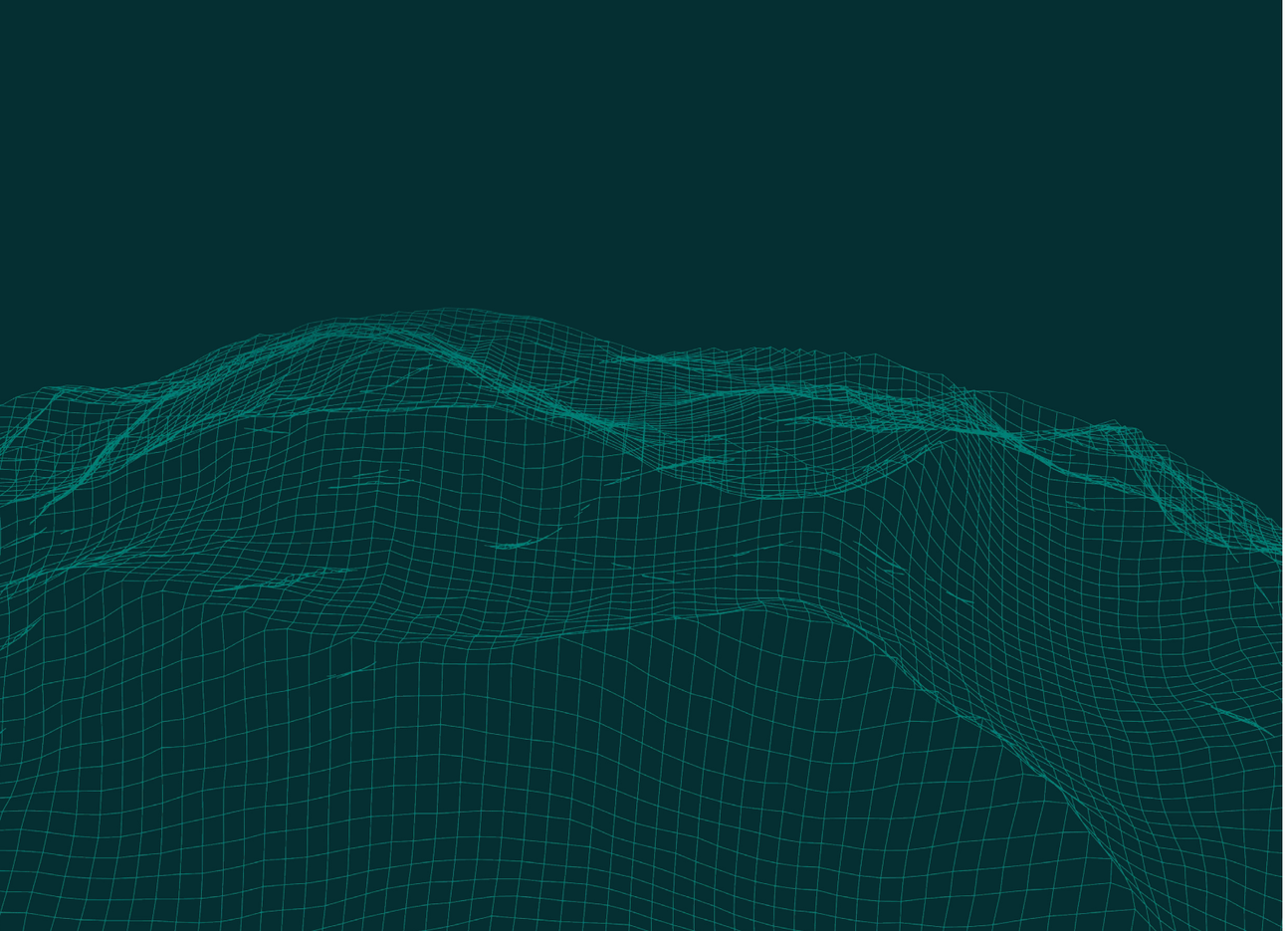
SEPTEMBER 2023

Cyber Ireland

State of the Cyber Security Labour Market in Ireland

Perspective Economics

CYBER|IRELAND
IRELAND'S CYBER SECURITY CLUSTER



Contents

Foreword

On current growth rates of 10% per annum, the cyber security sector workforce in Ireland could add an additional 10,000 jobs by 2030, supporting up to €2.5bn in GVA per annum. To meet this demand, the sector would need to recruit over 1,000 additional workers each year.

