	86	31	55	3
Ireland	**734**	**191**	**543**	**1.5**

Source: Perspective Economics

With reference to the four larger regions, with respect to count of cyber security offices:

- **The Dublin region** has a **higher number of firms than any other county** in Ireland and is home to many of the country's largest tech MNCs and financial services companies with growing cyber security teams, such as Microsoft, Amazon and Zurich. There is a strong base of indigenous SMEs, in particular MSSPs such as Integrity 360 and Ward Solutions. These companies hire talent from the universities in the region including Technological University Dublin, University College Dublin, and Dublin Business School who have dedicated cyber security courses. It is home to research assets such as the CeADAR Centre of Applied AI and the Centre for Cybersecurity and Cybercrime Investigation in UCD and the newly established Collaboratory at TUD. Ireland's National Cyber Security Centre is also based in Dublin. Across each of the taxonomy groups, it is home to c.50% of all offices.

- **The Cork region** hosts 129 cyber security offices and has more firms per capita than any other county in Ireland. The region has the highest concentration of cyber security multinationals and is home to the top five cyber security employers in Ireland. It is home to US firm McAfee's Centre of Excellence and Trend Micro's EMEA HQ. The national cyber security cluster, Cyber Ireland, is based in Cork, hosted at Munster Technological University. MTU is a major provider of cyber security talent to the region and leads the Cyber Skills initiative. University College Cork is another academic institute in the region, which has a Cyber Security Research Group. The region hosts c.24% of offices linked with firms that provide operational technology services, and 20% of offices linked with firms that secure applications, networks, cloud environments.

- **The Galway region** has the **second-highest number of firms per capita** and hosts key educational assets, such as the Galway-Mayo Institute of Technology and the National University of Ireland Galway. The region is **home to Hewlett-Packard's Global Cyber Defence Centre.**

- **The Limerick region** hosts 30 offices and education and research assets such as the University of Limerick and Lero, Irish Software Research Centre. While information is limited to firm-level data only, our research suggests that c.11% of all operational technology offices in Ireland are situated between the Clare/Limerick regions.

- Other regions of note include Clare, Kildare, Waterford, Louth, and Donegal (10+ offices identified).

To examine this on an all-island basis, a similar analysis is available for firms in **Northern Ireland Cyber Security Sector Snapshot 2021.**

04
Economic Contribution of Ireland's Cyber Security Sector

4.1 INTRODUCTION

This section provides an overview of the economic contribution that the cyber security sector generates for the wider Irish economy. This includes an estimate of:

- Total cyber security related revenue in Ireland.
- Cyber security related employment in Ireland.
- Gross Value Added (a measure of productivity) related to the cyber security sector in Ireland.

We also undertake benchmarking, which explores the size and scale of the Republic of Ireland's cyber security sector against five other regions and countries, including the UK, Northern Ireland, the United States, Estonia, and Israel.

These figures are estimates by Perspective Economics for the most recent year (2021) unless otherwise stated.

4.2 ESTIMATED CYBER SECURITY REVENUE

We estimate that in the most recent financial year, **annual cyber security-related revenue in Ireland reached approximately €2.1bn.**

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 (multiplied by the estimate of the proportion of the firm's activity related to cyber security).
- Reported cyber security revenue estimated (for the most recent financial year) through the business survey undertaken in 2021.

The nature of company data available means this is an estimate only and should be reviewed annually. We also note that revenue on a per capita basis compares strongly to the UK and Northern Ireland. This is explored further within Section 4.6 Benchmarking.

4.3 ESTIMATED CYBER SECURITY EMPLOYMENT

The research team reviewed company accounts and web data for the 489 businesses identified. This included web analysis with identification of 'cyber security-related roles'.

We estimate that there are **7,351 cyber security professionals** (full-time equivalents) working across Ireland's cyber security sector. We have examined the composition of these cyber security-related teams (i.e., the number of cyber security professionals working within each of the 489 teams). We find that:

- Typically, cyber security teams are small, with nearly two-thirds (65%) of firms employing between one to nine cyber security professionals.
- A further 27% employ between 10 – 49 cyber security professionals and only 8% of firms have teams of 50+ cyber security staff.

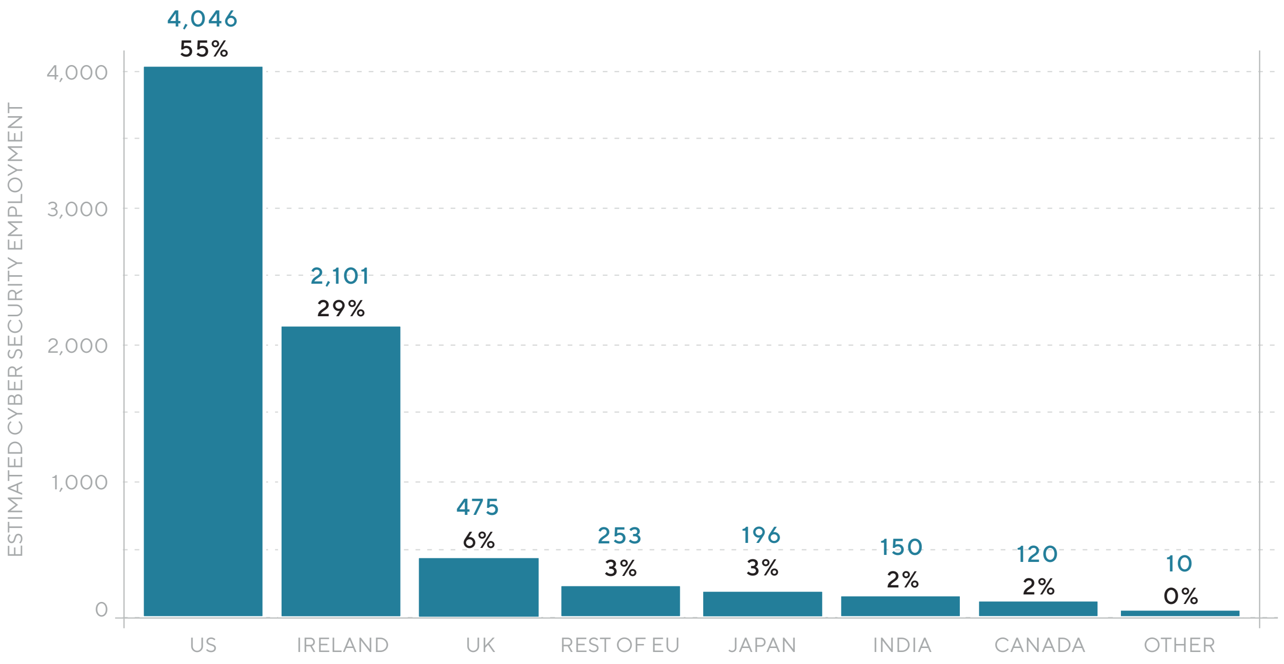
The following charts explore the extent of cyber security employment by the headquartered location, dedicated and diversified status, and by size. A granular breakdown of employment across Ireland's sub-regions is not provided due to data limitations.

CYBER SECURITY EMPLOYMENT (BY HEADQUARTERED LOCATION):

Figure 4.1 sets out that **over seven in ten roles in the cyber security sector in Ireland are supported by foreign-owned firms**, reflecting the importance of FDI to Ireland's economy. This is particularly pronounced among US-owned firms, which support approximately 55% of roles in the sector (over 4,000 FTEs).

However, over 2,100 roles are supported by Irish owned firms, which reflects a strong base to support domestic firm growth and expansion of their cyber security teams.

FIGURE 4.1 NUMBER OF CYBER SECURITY EMPLOYEES BY COUNTRY OF ORIGIN

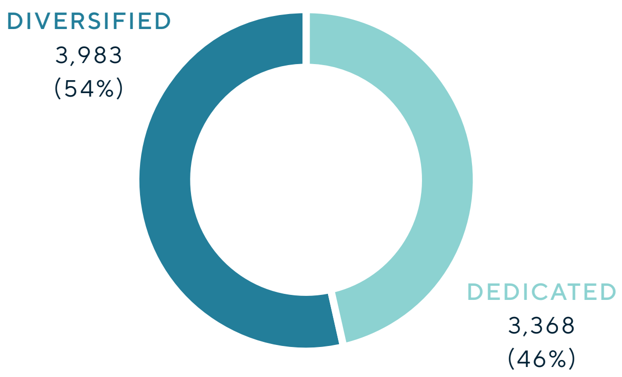


Source: Perspective Economics

CYBER SECURITY EMPLOYMENT (BY DEDICATED AND DIVERSIFIED STATUS):

Figure 4.2 highlights that employment within Ireland's cyber security sector is relatively split between dedicated (pure-play) and diversified firms. This highlights the importance of growing the cyber security ecosystem through support for both pure-play firms and also cyber security teams within broader firms.

FIGURE 4.2 NUMBER OF CYBER SECURITY EMPLOYEES BY DEDICATED & DIVERSIFIED STATUS



Source: Perspective Economics

CYBER SECURITY EMPLOYMENT (BY SIZE):

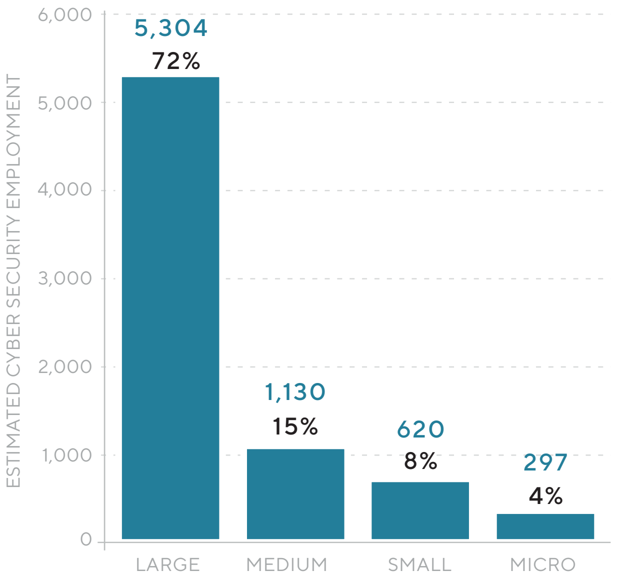
Figure 4.3 highlights that almost three in four cyber security roles within Ireland are based within larger companies (i.e., the company has 250+ staff). Much of this can be attributed to the role of foreign direct investment as set out previously. This may provide some context to skills and employment interventions within the sector.

For example, larger companies may influence the broader demand for cyber security professionals and also have the capacity to draw upon skills interventions such as retraining.

However, SMEs may also require support to attract talent to their teams, or to nurture internal talent. Policy-makers may seek to explore how to further encourage entrepreneurialism and opportunities for individuals to establish start-ups and scale-ups within the ecosystem.

Some of the challenges and opportunities with respect to skills and employment are explored further in Section 7.

FIGURE 4.3 NUMBER OF CYBER SECURITY EMPLOYEES BY COMPANY SIZE



Source: Perspective Economics

4.4 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.

This study is a baseline and is the first estimate of the GVA of the cyber security sector in Ireland. Company accounts within Ireland can often capture global or international economic activity, and we have therefore adjusted the estimates to account for this.

In other words, the estimated Gross Value Added reflects the economic contribution of the 489 cyber security firms, and their c. 7,351 staff employed in Ireland and relates to cyber security activity only.

In terms of the current GVA, we estimate that Ireland's cyber security sector generated approximately €1.1bn in 2021.

The table below sets out average salaries [11] advertised for cyber security roles in Ireland, estimated GVA per employee, and the total estimate for sector-wide GVA in Ireland.

TABLE 4.1 IRELAND CYBER SECURITY SECTOR GVA ESTIMATE (2021) (AND PER CAPITA)

TYPE OF FIRM	AVERAGE SALARY	ESTIMATED GVA PER EMPLOYEE	ESTIMATED NUMBER OF EMPLOYEES	TOTAL GVA
Dedicated	€75k	€136k	3,372	€459m
Diversified	€77k	€155k	3,983	€617m
Total estimated GVA:				**€1.1bn**

Source: Perspective Economics, Cyber Ireland

[11] Average advertised salaries estimated using Morgan McKinley cyber security role salary estimates: https://www.morganmckinley.com/ie/ireland-salary-guide-calculator

4.5 SECTOR SUMMARY

A summary of key firmographic statistics relating to the sector are presented below:

TABLE 4.2 SUMMARY TABLE

	NUMBER OF FIRMS		EMPLOYMENT	
Total:	489		7,351	
Dedication of Service	N	%	N	%
Dedicated Cyber Security Services	160	33%	3,368	46%
Diversified Services That Include a Cyber Security Offering	329	67%	3,983	54%
Country of Origin				
Domestic Firms	240	49%	2,101	29%
Foreign-Owned Firms	249	51%	5,250	71%
Size				
Large	217	44%	5,304	72%
Medium	58	12%	1,130	15%
Small	77	16%	620	8%
Micro	137	28%	297	4%

TABLE 4.3 TAXONOMY SUMMARY

SERVICES OFFERED (TAXONOMY GROUPS)	NO. OF FIRMS	% OF FIRMS
Managed Security Service Provision and Advisory Services	174	36%
Securing Applications, Networks and Cloud Environments	151	31%
Risk, Compliance and Fraud	138	28%
Threat Intelligence, Monitoring, Detection and Analysis	129	26%
Operation Technology Security and Connected Devices	64	13%
Identification, Authentication and Access Control	56	11%
Other Firms	92	19%

TABLE 4.4 GVA AND REVENUE ESTIMATE (2021)

TYPE OF FIRM	AVERAGE SALARY	ESTIMATED GVA PER EMPLOYEE	ESTIMATED NUMBER OF EMPLOYEES	TOTAL GVA
Dedicated	€75k	€136k	3,372	€459m
Diversified	€77k	€155k	3,983	€617m
Total estimate GVA:				**€1.1bn**
Total revenue estimate:				**€2.1bn**

Source: Perspective Economics, Cyber Ireland

4.6 BENCHMARKING

This section explores the cyber security sector in Ireland against other notable cyber security regions and provides insight and comparison (where possible) between areas including the UK (incl. Northern Ireland), the United States, Estonia, and Israel.

TABLE 4.5 CYBER SECURITY SECTORAL COMPARISON (WHERE DATA IS AVAILABLE / COMPARABLE)

REGION	NO. OF FIRMS (PER 100,000 NATIONAL POPULATION)	NUMBER OF EMPLOYEES	SECTOR REVENUE	SECTOR GVA	AVERAGE SALARY
Ireland	489 (9.7)[12]	7,351	€2.1bn	€1.1bn	€75k
Northern Ireland [13]	104 (6)[14]	2,299	Not Estimated	£161m (€190m)	£48k (€55k)
UK [15]	1,838 (2.7)[16]	52,727	£10.1bn (€11.9bn)	£5.3bn (€6.3bn)	£60k (€70k)[17]

Source: Perspective Economics, Cyber Ireland

[12] Worldometer (2022). 'Ireland Population (2022) – Worldometer'. Available at: https://www.worldometers.info/world-population/ireland-population/

[13] Centre for Secure Information Technologies (2021). 'Northern Ireland Cyber Security Snapshot 2021'. Available at: https://www.qub.ac.uk/ecit/CSIT/About/Filetoupload,1077295,en.pdf

[14] Northern Ireland Research and Statistics Agency (2019). 'NISRA Statistical Bulletin'. Available at: https://www.nisra.gov.uk/sites/nisra.gov.uk/files/publications/MYE20-Bulletin.pdf

[15] Department for Digital, Culture, Media and Sport (2022). 'UK Cyber Security Sectoral Analysis 2022:. Available at: https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2022

[16] Worldometer (2022). 'U.K. Population (2022) – Worldometer'. Available at: https://www.worldometers.info/world-population/uk-population/#:~:text=The%20current%20population%20of%20the,year%20according%20to%20UN%20data

[17] Department for Digital, Culture, Media and Sport (2022). 'UK Cyber Security Sectoral Analysis 2022:. Available at: https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2022

TABLE 4.6 BENCHMARK COMPARISON

COMPARATOR REGION	
Northern Ireland 	**Key Cluster Regions:** Belfast, Derry **Key Comparisons:** The Republic of Ireland is home to nearly 5 times as many cyber security firms as Northern Ireland and has more firms per capita. GVA per employee is also higher in Ireland at €150k, compared to NI's €82k, and the average salary is c.€75k in comparison to NI's c. €55k. The sector in both regions is shaped heavily by foreign direct investment as 70% of employment in Ireland is FDI supported, compared to 79% in Northern Ireland. **Key Strength:** Northern Ireland is the home of the well-respected UK wide innovation and knowledge centre for cyber security CSIT, affiliated with Queens University Belfast and the UK National Cyber Security Centre. Note the activity at CSIT – basic research, applied research, post-grad, PhDs, supporting start-ups & innovation. Northern Ireland has set a goal to become one of the leading cyber security economies globally, recognising and building on NI's "blend of world-class talent, leading forensic science expertise and tech re-search excellence", to achieve 5,000 cyber security job roles by 2030.
United Kingdom (including Northern Ireland) 	**Key Cluster Regions:** Cheltenham, Bristol, London, Manchester **Key Comparisons:** There are over three times as many firms providing cyber security products and services in the UK than in the Republic of Ireland; however, Ireland performs strongly on a per capita basis. On average, advertised cyber security salaries in Ireland appear slightly higher (c.€75k), compared to the UK average of £60k/€70k. In Ireland, GVA per employee also appears higher at €150k, compared to £100k/€120k in the UK. **Key Strength:** The UK's National Cyber Security Strategy outlines how the government aims to develop a 'programme of initiatives to give start-ups the support they need to get their first customers and attract further investment', comparative to Ireland, investing c.10 times more on cyber security per capita.[18] The UK is well placed to support cyber security start-ups through a range of government, industry and academic support services. These include initiatives to support early-stage ideas and start-ups (e.g., HutZero, Cyber 101, CyberASAP). The UK's Department for Digital, Culture, Media and Sports also support a range of initiatives tailored towards companies with high-growth potential, such as the NCSC Cyber Accelerator, the London Office for Rapid Cybersecurity Advancement (LORCA). Ireland should support the development of its domestic R&D and business support services, allocating greater public spend to the development of cyber security capabilities.
United States 	**Key Cluster Regions:** Virginia, Texas, Nevada **Key Comparisons:** There are an estimated 3,500 cyber security firms in the US, compared to the 491 in Ireland. **Key Strength:** The US market is of key significance to the Irish economy, and more than half of all employment within Ireland's sector is supported by firms from the United States. This supports best practice adoption and skill transfer from the US to firms based in Ireland. The US is considered world-leading in cyber security due to several factors such as its dominant military capabilities and domestic industry, alongside the government's evolved management of hacking risks.[19] The most important factor contributing to the country's overall capabilities is the breadth of firms focused on information and communication technology. Ireland should continue to engage and promote US-driven FDI. This will support best practice adoption in local markets, and enhance national capabilities. As outlined above FDI firms also support large scale employment.

[18] Irish Times (2021) False economies on cybersecurity. Available at: https://www.irishtimes.com/business/economy/false-economies-on-cybersecurity-1.4580298

[19] International Institute for Strategic Studies (2021) Cyber Capabilities and National Power: A Net Assessment. Available at: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power

COMPARATOR REGION

Estonia

Number of known firms: 55 domestic SMEs [20]

Key Strengths: The permeation of digital culture across Estonian society has allowed its citizens to interact with the state almost exclusively in an online environment through a personal digital identification card, and demonstrates how a state can proactively engage with the private sector to increase resilience and prevent cybercrime.[21] The cyberattack against the Estonian state in 2007 resulted in a coordinated reassessment of the nation's approach to cyber security, which saw greater cooperation between volunteers, government, and the private sector to ensure wider society was digitally literate and the online environment secure.

Ireland should learn from the Estonian approach to national cyber security, promoting cyber security due diligence across all aspects of society. This will reduce the threat of future attacks on the state and promote better integration of technology across society.