In our member survey 2023, 66% of organisations had skills, recruitment or retention issues, making it the top challenge for business for the past 5 years, since Cyber Ireland was established in 2019. If we can address these skills challenges with a coordinated approach across industry, education and government, Ireland can realise its cyber potential.

This report was commissioned by Cyber Ireland and assesses the recent, current, and upcoming demand for cyber security talent in Ireland.

The report provides clear evidence of the increasing demand for cyber security talent in Ireland, outlining how there were three times as many job postings in 2022 compared to 2019 – that's up to 6,707 unique vacancies in the most recent year.

The benefits of growing the sector nationally are also highlighted. The advertised median salary for cyber security professionals is almost double the national median salary, and there is a growing demand for cyber security talent across all Irish regions, which offers significant opportunities for supporting regional employment growth.

In international comparisons, demand for cyber security talent in Ireland makes up a higher proportion of the national job market compared to countries identified in the benchmark exercise. Ireland's cyber security sector also has a higher median advertised cyber security salary than most comparator regions.

This research will support Cyber Ireland and our partners in assessing where labour market demands are greatest. We will continue our work with educators and training providers to ensure that Ireland's pipeline of talent is appropriately trained and capable of meeting the security needs within the private sector, as well as across public services, making Ireland a safe and secure place to live and work online.

Eoin Byrne

DR EOIN BYRNE,
CLUSTER MANAGER, CYBER IRELAND

Executive Summary

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.

Cyber Ireland has commissioned Perspective Economics to undertake a demand mapping exercise of Ireland's cyber security labour market between 2019 and 2022.

To support the analysis of demand and skills, the research team has collaborated with Lightcast, which is an experimental platform that supports the collection and analysis of labour market data. Lightcast provides data on occupations, skills in demand, and career pathways, collected in real-time from over 40,000 sources every day, contributing to a database of over 1 billion global job postings.

This analysis focuses on the c.17,800 job postings between 2019 and 2022 that were related to the cyber security sector in Ireland, with a summary of key insights provided below:

KEY FINDINGS:

PIPELINE AND DEMAND

- The State of the Cyber Security Sector 2022 report identified 7,351 private sector professionals working in the cyber security sector, with the potential for 17,000 private sector jobs by 2030.
- To meet this demand, the sector would need to recruit an additional c.1,000 workers each year.

Number of vacancies

- In 2022, there were 6,707 unique job postings for cyber security professionals in Ireland – demand more than trebling from 2019.

SECTOR SALARY

- Ireland's median cyber security salary for 2022 (€75k) was almost twice the official median salary for Ireland (€41k, 2020).
- Ireland's median cyber security salary has seen yearly growth, increasing 4% from 2021 and 8% from 2020. Salaries are highest in Dublin and the South West.

REGIONAL DEMAND

- All of Ireland's regions have seen a significant increase in cyber security job postings between 2019 and 2022. The regions with the highest demand in 2022 include Dublin (4,396 posts), the South-West (983), the Mid-West (309), and the Mid-East (289).
- The largest net increase in job postings can be seen in Dublin (2,967 jobs), the South West (715 jobs), the South East (255), Mid-West (224), and Mid-East (217), yet relative to their baseline, all regional job postings have increased at a faster rate than Dublin.

SECTORAL DEMAND

- Lightcast suggests that c.34% of all online vacancies are advertised via a third-party recruitment agency.
- Excluding recruiters, sectors with the highest levels of demand include Information Technology sector (17%), the Financial Services sector (16%), and Cyber Security (14%).

JOB ROLES AND TECHNICAL SKILLS

71% of job posts were in one of three categories:

- Cyber security implementers[1] (46% of job roles) handle product development, integration, and maintenance. They need skills in solution integration, security assessment, coding, and communication.
- Cyber incident responders[2] (13%) create and assess Incident Response Plans, handle incidents, manage vulnerabilities, measure response effectiveness, and document actions. Key skills encompass technical handling, threat analysis, system operation, pressure handling, communication, and log analysis.
- Cyber security risk managers [3] (12%) develop risk strategies, manage asset inventory, assess threats, propose risk treatments, monitor controls, and ensure risk levels are acceptable. Skills involve framework implementation, compliance, risk analysis, stakeholder communication, and risk-sharing.