Israel

Number of firms: 424 [22] (5 per 100,000 national population)

Key comparisons: Ireland is similar to Israel, in terms of GDP and national population, while also having few natural resources.

Ireland is similar to Israel, in terms of GDP and national population, while also having few natural resources. Key strengths: Israel has a strong domestic cyber security market and is a leader in cyber security start-ups, innovation & investment.

Key Strengths: Number of firms: 424 (5 per 100,000 national population)

Israel has a strong domestic cyber security market and is a leader in cyber security start-ups, innovation & investment.

The Israeli government supports the cyber security sector in a number of ways. The country has a strong technological sector that is supported well by the government and their Advanced Technology Park (one of six centres nationally) facilitates both theoretical and practical development of the sector in line with public and private interests, attracting international firms like Oracle, Dell, EMC, IBM and Deutsch Telekom to conduct R & D work in Israel.

COMPARATOR REGION

In 2016, Israel successfully attracted 20% of global FDI related to cyber security and is home to the largest concentration of cyber security start-ups and investment, and has exported c.$6.5bn dollars' worth of cyber security technology, at a time when Ireland was estimated as exporting €200m[23].

Key factors attributed to supporting Israel's success include government support in coordinating the sector to drive business growth, use of the military as an incubator space, supporting multi-disciplinary collaboration, and long-term investment in education to support a sustainable pipeline of talent.

Ireland should develop a long-term education pathway to ensure there is a pipeline of new talent entering the sector.

[20] Invest in Estonia (2021). 'Estonia – the rise of a cybersecurity giant — Invest in Estonia'. Available at: https://investinestonia.com/estonia-the-rise-of-a-cybersecurity-giant/

[21] The Irish Times (2021). 'Ireland must learn lessons from Estonia on cybersecurity'. Available at: https://www.irishtimes.com/business/technology/ireland-must-learn-lessons-from-estonia-on-cybersecurity-1.4578039

[22] Statista (2021). 'Israel cybersecurity companies 2011-2020'. Available at: https://www.statista.com/statistics/1003442/israel-cyber-security-companies/#:~:text=This%20statistic%20shows%20the%20number,of%20450%20companies%20in%202018

[23] Larkin, P. (2018). 'Securing Ireland's digital future A new and expanded national cyber security strategy'.

05
Labour Market Overview

5.1 INTRODUCTION

This section explores Ireland's cyber security labour market in relation to the size of the workforce, and demand for talent. It also explores the current demand for cyber security skills both in Ireland and globally, and the potential opportunities that this can generate.

5.2 DEMAND FOR CYBER SECURITY

As set out above, **we estimate there are approximately 7,351 employees in the cyber security sector in Ireland.** This is closely aligned to the National Cyber Security Strategy, which estimated approximately 6,500 employees in 2019/20.

Whilst this study is a baseline, this suggests that the cyber security sector is growing (with respect to the workforce) in Ireland by a similar magnitude to other countries. We would estimate this growth in the region of c. 10% per annum. This is reserved in comparison to growth ambitions among surveyed firms, with 83% of firms surveyed (n=76) predicting growth, **half of all firms expecting to grow at a rate of 25% or higher over the next 12 months.**

There are a wide range of studies exploring the shortfall in cyber security talent, against a backdrop of increased demand. Indeed, one of the most significant factors leading to data breaches across digital structures globally is the lack of training of non-technical employees and the lack of highly skilled cybersecurity professionals.[24]

The **ISC² Cybersecurity Workforce Study** (2021)[25] estimates that Ireland has an annual shortfall of approximately 10,000 people in cyber security roles (across the broader economy). This is also explored in the Cyber Ireland Cyber Security Skills Report 2021.[26]

JOB VACANCIES ANALYSIS

One proxy for understanding employer demand for cyber security talent is to undertake job vacancy analysis i.e., identify and measure the number of employer job posts for relevant roles in Ireland.

In December 2021, the LinkedIn platform had approximately 800 active job vacancies related to cyber security skills in Ireland (as shown in Figure 5.1). Please note this only tracks job vacancies posted or identified on LinkedIn, and may therefore underestimate wider demand for cyber security roles across Ireland posted on alternative platforms or job boards.

The research team undertook an initial analysis of these job vacancies where appropriate. This includes a review of location and experience. Overall, this suggests that cyber security roles are typically concentrated in Dublin and Cork; however, the rise of remote working means there is more opportunity across the entire island.

Further, the vacancy analysis (Figure 5.2) suggests there is a higher demand for cyber security employees with middle to senior-level experience (typically 5+ years). Whilst this may reflect the nature of advertising through LinkedIn, it suggests a need to further develop domestic entry-level talent to help stem the skills gap.

[24] Kesselring, L. (2017). 'Cyber Security Skills Crisis Causing Rapidly Widening Business Problem'. Available at: https://www.prweb.com/releases/2017/11/prweb14899778.htm

[25] ISC2 (2021). 'A Resilient Cybersecurity Profession Charts the Path Forward'. Available at: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

[26] Somers, C. and Byrne, E. (2021) 'Cyber Security Skills Report 2021' Available at: https://cyberireland.ie/wp-content/uploads/2021/02/Cyber-Ireland-Skills-Report-2021.pdf

FIGURE 5.1 NUMBER OF JOB POSTINGS (DECEMBER 2021)

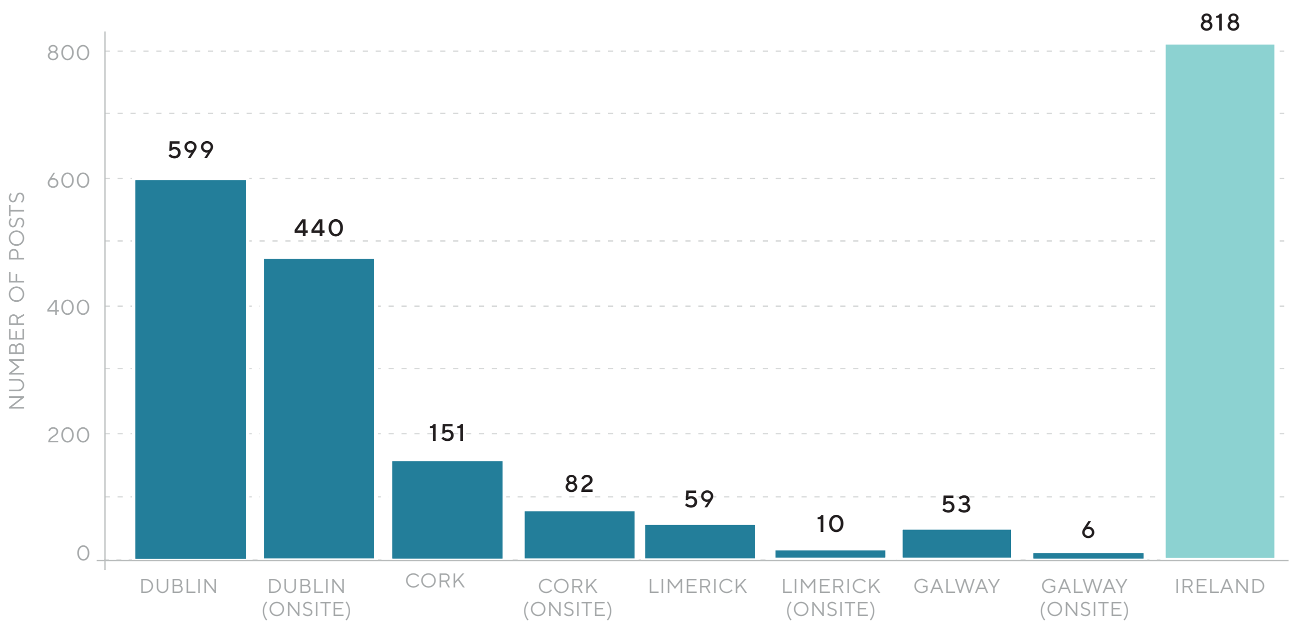
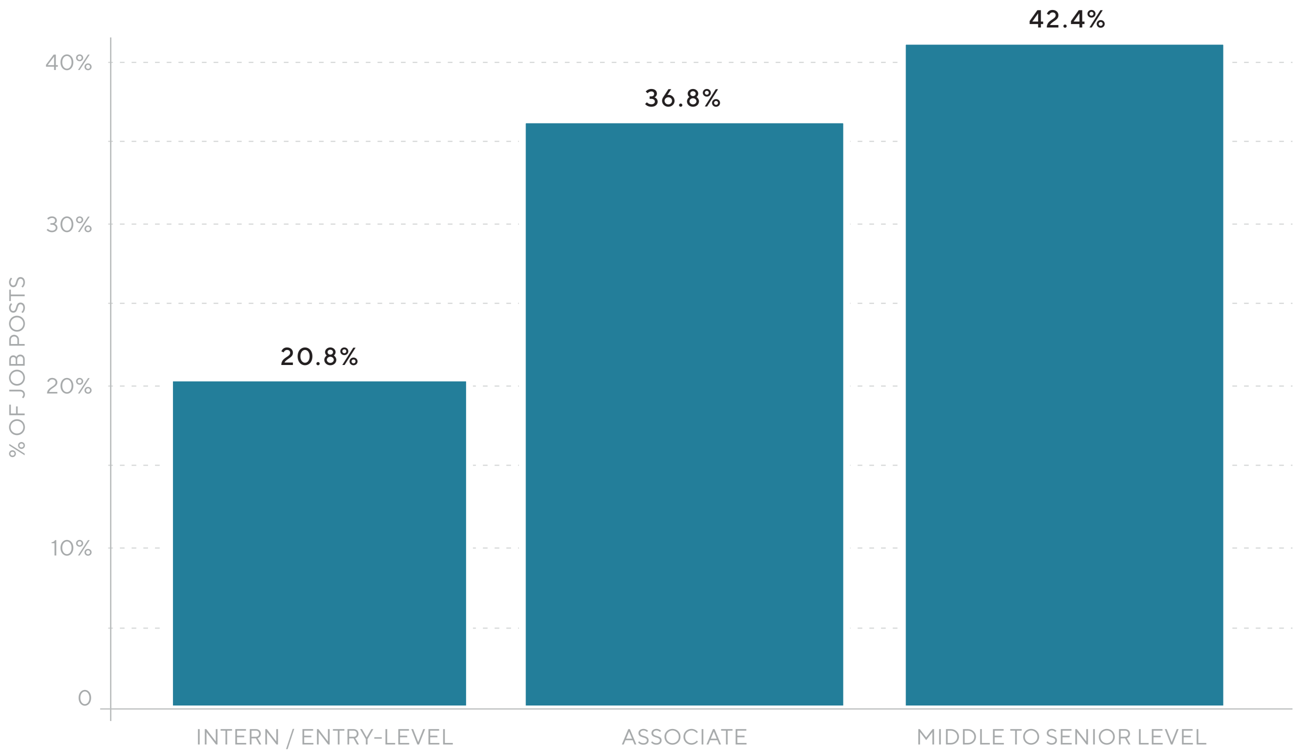


FIGURE 5.2 JOB POST EXPERIENCE LEVEL



Source: LinkedIn recruitment data (December 2021)
Source: LinkedIn recruitment data (December 2021) (n=658 with experience level requested)

Excluding recruitment firms, key advertisers identified through LinkedIn job postings for cyber security related roles include EY (27 posts), Amazon (26), State Street (18), BAE Systems Applied Intelligence (17), Acronis (16), Avanade (15), Zurich Insurance (13), and TikTok (13).

Our estimates suggest that approximately one in every three hundred people currently employed in Ireland are engaged in cyber security services.[27] In comparison to this, in December 2021, approximately one in every fifty job posts on LinkedIn are directed towards cyber security professionals. This suggests a strong demand for staff in the sector, with firms competing for talent, which in turn signals the need for further skills interventions and supply. It is therefore crucial that Ireland considers how it can increase the supply of new talent to meet this growth.

Assuming comparable growth (+10% compound annual growth from the current baseline), the Irish cyber security sector could scale to the region of 15,000+ cyber security professionals by 2030. Therefore, thousands of individuals will need to be trained and recruited into the sector to meet this demand.

Globally, the increased gap in the skills market has led several multinational firms to engage with education to support upskilling and reskilling in the market. Microsoft has launched a scheme in the US to train 250,000 professionals by 2025[28], an approach it has also taken in Northern Ireland, supporting the creation of 85 new jobs.[29] Google and IBM are also engaging with the labour market to increase skills and train staff, collectively committing to train a quarter of a million staff.[30]

This suggests that industry can engage with government and academia to increase momentum, and reduce barriers of entry into the sector.

In Ireland, similar training programmes for cyber security exist from entry-level programmes (such as Future in Tech, CyberQuest, FIT Cyber Apprenticeship and Cyber Bootcamp) to industry upskilling through Cyber Skills, which aims to train up hundreds of professionals from industry into cyber roles within their organisations.

It is therefore essential that increased engagement with industry will be required to ensure that a pipeline of suitably trained talent can be developed to support international demand, to support domestic markets, and to ensure that other parallel sectors are not displaced.

[27] Trading Economics (2022). 'Ireland Employed Persons' Available at: https://tradingeconomics.com/ireland/employed-persons

[28] Cyber. (2021). 'Microsoft to train 250k new cybersecurity workers by 2025'. Available at: https://cybermagazine.com/cyber-security/microsoft-train-250k-new-cybersecurity-workers-2025

[29] 4NI (2020) 'Microsoft Creates 85 Jobs In Belfast'. Available at: https://www.4ni.co.uk/northern-ireland-news/269754/microsoft-creates-85-jobs-in-belfast

[30] Business Insider (2021). 'Big tech firms pledge more than $31 billion and 250,000 jobs to strengthen cybersecurity'. Available at: https://www.businessinsider.com/apple-amazon-google-microsoft-ibm-pledge-31-billion-to-cybersecurity-2021-8?r=US&IR=T

06 Investment in Ireland's Cyber Security Sector

6.1 INTRODUCTION

The cyber security sector is of increasing interest to the investor community, and 2021 was a record year for the cyber security market[31] in terms of investment and strategic activities, reflected by deals, mergers, and Venture Capital (VC) activity, surpassing $20bn in 2021[32].

The increased move to working from home, alongside spikes in ransomware and critical zero-day vulnerabilities is likely to sustain this global demand for investment in establishing and emerging cyber security firms.

Crunchbase's Global Cybersecurity Venture Funding research (2021) explores how the global cyber security venture capital scene has grown in recent years. It suggests that:

- Investment in cyber security firms has grown more than ninefold since 2011;
- Over $20bn has been raised globally by cyber security firms in 2021;
- Over three quarters (76%) of investment in 2020 was raised by US companies, followed by Israel (13%) and the UK (3%).

Ireland can benefit from this increased investment in cyber security firms in two ways. First, directly, where investments in Irish cyber security start-ups and SMEs can fund expansion and growth in operations. Second, indirectly, whereby international firms raise funds that can be used to fund expansion and growth in their Irish divisions.

This section explores investment in Irish firms by Venture Capital using the Crunchbase database, where the 489 businesses identified within the sectoral analysis have been matched against Crunchbase to identify respective investments.

This focuses upon dedicated cyber security firms registered (headquartered) in Ireland that have secured external investment within the last five years, whereby the investment raised has been publicly available / identified by Crunchbase.

6.2 INVESTMENT METRICS

Using Crunchbase data, we have identified **twenty dedicated cyber security practices headquartered in Ireland** that have secured external investment (i.e. at least one funding round).

In total, these twenty firms have raised over $130m (>€110m) in external investment in the last five years. Please note some investments are undisclosed, and as such, this figure may be higher.

Some notable investments, which are profiled in Section 6.3, raised include companies such as Tines, 4Securitas, Vaultree, and Nova Leah.

6.3 INVESTMENT CASE STUDIES

An overview of firms that have successfully raised funds in Ireland is presented below. These firms offer a good example of how Irish firms can scale and grow to meet the needs of clients internationally.

[31] CPO Magazine (2021) '1H 2021 Cybersecurity Market Sees Record Investment Activity; Cybersecurity Stocks Outperform NASDAQ and S&P'. Available at: https://www.cpomagazine.com/cyber-security/1h-2021-cybersecurity-market-sees-record-investment-activity-cybersecurity-

[32] Crunchbase (2022) Cybersecurity Venture Funding Surpasses $20B In 2021, Fourth Quarter Smashes Record. Available at: https://news.crunchbase.com/news/cybersecurity-venture-funding-2021-record/?utm_source=cb_daily&utm_medium=email&utm_campaign=20220106&utm_content=intro&utm_term=content&utm_source=cb_daily&utm_medium=email&utm_campaign=20220106

tines	Tines automation solution supports cyber security professionals in managing and mitigating risks, supporting threat intelligence interventions, vulnerability management, endpoint detection and response, and fraud analysis and reporting. Tines has successfully raised $41m across 3 funding rounds. The company received initial funding in Q4 2019 and has since then received investment in Q1 2021, and again in Q2. Investors include Blossom Capital, Accel, Silicon Valley CISO Investments among others.
NOVA LEAH	Nova Leah develop expert cybersecurity risk assessment solutions specific for connected medical devices. Nova Leah has successfully raised €6.5m across 3 funding rounds between Q4 2017 and Q1 2019. Investors include Enterprise Ireland, COSIMO Venture, Sure Valley Venture, and Kernal Capital. The firm has recently received backing from the venture arm of US-health giant Northwell Health, a New York healthcare provider with 23 hospitals and 830 outpatient facilities, and has continued ambitions to grow.
Vaultree	Vaultree offer encryption as a service that enables firms to communicate safely in a manner that supports compliance. Vaultree has successfully raised $3.3m in their first funding round during Q4 of 2021. Investors include Enterprise Ireland, Unpopular Ventures, Halo Business Angel Network, TenEleven Ventures among others.
4SECURITAS PROTECTING YOUR DATA ASSETS	4Securitas provide a 'post-perimeter' security tool that complements a traditional perimeter security model that resides at the application or data layer and monitors and protects physical/VM/Cloud/Container platforms where the data is stored. 4Securitas raised €2.4m worth of funding across 2 funding rounds in October 2019 and September 2021. Investors include AVM Gestioni, Enterprise Ireland, and ITrust.

These firms reflect several of the core recommendations included within Enterprise Ireland's European Cybersecurity Market opportunity mapping exercise.[33] Those most relevant include:

- Offer products/services that can be included in major ICT companies, integrators, and Cybersecurity providers' offer to large customers;
- Ensure compatibility and interoperability with target customer's systems;
- Leverage available networks to gain access to new markets; and
- Capitalise on current "hot" cyber security sub-segments.

6.4 INVESTMENT SUPPORT LANDSCAPE

Ireland's domestic tech start-up and scale-up sector employ c.47k people across c.2,000 companies, almost half of which are based outside of Dublin. Those employed in scale-up companies are typically in high-value jobs and support wider job creation at a ratio of 5:1.[34]

While the COVID-19 pandemic reduced the number of new investments across Ireland (a trend that was seen globally)[35], previous years suggest that Ireland's technology sector is maturing.

Investment for cyber firms is likely to increase given the commercial opportunities that exist within the sector. [36] Scale-up firms engaged in sectors such as cyber security are unique in that they typically face a negative cash flow in their early stages, but are considered vital to support the rapidly evolving, open knowledge economy.

In addition to private venture capital, Ireland's cyber security sector can seek support from Enterprise Ireland (EI), Ireland's indigenous SME support agency, and Venture Capital arm of the government.

EI is the largest seed capital investor in Ireland and one of the world's largest seed-stage Venture Capitals, which supports indigenous firms with global ambition.

EI invests directly in start-up companies and their Growth Capital Team manage investments, as Limited Partners, into venture capital funds. They directly invest in over 70 High Potential Start-Up companies each year and manage a portfolio of over 1300 investments in client companies.