GLOBAL BENCHMARKING

- Cyber security job posts make up 0.8% of all job posts in Ireland, which is a higher proportion of national job posts of any comparator region other than the United States[4]. This suggests that in proportion to the available labour force, Ireland has a significant demand for cyber security skills.
- The cyber security salary premium is also significant in Ireland, behind only the United States and France[5].

FACTORS IMPACTING NATIONAL DEMAND

- The increase in national job vacancies was most notable between 2019 and 2021, slowing in 2022. Stakeholders attribute this slowdown in recruitment to wider market uncertainty and correction for over hiring during the COVID-19 pandemic.
- Businesses in Ireland have paid out ransoms more regularly than other European countries, paying five times or more to recover data[6]. This suggests industry could better incorporate cyber security into their business practices. Growing awareness in this area, and increased regulatory requirements have both been noted as factors contributing to the growing demand for cyber security.
- There is a need to incorporate cyber security practices and improve understanding across wider society. Stakeholders suggest that this should include increased engagement with students in primary and secondary education, and the inclusion of cyber security modules in more general IT courses at the university level, and in courses that will likely lead to employment in sectors that are currently hiring for cyber security roles (e.g. finance).
- Mid to senior level roles have been noted as most in demand by stakeholders, and in demand skills are driven by industry-specific regulation, e.g., OT-specialists as a result of the NIS2 directive, and the role of the Digital Operational Resilience Act (DORA) on the financial services sector.

[1] Alternative job titles for this role include: Information Security Implementer, Cyber security Solutions Expert, Cyber security Developer, Cyber security Engineer, Development, Security & Operations (DevSecOps) Engineer

[2] Alternative job titles for this role include: Cyber Incident Handler, Cyber Crisis Expert, Incident Response Engineer, Security Operations Center (SOC) Analyst, Cyber Fighter /Defender, Security Operation Analyst (SOC Analyst), Cyber security SIEM Manager

[3] Alternative job titles for this role include: Information Security Risk Analyst, Cyber security Risk Assurance Consultant, Cyber security Risk Assessor, Cyber security Impact Analyst, Cyber Risk Manager

[4] Comparator region and proportion of cyber security job posts include: United States (1%), Ireland (0.8%) Germany (0.7%), France (0.6%), UK (0.6%), Netherlands (0.4%), and Poland (4%)

[5] Comparator region salary premiums include: United States (140%), France (138%), Ireland (112%), Poland (84%), UK (66%), and the Netherlands (47%)

[6] Hiscox Group (2022) Cyber Readiness Report. Available at: https://www.hiscoxgroup.com/sites/group/files/documents/2022-05/22054%20-%20Hiscox%20Cyber%20Readiness%20Report%202022-EN_0.pdf

RECOMMENDATIONS

Recommendations developed as a result of this research are grouped across three main themes, outlined below:

UNDERSTANDING THE SKILL PIPELINE

While this study provides an assessment of the current level of demand for cyber security talent, additional research should be undertaken to determine the current skill supply in Ireland. Recommendations relevant to supply-side skills assessment include:

Evaluation of the supply-side skills in Ireland's cyber security market: The cyber security sector study completed in 2022 identified c.7,351 cyber security employees across 489 organisations in Ireland. Further research to identify what skills are readily available in the labour market, and where the perceived shortfall exists will support Cyber Ireland and its partners' understanding of the market, to be used to inform the development of existing and future training and education schemes.

Assess the applicability of the ENISA's European Cybersecurity Skills Framework to Ireland's private sector and education market: This research has used the ECSF skills profiles to classify job postings. The ECSF has been developed to establish a common terminology for the cyber security sector within the EU. Future research should assess the applicability of the ECSF in Ireland's market context, alongside its alternatives, e.g., the NICE Framework. The incorporation of existing frameworks into sector planning will support skill tracking and policy design.