EI provides c. 400 supports to firms in Ireland, which are signposted in the "Start in Ireland" service. These include specific support and investment for start-ups and scale-ups such as the New Frontiers Programme, Competitive Start Fund (CSF), and Innovative HPSU Fund (Equity)[37].

[33] Enterprise Ireland (2019). 'The European Cybersecurity Market Mapping The Opportunities And Route To Market For Irish SMES'. Available at: https://globalambition.ie/wp-content/uploads/2019/11/The-European-Cybersecurity-Opportunities-for-Irish-SMEs_Key-Takeouts.pdf

[34] Scale Ireland (2022). 'Promoting Irish Tech Start-ups & Scale-ups '. Available at: https://www.scaleireland.org/

[35] Earley, K. (2020). 'How has Irish start-up funding been impacted by Covid-19?'. Available at: https://www.siliconrepublic.com/start-ups/startup-funding-ireland-covid19-techireland

[36/37] Enterprise Ireland (2020). 'In Ireland cybersecurity takes center stage - The Irish Advantage'. Available at: https://irishadvantage.us/in-ireland-cyber-security-takes-center-stage-us/

07
Opportunities for Ireland's Cyber Security Sector

7.1 INTRODUCTION

Ireland is well placed as an enterprise-friendly point of entry into the European Union and is home to a highly-skilled, English-speaking workforce. Furthermore, it holds a range of public and industry-driven research facilities and is developing a pipeline of talent.

This section provides an overview of the projected growth within Ireland's cyber security sector alongside the key market opportunities and challenges that exist within the sector that can impact a sustainable growth rate.

7.2 GROWTH POTENTIAL

As set out previously, we estimate that the cyber security sector in Ireland currently employs more than 7,350 people, and generates direct GVA for the Irish economy of approximately €1.1bn per annum.

As this is the first baseline report, there is limited data regarding the size and scale of the sector in previous years. However, we estimate that the sector has the potential to grow by a similar percentage as areas such as the UK. We estimate that compound annual growth is likely to be in the region of 10%.

Applying a 10% annual growth rate to the current estimates suggests that Ireland's cyber security sector could scale to approximately €2.5bn in annual GVA and support over 17,000 cyber security roles by 2030, as outlined below:

TABLE 7.1 GROWTH PROJECTIONS (10% CAGR SCENARIO)

	GVA	EMPLOYMENT
2021	**€1,075,523,670** (current estimate)	**7,351** (current estimate)
2022	€1,183,076,038 (projection)	8,086 (projection)
2023	€1,301,383,641	8,895
2024	€1,431,522,005	9,784
2025	€1,574,674,206	10,763
2026	€1,732,141,627	11,839
2027	€1,905,355,789	13,023
2028	€2,095,891,368	14,325
2029	€2,305,480,505	15,758
2030	**€2,536,028,556 (c. €2.5bn)**	**17,333**

Source: Perspective Economics

INDUSTRY ATTITUDE TO GROWTH

Cyber Ireland's business survey, conducted as part of this research, provides insight into the attitude towards growth within Ireland's cyber security market. In total, 83% of businesses expect that their cyber security team will grow over the next twelve months, and more than half (51%) expect that this growth will occur at a rate of 25% or higher.

Some of the expected avenues to growth include:

- **Expansion of current services** through graduate recruitment;
- **Expansion to meet market requirements** (i.e., increased technology use due to the global pandemic);
- Expansion supported by **larger-scale projects;**
- **Merger and acquisition** of smaller firms (domestic firms, dedicated to cyber security service provision, have been responsible for at least fourteen identified acquisitions to date)[38]; and
- Leveraging of international presence to attract further **international investment** to Ireland.

CHALLENGES TO GROWTH

The potential for growth outlined above also presents an important challenge to industry, government, and academia. While responses in Cyber Ireland's business survey demonstrate optimism and commitment, key challenges facing the sector were also highlighted. Core challenges are outlined below:

- **61% of respondents noted a personnel-related issue**, such as a lack of candidates in the labour market with the **appropriate skill level** (41%), **competition** from other cyber security businesses (33%), lack of **non-technical skills** (22%), or unaffordable salaries (21%)
- **33% of respondents viewed market uncertainty as a barrier to the business**, specifically related to **COVID-19** (24%) or the **UK's Exiting from the European Union** (11%)
- **26% faced issues with raising or securing finance**, such as a **lack of finance to grow or expand operations** (16%), **insufficient scale** to serve larger clients (14%), or a **lack of cash flow** or working capital (8%).

[38] Crunchbase (2022) 'About Crunchbase'. Available at: https://about.crunchbase.com

DEVELOPING A TALENT PIPELINE

Note that in 2021, Cyber Ireland launched its first 'Cyber Security Skills Report'. This separate report further outlines the need to address cyber security skills shortages in Ireland.

We provide a summary of some of the key opportunities in Ireland that should be explored collaboratively between the public and private sector to support growth and to encourage entry into the sector.

- **Ireland should leverage the skill level within its current workforce**, as it is home to the highest ratio of AI talent in Europe [39], and higher than average third-level attainment among 30-34-year-olds (55%, in comparison to the EU average of 40%). Overall, it is home to c.30k professionals with relevant cyber security skills, and c.50 courses developed in line with industry needs.
- With increased engagement with industry and academia, Ireland can **support education and entry into the sector** to ensure demand for skills does not outweigh supply. While there is a strong pipeline of talent in Ireland, more is needed to address the wider shortfall within the cyber security workforce. This could include greater incorporation of security concepts or training into more general STEM-based or IT-specific courses, targeting core cyber skills such as security analysis, incidence response, and threat intelligence [40]. Increased engagement with both industry and academia could also reduce latency between academic learning and industry needs.
- **Transitioning workers with relevant skills from parallel industries will also support the maturing sector.** This should involve industry schemes, government support, and include programmes such as Springboard+ and apprentice programmes, such as FastTrack to Information Technology (FIT).
- Ireland should also **promote itself as a destination for learning, incentivising students to study, and work in Ireland.** This exists currently in the form of a 2-years residency visa post-study, and scholarships that cover up to 50% of tuition fees [41] for applicable cyber security students. It should be noted that affordability and cost of living can play a role in whether Ireland is seen as a viable location for study. Therefore, courses outside of the capital city could be promoted, or subsidies considered for prospective students.
- **Ireland could also explore apprenticeship or retraining schemes** that support collaboration between international businesses and academic institutions. This has worked well in Northern Ireland, with Microsoft supporting a pre-employment training course with Belfast Met that will result in c.85 new jobs based within Microsoft's new Cyber Security Centre.

[39] DA Ireland (2021). 'Why Ireland for Cyber Security'. Available at: https://www.idaireland.com/newsroom/publications/why-ireland-for-cyber-

[40] Am Cham (n.d). Ireland The Strongest Link in the Chain - Ireland's Global Cyber Security Leadership. Available at: https://www.amcham.ie/getattachment/555c3301-643a-4a90-b05f-5bf05a966cb1/AmCham-Ireland-The-Strongest-Link-in-the-Chain-Ireland-s-Global-Cyber-Security-Leadership.pdf.aspx?ext=.pdf

[41] Go Ireland (2022). 'Masters in Cyber Security in Ireland | MS in Cybersecurity in Ireland'. Available at: https://www.goireland.in/cyber-security-course-ireland

7.3 PROMOTION OF IRELAND WITHIN THE GLOBAL CYBER SECURITY SUPPLY CHAIN

Ireland has the opportunity to position itself within the global cyber security supply chain. This can include increased engagement with foreign-owned firms seeking access to EU markets, and for domestic firms, seeking to internationalise.

Our research explored the importance of exporting and international trade through the Cyber Ireland business survey. The business survey highlighted that **80% of surveyed firms (n=71) develop either products or services for export.**

Table 7.2 provides an overview of responses broken down by firm headquarters (domestic or foreign-owned) and company size (large or SME).

TABLE 7.2 BUSINESS SURVEY – EXPORT REGIONS

	ALL FIRMS	DOMESTIC FIRMS	FOREIGN-OWNED FIRMS
Percentage of surveyed firms that export	80%	83%	79%
For firms that export, key regions			
Europe incl. EU, EEA, EFTA	89%	83%	100%
United Kingdom	86%	93%	87%
North America	73%	70%	80%
Asia-Pacific	61%	55%	70%
Gulf States	38%	33%	47%
Central or South America	32%	23%	47%
Africa	27%	20%	37%
Other	6%	5%	7%

Source: Cyber Ireland Business Survey

OPPORTUNITY TO SUPPORT DOMESTIC BUSINESSES TO EXPORT

Table 7.2 outlines that for domestic firms, the UK is the primary export market (37 responses, 93%), followed by Europe and the US.

In comparison to this, 100% of foreign-owned firms that completed the business survey export to the EU. This suggests that there is an opportunity to promote greater entry into EU markets for domestic firms.

These firms are well placed to support further international engagement as Ireland is now the primary English-speaking nation in the EU, hosts approximately 30% of the EU's data, and is ranked 7th out of 28 EU member states in the European Commission Digital Economy and Society Index (DESI) 2019.[42] Ireland is also a member of Digital 9 (D9), which is a group of digital frontrunners within the EU, championing issues such as the free flow of data initiatives.

OPPORTUNITY TO ATTRACT NEW MULTINATIONAL FIRMS

Ireland already has a wide array of assets and credentials that make it attractive to foreign markets. These include Ireland's range of pro-trade and investment policies which encourage the development of high-value-added industry clusters. Ireland's national strategy also recognises the importance of cyber security in supporting Ireland's digital economy.[43]

Accenture reports that Ireland is home to the highest proportion of cybersecurity leaders globally.[44] "Leaders" are firms that achieve "significantly better results from their cyber security technology investments than other organisations", delivering and developing solutions at the highest standard within industry. This showcases the current skill level of Ireland's cyber security workforce.

The promotion of Ireland as an international destination for cyber security is key, as often the supply chain within the cyber security sector is global, operating across markets.

While Ireland's unique position can be leveraged to support its existing connections internationally, it can also be used to engage UK-based firms that have an office in Ireland, or who are considering setting up an office to support existing relationships with EU operations.

Currently, there are c.50 UK-based firms with a cyber security team operating in Ireland, including firms that offer diversified services such as PwC, EY, and KPMG, as well as dedicated firms such as Sophos.

UK-based Calligo is a key example of a UK firm expanding into Irish markets. Calligo completed the acquisition of Irish firm Cinnte in November 2020, which is their third acquisition of an Irish firm in three years as part of a wider growth plan that includes five other international acquisitions.

[42] Privacy Solved (2022). 'Cybersecurity: Focus on Ireland's National Cyber Strategy'. Available at: https://www.privacysolved.com/cybersecurity-focus-on-irelands-national-cyber-strategy/

[43] Rialtas na hÉireann (2019). National Cyber Security Strategy 2019-2024. Available at: https://www.skillnetireland.ie/wp-content/uploads/2020/01/National-Cyber-Security-Strategy-2019-2024.pdf

[44] TechCentral (2020). Ireland has highest proportion of cyber security leaders globally. Available at: https://www.techcentral.ie/ireland-has-highest-proportion-of-cyber-security-leaders-globally/

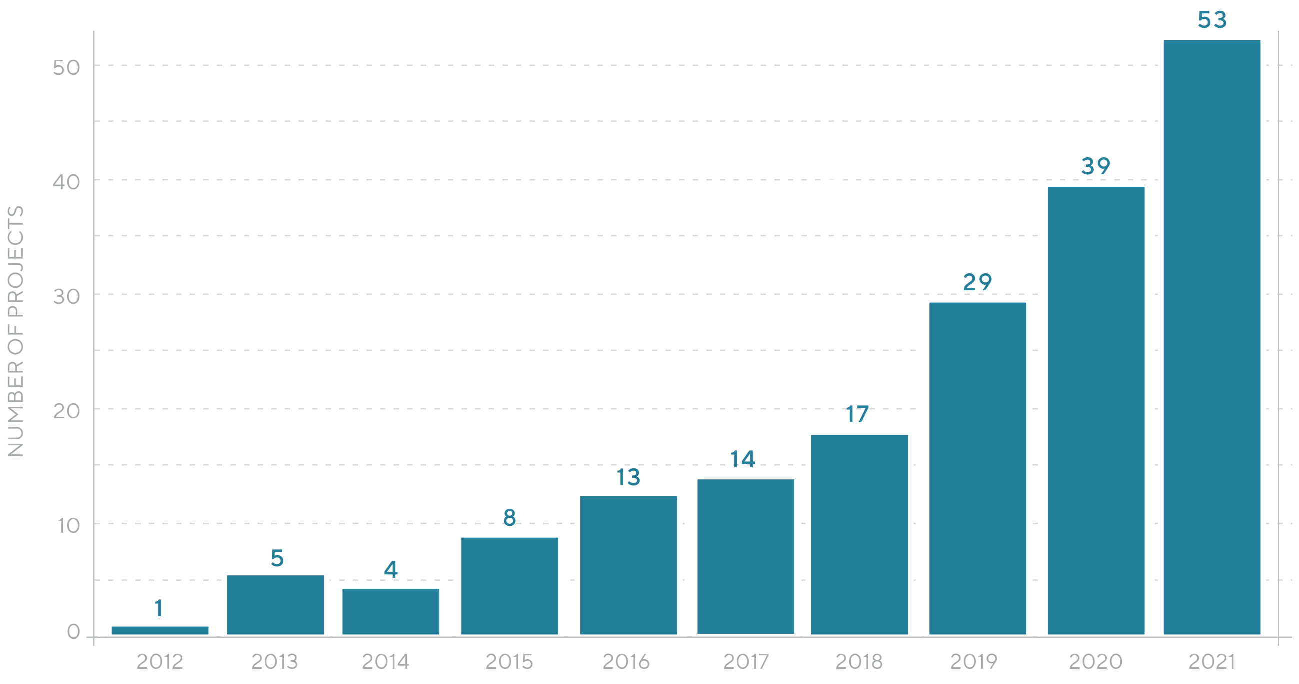
7.4 LEVERAGING INCREASED PUBLIC SUPPORT

There is an opportunity in Ireland to support sector growth by leveraging public support. Following the cyber-attack on Ireland's health service, there has been a greater commitment to support the market nationally. These include the commitment to nearly doubling the number of staff in the National Cyber Security Centre over an 18-month period, to increasing annual budgets by €2.5m and to provide wider support for the sector through other avenues, such as a cyber security graduate training programme.

SUPPORTING GROWTH THROUGH PUBLIC PROCUREMENT

The public sector can play a critical role in shaping the cyber security sector as a key buyer of products and services. An analysis of tenders published publicly in Ireland[45] was conducted to assess current and historic demand for cyber security services between 2012 and 2021. Tenders were identified using pre-existing categories defined by Ruohonen (2020)[46] which are based on project CPV codes. The number of tenders publicly advertised is presented below, showing a tenfold increase in procured projects in a ten-year period:

FIGURE 7.1 NUMBER OF PUBLICLY PROCURED TENDERS



Source: Published tenders - eTenders Public Procurement - EU Supply

[45] Etenders (2022). 'Published tenders'. Available at: https://irl.eu-supply.com/ctm/Supplier/PublicTenders

[46] Ruohonen, J. (2020). 'An Acid Test for Europeanization: Public Cyber Security Procurement in the European Union'. Available at: https://www.semanticscholar.org/paper/An-Acid-Test-for-Europeanization%3A-Public-Cyber-in-Ruohonen/

The most common services requested included support in delivering/ developing security software packages (n=95), data security software packages (n=59), data security software development services (n=38), security software development services (n=32), and file security software packages (n=30).

The growth in public procurement opportunities should be utilised as a crucial growth driver for Ireland's cyber security sector where possible. There is an opportunity to engage the government to ensure that future tenders support larger firms as well as domestic firms at the scale-up and start-up stage.

Future tenders should be tailored to facilitate growth within the sector, with Cyber Ireland's business survey highlighting that:

- **Contracts can be too restrictive for newer firms to engage with:** "We have the skills and experience to compete with the bigger players in the market but as we are a new company many opportunities have passed us by due to a lack of years in business and revenue currently generated."; and
- **Contracts not suitable for SME firms:** "A lack of contracts targeted for SMEs"

GOVERNMENT'S ROLE IN SUPPORTING SECTOR GROWTH

While Ireland has committed to increasing its budget for cyber security services it should be highlighted that there has been a historic underspend in Ireland's public sector on cyber defence.[47]

The Global Cyber Security Index (2020)[48] is an initiative of the International Telecommunication Union that compares national capabilities across five core areas: legal measures, technical measures, organisational measures, capacity development, and cooperative measures.

While the GCI notes that Ireland shows relative strength in legal and technical areas it also suggests that more can be done to develop national cooperative measures.

Cooperative measures are those: "based on the existence of partnerships, cooperative frameworks, and information sharing networks... Greater cooperation can enable the development of much stronger cybersecurity capabilities, helping to mitigate cyber risks and enable better investigation, apprehension, and prosecution of malicious agents".

Increased engagement with the sector and wider networks has the potential to increase awareness of cyber threats in Ireland's business landscape, where **61% of businesses reported that they suffered a cybercrime between 2017 and 2019. This is slightly more than UK businesses**, of which 46% of which reported a breach.[49]

Increased collaboration both nationally, and with wider markets is strategically aligned to goals set out in the EU's Declaration on "European Data Gateways as a key element of the EU's Digital Decade"[50] which commits to:

- strengthen international partnerships for connectivity;
- offer EU data storage and processing services to partners outside of Europe; and
- ensure safe and secure connectivity networks.

With Ireland's even split of domestic and foreign-owned firms and Ireland's data-hosting capabilities, there is an opportunity for the sector to position itself as a gateway into Europe.

[47] Hurley, S., (2021). Ireland should spend '10 times more' on cyber security. Available at: https://www.rte.ie/news/2021/0525/1223759-hse-cyber-attack/

[48] International Telecommunication Union (2020) Global Cybersecurity Index. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[49] Stryvesecure (2021) 'How The UK and Ireland Compare When it Comes to Cybersecurity?'. Available at: https://www.stryvesecure.com/blogs/how-the-uk-and-ireland-compare-when-it-comes-to-cybersecurity

[50] European Commissiom (2021) Digital Day 2021: Europe to reinforce internet connectivity with global partners. Available at: https://digital-strategy.ec.europa.eu/en/news/digital-day-2021-europe-reinforce-internet-connectivity-global-partners

ATTITUDES TO COLLABORATION

Cyber Ireland's business survey assesses to which extent firms are engaging with wider networks. Overall:

- 56% of firms engaged with a cyber security cluster;
- 51% engaged with a university, Institute of Technology, or other higher education provider;
- 44% engaged with a public organisation that offered economic development support (e.g., Enterprise Ireland, local council);
- 35% engaged with other cyber security businesses;
- 33% engaged at meetup events; and
- 20% engaged with other public sector bodies.

Some of the commonly cited reasons for collaboration included increasing awareness of brand (60%), making new business deals (46%), supporting R&D activities (31%), providing mentorships to others (21%), and attracting investment (17%).

This suggests that firms are willing to collaborate to promote their business and to increase their presence within the national sector and that while there are varying levels of participation, there is still potential to increase engagement with networks, academia, government, and wider industry.

Cluster initiatives, therefore, continue to play an important role in encouraging collaboration among SMEs. Given the distribution of micro, small and medium firms in Ireland, such initiatives provide an optimum opportunity to scale activities or to promote engagement with larger, or established firms already present in Ireland's cyber security sector.

08 Key Findings and Recommendations

This section provides an overview of key findings identified within the project, alongside some recommendations to help stimulate and sustain future growth in the industry.