Assess cyber security regulatory requirements and what this means for future skills demand: Stakeholders have noted how regulation is a significant driver for cyber security employment. Cyber Ireland should work collaboratively with industry and Government to identify the current and future regulatory requirements likely to influence demand for cyber security talent. This includes, e.g., demand brought on by NIS2, CRA, and DORA. This can help inform future workforce planning, and potentially support the development of entry-level pathways such as cyber security apprenticeships focused on areas such as OT and regulatory compliance.

SUPPORTING EDUCATION & SKILL DEVELOPMENT

Evaluation of education and training pathways to determine entry-level competencies: Cyber Ireland have identified 69 cyber security courses in Ireland. Future research that explores the volume of students completing these courses, the competencies they develop, and their career progression will present a clear picture of Ireland's cyber security talent pipeline and the entry-level skillsets available to the market. It will also support Cyber Ireland and partners in assessing to what extent available courses are meeting the current skills demand in the market.

Source: Cyber Ireland Business Survey

Increase awareness and education at primary and post primary level through a nationally funded, coordinated scheme: Cyber Ireland should continue to work collaboratively with Government to develop a national scheme to facilitate sectoral awareness among young people. This scheme should build on and incorporate learning from smaller scale schemes that have previously been active in Ireland, e.g., Cyberwise, CyberFutures and Schools Capture The Flag (CTF) Events.

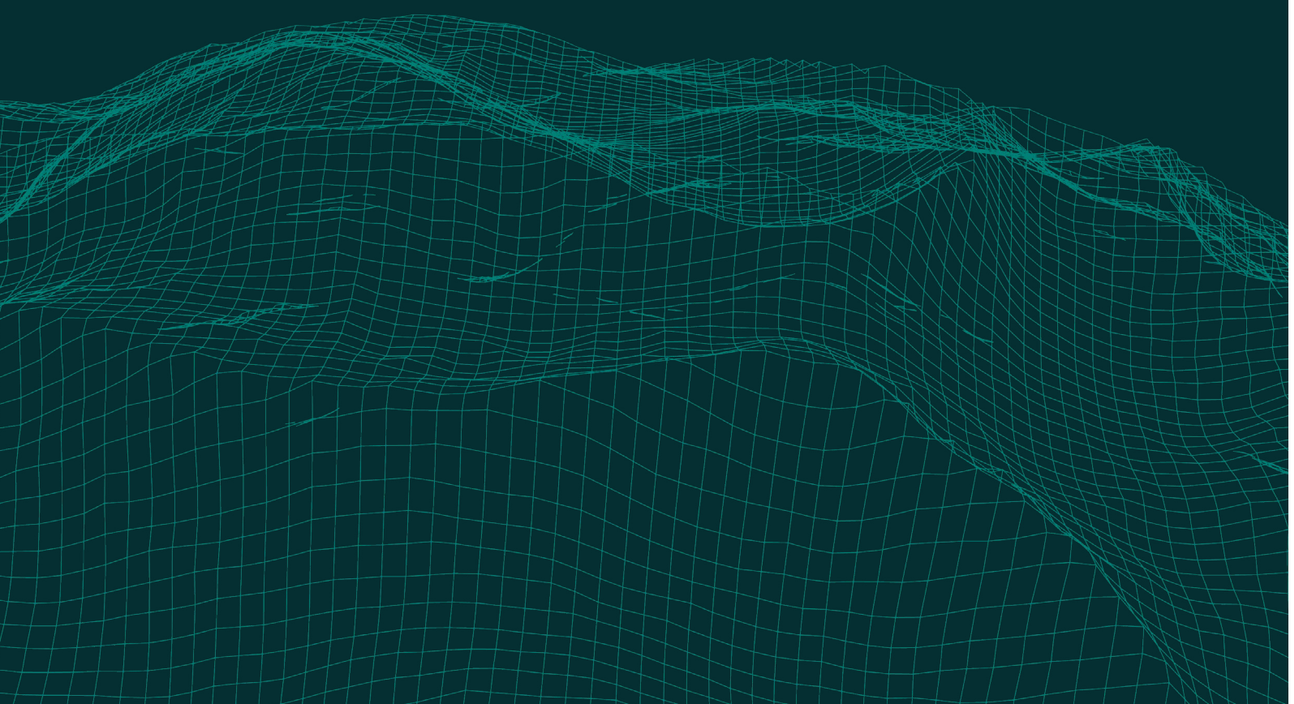
SUPPORTING CYBER SECURITY RESILIENCE WITHIN THE PRIVATE SECTOR

Establish a baseline security standard for cyber security practice through certification: While available literature suggests that businesses are becoming more aware of the risks associated with poor cyber security measures, the adoption of certification, similar to the UK's Cyber Essentials Certification, will have significant impact on the cyber security resilience of Ireland's private sector, also creating further opportunities to support entry-level employment.. This could also be embedded within public procurement processes to ensure private contractors are meeting minimum cyber security standards.

Schemes to support cyber security employment in strategic sectors: Cyber Ireland should engage with recruiting firms within strategic sectors (e.g., IT and finance) to identify skills demand and to establish career development pathways. This could include upskilling and transition of existing staff with similar skillsets into cyber security roles. Examples of similar schemes include the UK's Department for Science, Innovation and Technology's Upskill in Cyber programme, delivered in partnership with the SANS Institute.

01
Introduction

This section of the report provides a context to the current study, including an overview of Cyber Ireland, the study background, and the research objectives.



1.1 INTRODUCTION TO CYBER IRELAND

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.

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 also the industry partner to the Higher Education Authority funded initiative Cyber Skills, a government-backed initiative designed to address skill shortages in the cyber security sector.

1.2 STUDY BACKGROUND

Cyber Ireland's Cyber Security Skills Report (2021) highlights how many of its members consider recruitment and retention as their main obstacle for growth. The Cyber Security Skills Report suggests that 48% of firms have open but unfilled roles, 46% of security teams feel understaffed, and 20% of roles take more thansix months to fill.

Where skills gaps or shortages persist, there are a wide range of implications that can be damaging to the economy and society. As such, there is a need to understand the demand shown for cyber security professionals across Ireland's economy to gauge what extent of intervention may be required with respect to skills, retraining, and attracting people to work in the sector.

1.3 NUMBER OF EMPLOYEES IN THE CYBER SECURITY SECTOR

The State of the Cyber Security Sector 2022 report identified 7,351 private sector professionals working in the cyber security sector, with the potential for 17,000 private sector jobs by 2030.

Large organisations (250+ employees) account for most cyber security related employment (5,304, 72%), however approximately two-thirds (65%) of cyber security teams are small, consisting of between one to nine cyber security professionals. A further 27% of firms employ between 10 - 49 cyber security professionals and only 8% of firms have a team of 50+ cyber security professionals (typically dedicated practices).

Foreign-owned firms play a significant role in growing the sector. US-headquartered firms support 55% of all cyber security related employment - compared to domestic firms, which support 29% of employment.

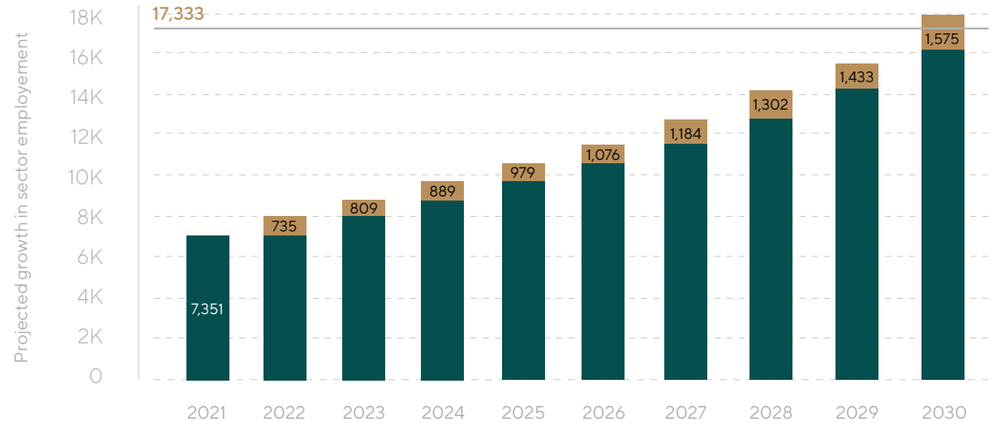
The sector report also found that 83% of businesses expect that their cyber security team will grow over the next twelve months (between 2022 and 2023), and more than half (51%) expect that this growth will occur at a rate of 25% or higher.