8.1 KEY FINDINGS

- We have identified 489 firms offering a product or service within the sector, or that employ cyber security professionals into their wider R&D teams.
- Of the 7,351 employees in the sector, 71% are employed in a firm headquartered overseas. US-headquartered firms, in particular, play a pivotal in shaping the sector, supporting 55% of all employment.
- The number of large multinationals is significantly higher than in other studies, which shows potential for team-based growth for foreign-owned firms in Ireland, while Irish firms are typically SMEs, suggesting they would benefit from support services to increase their size and scale.
- There are 734 offices across the country, mainly concentrated in Dublin, Cork, Galway, and Limerick but with emerging growth nationwide. While Dublin is home to more offices overall, both Cork and Galway have more firms per capita and host a range of assets that support the development of a thriving cyber security ecosystem.
- The cyber security sector is currently generating approximately €1.1bn in direct GVA for the Irish economy.
- GVA per employee within the cyber security sector is strong in Ireland (€150k) signalling a productive workforce. This compares favourably to the UK estimate of c. £100k (c. €120k).

8.2 STRENGTHS & OPPORTUNITIES

- Ireland is well placed as an enterprise-friendly point of entry into the European Union and is home to a highly-skilled, English-speaking workforce.
- Ireland has a range of pro-trade and investment policies which encourage the development of high-value-added industry clusters, and the national strategy recognises the importance of cyber security in supporting Ireland's digital economy. It is also in a strong position to promote relevant assets to potential investors, and showcase outputs delivered by its network of R&D facilities.
- Ireland hosts approximately 30% of EU data and is ranked 7th out of 28 EU member states in the European Commission Digital Economy and Society Index (DESI) 2019.
- Ireland is home to the highest proportion of cyber security leaders globally, these are firms that achieve "significantly better results from their cyber security technology investments than other organisations", delivering and developing solutions at the highest standard within industry, which showcases the current standard and skill-level of the cyber security workforce.
- The cyber security sector is growing (with respect to the workforce) in Ireland by a similar magnitude to international growth (at a rate of 10%+ per annum). This suggests that based on the current baseline estimates, Ireland's cyber security ecosystem could support up to €2.5bn in annual GVA and the employment of over 17,000 cyber security professionals in the sector by 2030.
- Ireland already has a range of services available to support firms at the start-up and scale-up level. Ireland's unique split of domestic and foreign-owned firms also presents an opportunity for investment both directly and indirectly. First, directly, where investments in Irish cyber security SMEs can fund expansion and growth in operations. Secondly, indirectly, whereby larger international firms raise funds that may be used to fund expansion and growth in their Irish divisions.
- Ireland has an opportunity to attract FDI firms seeking to avail of EU data storage and processing services. Ireland has a growing reputation as a cyber security hotspot strategically placed as the primary English-speaking country in the EU, boasting an array of research facilities across each of its core clusters.
- The public sector can also play a critical role in shaping the cyber security sector as a key buyer of products and services. The analysis of tenders published publicly suggests a year-on-year increase in procurement activity that should be utilised as a crucial growth driver for Ireland's cyber security sector where possible.
- The cyber-attack on the HSE in Ireland resulted in further commitments to increase public spend on cyber security services. Longitudinal analysis of procurement data also suggests an increase in government spend. There is an opportunity for future procurement activity to be tailored to support sector entry, scale-up, and partnerships between larger firms and SMEs. There is considerable potential for wider collaboration between both the private and public sector to protect infrastructure and businesses across the Irish economy.

8.3 CHALLENGES

- Findings from Cyber Ireland's business survey suggest that over half of firms surveyed have staff-related issues, including lack of suitable candidates, skill-level, and unaffordable salaries.
- There are a wide range of studies exploring the shortfall in cyber security talent, against a backdrop of increased demand, with one of the most significant factors leading to data breaches across digital structures globally being the lack of training of non-technical employees and the lack of highly skilled cybersecurity professionals. [51]
- The ISC2 Cybersecurity Workforce Study (2021) [52] estimates that Ireland has an annual shortfall of approximately 10,000 people in cyber security roles (across the broader economy). This is also explored in the Cyber Ireland Cyber Skills Report 2021.[53]
- Vacancy analysis using LinkedIn data suggests there is a higher demand for cyber security employees with middle to senior-level experience (typically 5+ years). Whilst this may reflect the nature of advertising through LinkedIn, it also suggests a need to further develop entry-level talent to help stem the skills gap.
- Wider barriers reported by firms include uncertainty linked with COVID-19 and the UK's exit from the EU, and issues linked with accessing and securing finance.
- The overall level of collaboration within Ireland's cyber security sector and wider networks can be increased. Both Cyber Ireland's business survey and the GCI Index suggest that there is potential for Ireland to grow its existing "partnerships, cooperative frameworks and information sharing networks
- There is also more that can be done to increase awareness of cyber threats in Ireland's business landscape with 61% of businesses reporting that they suffered a cybercrime between 2017 and 2019. This is slightly more than UK businesses, of which 46% of which reported a breach.[54]

[51] Kesselring, L. (2017). 'Cyber Security Skills Crisis Causing Rapidly Widening Business Problem'. Available at: https://www.prweb.com/releases/2017/11/prweb14899778.htm

[52] ISC2 (2021). 'A Resilient Cybersecurity Profession Charts the Path Forward'. Available at: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

[53] Somers, C. and Byrne, E. (2021) 'Cyber Security Skills Report 2021' Available at: https://cyberireland.ie/wp-content/uploads/2021/02/Cyber-Ireland-Skills-Report-2021.pdf

[54] Stryvesecure (2021) 'How The UK and Ireland Compare When it Comes to Cybersecurity?'. Available at: https://www.stryvesecure.com/blogs/how-the-uk-and-ireland-compare-when-it-comes-to-cybersecurity

8.4 RECOMMENDATIONS

There are a range of recommendations that should be considered by government, industry and academia to take forward to help promote sustainable growth within the sector. These include:

Developing a talent pipeline:

1 There should be an increased emphasis on developing a pipeline of suitable talent to support sustainable growth within the sector. This could involve engagement with industry to ensure existing courses offer a curriculum that prepares students for a career within the sector, teaching them the skills necessary to engage at an entry-level. There is also potential to promote cyber security to students in wider STEM or IT courses by encouraging universities to offer relevant cyber security modules to more general learning.

2 Further initiatives such as reskilling and retraining could also promote entry into the cyber security sector. There is a good baseline of technical talent in Ireland also, with current estimates suggesting that there are c.80k professionals engaged in technological sectors in Ireland.[55] There is potential to support firms by developing transition courses or training schemes to support entry from other industries to address skill shortages.

Government's role in supporting the sector through awareness, procurement, and business support:

3 Public sector commitment to supporting cyber security services has increased. This could help Ireland to improve national resilience. The recent attack on HSE should demonstrate the importance of investment in cyber security, and increased integration of cyber security practices across all aspects of society. Ireland can also learn from international models undertaken in countries such as the UK, Estonia, USA and Israel.

4 Public procurement is a powerful mechanism for increasing spend on cyber security and promoting resilience across the Irish economy. Within the business survey, conducted for this research, many firms report that specifications for tenders can be restrictive and difficult to engage with. We suggest that there is potential to engage further with cyber security SMEs to help co-create inclusive and impactful tender opportunities, which would also help cyber security SMEs to scale domestically.

5 Many cyber security SME firms reported that they are experiencing a competitive labour market, particularly with respect to competing with salaries offered by larger firms. The government could consider supporting the development of the domestic ecosystem through the enhanced use of grants and initiatives to support employment growth within start-ups and scale-ups.

[55] An Rionn Fiontar, Trádála, agus Fostaíochta | Department of EnterpriseTrade and Employment (2022). 'Attracting Tech Talent to Ireland'. Available at: https://enterprise.gov.ie/en/What-We-Do/Workplace-and-Skills/Skills-for-Enterprise/Attracting-Tech-Talent-to-Ireland/

6 The success of cyber security services hinges upon their application across different global regions. The composition of Ireland's sector suggests that foreign-owned firms have been particularly successful in developing cyber security teams in Ireland. Ireland's expertise and attractiveness as a location for setting up cyber security teams could be used to encourage further investment from external firms seeking to further develop their cyber security capability and capacity.

Promoting clusters and collaboration:

7 Sector composition indicates that domestic firms in Ireland typically have smaller teams. These firms are therefore likely to benefit from increased support focused on scaling up their offering. While there are a range of services available in Ireland, direct engagement with SME firms may increase awareness of services and uptake. There is also wider potential to develop support informed by Enterprise Ireland's European Cybersecurity Market opportunity mapping exercise[56] which focuses on promoting engagement in European markets.

8 Firms also report difficulty engaging with larger firms. Building on the above point smaller firms could also be paired with larger firms to drive collaboration and increase market offering. There is potential to leverage existing connections with organisations such as Enterprise Ireland, IDA Ireland, InterTrade Ireland, and Cyber Ireland to promote business networking and collaboration between domestic SMEs and larger firms.

[56] Enterprise Ireland (2019). 'The European Cybersecurity Market Mapping The Opportunities And Route To Market For Irish SMES'. Available at: https://globalambition.ie/wp-content/uploads/2019/11/The-European-Cybersecurity-Opportunities-for-Irish-SMEs_Key-Takeouts.pdf

09 Appendices

9.1 METHODOLOGY

Cyber Ireland brings together industry, academia, and government to represent the needs of the Cyber Security ecosystem in Ireland to enhance the innovation, growth, and competitiveness of the companies and organisations which are part of the cluster.

The four objectives of the organisation are outlined below and include:

- **Building the Community:** stronger promotion and supporting cross-industry collaboration;
- **Talent and Skills:** ensuring a sustainable pipeline of Cyber Security talent;
- **Research and Development:** enhancing collaborative R&D between industry and academia; and
- **Business Development:** supporting Irish SMEs and start-ups to grow and export globally from Ireland.

This project supports Cyber Ireland's objectives and sets out to create the first comprehensive overview of the Cyber Security sector in Ireland, its contribution to the Irish economy, and the potential for future growth.

The objectives of this study are:

01 To understand the current size and make-up of the cyber security sector in Ireland and to track its future development.

02 To assess the economic contribution of the cyber security sector in Ireland and its importance to the economy.

03 To assess the international cyber security market opportunities for Irish start-ups and SMEs and foreign direct investment opportunities for Ireland.