The availability of skills is however a significant factor influencing sector growth, with 61% of respondents noting 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%).

1.4 PROJECTED DEMAND BY 2030

The potential for growth in Ireland's cyber security sector is estimated at c.10% per annum. This would suggest that cyber security employment in Ireland could increase from 7,351 employees in 2021 up to 17,333 in 2030. Projected yearly growth is outlined in the figure on the next page:

FIGURE 1.1 PROJECTED YEARLY GROWTH OF IRELAND'S CYBER SECURITY SECTOR (2021 - 2030)



Source: Cyber Ireland, State of Cyber Security Sector in Ireland (2021)

The projected market growth will have implications on the demand for cyber security talent in Ireland, suggesting that an additional net 1,000 people per annum will need to be trained, upskilled, or recruited into the sector to meet demand in the coming years.

RESEARCH OBJECTIVES

To support Ireland's growth potential, Cyber Ireland has commissioned Perspective Economics to undertake a demand mapping exercise of Ireland's cyber security labour market between 2019 and 2022. This analysis will support Cyber Ireland in their efforts to understand where demand is coming from, for what roles, and in what regions. Specifically, the evidence gathered through this research exercise assesses:

- Annual number of unique cyber security job postings in Ireland;
- Job roles included in job postings;
- Advertised salary attached to each job post;
- Variation in job postings across the different regions in Ireland; and
- How Ireland compares to other countries with regards to cyber security recruitment.

1.5 SUMMARY OF METHODOLOGY

The methodology for this demand mapping exercise consists of three main strands, each of which are outlined in the visual below:

FIGURE 1.2 STUDY METHODOLOGY

Desk Review	A rapid desk review of Cyber Ireland skills studies and other available literature to: • Identify gaps in knowledge and supporting evidence. • Support Cyber security role classification.
Recruitment Data Analysis	Granular Analysis of two data sources provided by global recruitment data provider Lightcast, including: • An export of 10,832 job postings between 2019 and 2022; and • Access to the online data platform Lightcast Spotlight to support global analysis.
Qualitative Engagement	Stakeholder interviews with cyber security organisations and recruitment agencies to address key themes, e.g., the cyber security skills gap, candidate skill level, career progression, and pathways to cyber security.

Source: Perspective Economics

1.6 RESEARCH CAVEATS AND INTERPRETATION OF DATA

In Ireland, there is currently no official statistical analysis available that provides an appropriate level of detail on the cyber security labour market. To support the analysis of demand and skills, the research team has collaborated with Lightcast, which is a leading platform in the collection and analysis of information on the labour market. Lightcast provides data on occupations, skills in demand, and career pathways, collected in real-time from over 40,000 sources every day, contributing to a database with over 1 billion job postings and billions of other data points.

Lightcast has provided the research team with access to two data sources, each offering insight into different aspects of Ireland's cyber security labour market:

LIGHTCAST SPOTLIGHT PLATFORM	EXTRACT OF JOB POSTINGS
Lightcast Spotlight is an experimental online platform that allows users to compare global job markets. Variables available through Lightcast Spotlight include: • Number of job postings • Date of job posting • Advertised salary • Top recruiters • Regional recruitment (NUTS 3-level)	Lightcast also provided an in-depth export of 10,832 unique job postings covering 2019 – 2022. Key metrics available in this dataset include: • Job title • ENISA ECSF classification • Date of job posting • Requested level of experience • Skillset required.