04 Produce recommendations to support the development and economic growth of Ireland's cyber security sector, from evidence-based assessments.

The objectives above inform the structure of this report, which includes an overview of the size and make-up of the Irish Cyber Security sector, its economic contribution, the current market opportunities, and wider recommendations.

Other outputs include a longlist of firms engaged in Cyber Security operations working in a dedicated or diversified capacity and a survey of approximately 100 firms working in Ireland's cyber security sector.

Within this research, the team has identified 489 providers of cyber security products and ser-vices (aligned to the definition set out within the UK Cyber Security Sectoral Analysis, and the Centre for Secure Information Technologies' sectoral study for Northern Ireland).

Each business has been matched against Companies Registration Office (CRO) registration da-ta (to understand the name, description, locations, etc) and web data. Revenue and employment activity has been identified through the use of company accounts, LinkedIn, and or direct en-gagement with site leads. The key stages are set out below:

SECTOR PROFILING

The sector profile was generated collaboratively with Cyber Ireland and includes known members of Cyber Ireland's network as well as other firms identified in CRO records and identified online through both LinkedIn and general web searches. Search criteria include a c.600-word taxonomy.

The products and services offered within Ireland's cyber security firms were then identified from website descriptions. The final descriptions were used to group firms into six broad service categories, using a 'best-fit' methodology reflecting the main product and service offerings.

This taxonomy used in this study is informed by previous definitions designed in collaboration with the Centre for Secure Information Technology (CSIT), which were developed to reflect the areas of relative industrial strength on the island of Ireland. The definitions span 7 final categories and are outlined below:

- Managed security service provision and advisory services;
- Risk, compliance, and fraud;
- Securing applications, networks, and cloud environments;
- Operational technology, security, and connected devices;
- Threat intelligence, monitoring, detection, and analysis;
- Identification, authentication, and access control; and
- Other firms (i.e., firms that do not fit into the sector in a traditional sense but support employment, e.g., recruitment, internal R&D, IoT-driven security).

A headcount of total employees within the sector was also completed, building on previous engagement undertaken by Cyber Ireland with firms, as well as the review of publicly available employment figures from LinkedIn profiles and CRO.

A business survey was also sent out to the firms. There was a total of 100 responses used to identify the strengths, opportunities, and barriers faced by Ireland's cyber security sector.

ECONOMIC PROFILING AND POTENTIAL

An economic profile of the sector was produced using company accounts data (where available using Bureau van Dijk) and survey responses. Employment estimates were also augmented using the most recent company team size on LinkedIn (filtered by cyber security roles only).

The research team used company accounts and survey data to estimate cyber security-related employment, followed by revenue and GVA. Where there were gaps in data, estimates have been used on a 'per employee basis. A simple CAGR of 10% is assumed for employment and GVA forecasting up to 2030.

9.2 REFERENCES

4NI (2020) 'Microsoft Creates 85 Jobs In Belfast'. Available at: https://www.4ni.co.uk/northern-ireland-news/269754/microsoft-creates-85-jobs-in-belfast

Am Cham (n.d). Ireland The Strongest Link in the Chain - Ireland's Global Cyber Security Leadership. Available at: https://www.amcham.ie/getattachment/555c3301-643a-4a90-b05f-5bf05a966cb1/AmCham-Ireland-The-Strongest-Link-in-the-Chain-Ireland-s-Global-Cyber-Security-Leadership.pdf.aspx?ext=.pdf

An Rionn Fiontar, Trádála, agus Fostaíochta | Department of EnterpriseTrade and Employment (2022). 'Attracting Tech Talent to Ireland'. Available at: https://enterprise.gov.ie/en/What-We-Do/Workplace-and-Skills/Skills-for-Enterprise/Attracting-Tech-Talent-to-Ireland/

Business Insider (2021). 'Big tech firms pledge more than $31 billion and 250,000 jobs to strengthen cybersecurity'. Available at: https://www.businessinsider.com/apple-amazon-google-microsoft-ibm-pledge-31-billion-to-cybersecurity-2021-8?r=US&IR=T

Central Statistics Office (2021). 'Business Demography 2019 - CSO - Central Statistics Office'. Available at: https://www.cso.ie/en/releasesandpublications/er/bd/businessdemography2019/

Centre for Secure Information Technologies (2021). 'Northern Ireland Cyber Security Snapshot 2021'. Available at: https://www.qub.ac.uk/ecit/CSIT/About/Filetoupload,1077295,en.pdf

Comparitech (2022) 'US Cybersecurity Salary & Employment Study - which state has the best prospects?'. Available at: https://www.comparitech.com/blog/vpn-privacy/cybersecurity-employment-study/

CPO Magazine (2021) '1H 2021 Cybersecurity Market Sees Record Investment Activity; Cybersecurity Stocks Outperform NASDAQ and S&P'. Available at: https://www.cpomagazine.com/cyber-security/1h-2021-cybersecurity-market-sees-record-investment-activity-cybersecurity-stocks-outperform-nasdaq-and-sp/

Cyber. (2021). 'Microsoft to train 250k new cybersecurity workers by 2025'. Available at: https://cybermagazine.com/cyber-security/microsoft-train-250k-new-cybersecurity-workers-2025

Department for Digital, Culture, Media and Sport (2021). 'Cyber Security Sectoral Analysis 2021'. Available at: https://www.gov.uk/government/publications/cyber-security-sectoral-analysis-2021

Earley, K. (2020). 'How has Irish start-up funding been impacted by Covid-19?'. Available at: https://www.siliconrepublic.com/start-ups/startup-funding-ireland-covid19-techireland

Enterprise Ireland (2019). 'The European Cybersecurity Market Mapping The Opportunities And Route To Market For Irish SMES'. Available at: https://globalambition.ie/wp-content/uploads/2019/11/The-European-Cybersecurity-Opportunities-for-Irish-SMEs_Key-Takeouts.pdf

Enterprise Ireland (2020). 'In Ireland cybersecurity takes center stage - The Irish Advantage'. Available at:

https://irishadvantage.us/in-ireland-cyber-security-takes-center-stage-us/

Enterprise Ireland (2022). 'Start in Ireland'. Available at: https://www.enterprise-ireland.com/en/startinireland/

Etenders (2022). 'Published tenders'. Available at: https://irl.eu-supply.com/ctm/Supplier/PublicTenders

European Cyber Security Organisation (2021). 'A Taxonomy for the European Cybersecurity Market'. Available at: https://www.ecs-org.eu/documents/publications/605de1e3a768a.pdf

Go Ireland (2022). 'Masters in Cyber Security in Ireland | MS in Cybersecurity in Ireland'. Available at: https://www.goireland.in/cyber-security-course-ireland

Hurley, S., (2021). Ireland should spend '10 times more' on cyber security. Available at: https://www.rte.ie/news/2021/0525/1223759-hse-cyber-attack/

IDA Ireland (2021). 'Why Ireland for Cyber Security'. Available at: https://www.idaireland.com/newsroom/publications/why-ireland-for-cyber-security

Invest in Estonia (2021). 'Estonia – the rise of a cybersecurity giant — Invest in Estonia'. Available at: https://investinestonia.com/estonia-the-rise-of-a-cybersecurity-giant/

ISC2 (2021). 'A Resilient Cybersecurity Profession Charts the Path Forward'. Available at: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

Kesselring, L. (2017). 'Cyber Security Skills Crisis Causing Rapidly Widening Business Problem'. Available at: https://www.prweb.com/releases/2017/11/prweb14899778.htm

Larkin, P. (2018). 'Securing Ireland's digital future A new and expanded national cyber security strategy'.

Northern Ireland Research and Statistics Agency (2019). 'NISRA Statistical Bulletin'. Available at: https://www.nisra.gov.uk/sites/nisra.gov.uk/files/publications/MYE20-Bulletin.pdf

Privacy Solved (2022). 'Cybersecurity: Focus on Ireland's National Cyber Strategy'. Available at: https://www.privacysolved.com/cybersecurity-focus-on-irelands-national-cyber-strategy/

Rialtas na hÉireann (2019). National Cyber Security Strategy 2019-2024. Available at: https://www.skillnetireland.ie/wp-content/uploads/2020/01/National-Cyber-Security-Strategy-2019-2024.pdf

Ruohonen, J. (2020). 'An Acid Test for Europeanization: Public Cyber Security Procurement in the European Union'. Available at: https://www.semanticscholar.org/paper/An-Acid-Test-for-Europeanization%3A-Public-Cyber-in-Ruohonen/f4afbdca627b98bfe279d0d707bed295825736d2

Scale Ireland (2022). 'Promoting Irish Tech Start-ups & Scale-ups '. Available at: https://www.scaleireland.org/

Somers, C. and Byrne, E. (2021) 'Cyber Security Skills Report 2021' Available at: https://cyberireland.ie/wp-content/uploads/2021/02/Cyber-Ireland-Skills-Report-2021.pdf

Statista (2021). 'Israel cybersecurity companies 2011-2020'. Available at: https://www.statista.com/statistics/1003442/israel-cyber-security-companies/#:~:text=This%20statistic%20shows%20the%20number,of%20450%20companies%20in%202018

Stryvesecure (2021) 'How The UK and Ireland Compare When it Comes to Cybersecurity?'. Available at: https://www.stryvesecure.com/blogs/how-the-uk-and-ireland-compare-when-it-comes-to-cybersecurity

TechCentral (2020). Ireland has highest proportion of cyber security leaders globally. Available at: https://www.techcentral.ie/ireland-has-highest-proportion-of-cyber-security-leaders-globally/

Technology Ireland ICT Skillnet (2022). 'Cybersecurity Skills Courses'. Available at: https://www.ictskillnet.ie/cyber-security-skills/

The Cyber Research Databank. (2022). 'USA Cyber Security Companies'. Available at: https://www.cyberdb.co/database/usa/

The Irish Times (2021). 'Ireland must learn lessons from Estonia on cybersecurity'. Available at:

CYBER|IRELAND
IRELAND'S CYBER SECURITY CLUSTER

CYBERSKILLS
BUILDING IRELAND'S CYBER SECURITY SKILLS

Perspective
Economics