Source: Lightcast, Perspective Economics

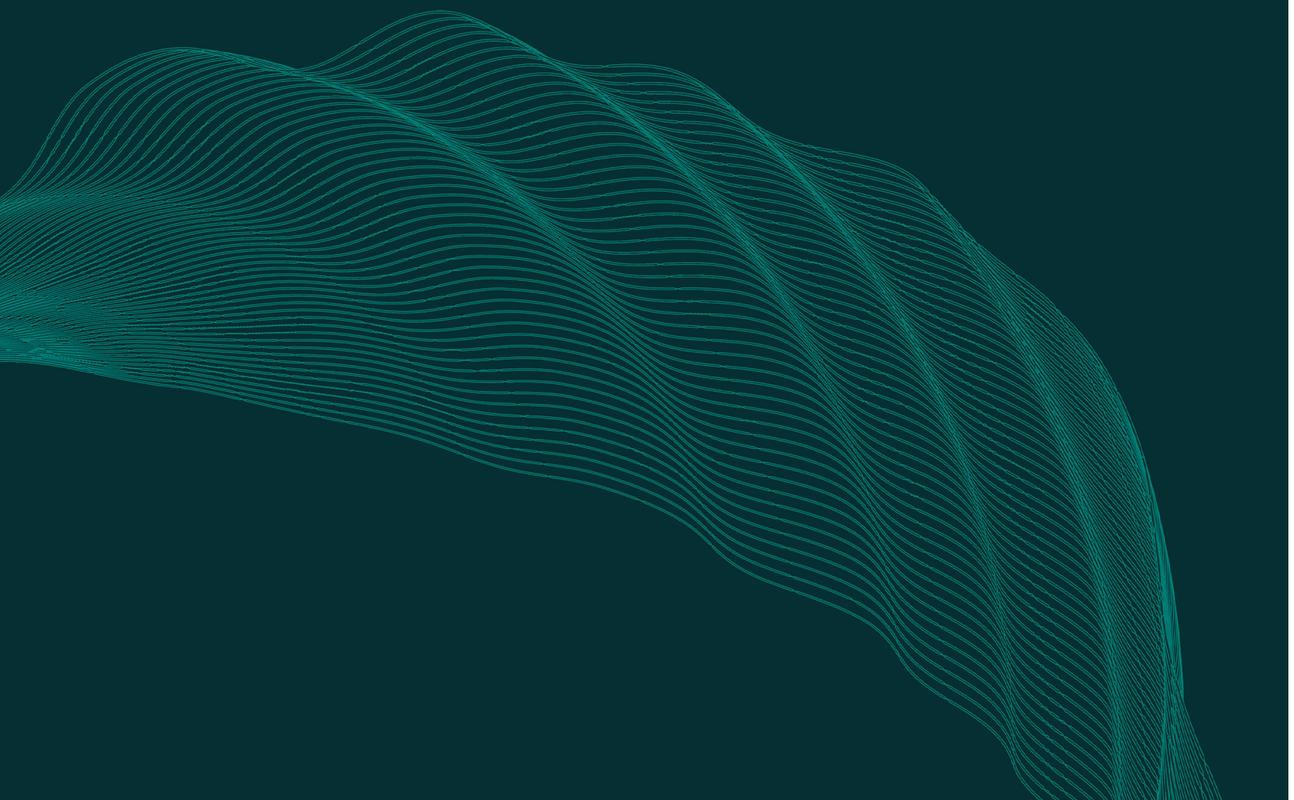
It is important to note that this analysis is **experimental in nature and is an interpretation of available recruitment activity in Ireland.** To ensure accuracy within our analysis we have engaged with eight strategic stakeholders, including a subset of recruiters and cyber security businesses, and Government departments. The quantitative analysis conducted has been tested with stakeholders, and the testimonies provided used to enrich our analysis and to provide context on labour market trends.

1.7 ACKNOWLEDGEMENTS

The research team would like to acknowledge each of the stakeholders that contributed to this study, Lightcast for their provision of recruitment data, and Cyber Ireland for the support provided throughout.

02
Cyber security job vacancies

This section of the report outlines headline recruitment statistics relating to number of job postings, advertised median salary, and regional and sectoral variations. Please note that this section assesses historic performance only, with interpretation of future market trends presented in section 5.



2.1 NUMBER OF JOB VACANCIES

The Lightcast Spotlight platform suggests that there is a growing demand for cyber security professionals in Ireland, aligned to previous studies in the area, e.g., Indeed's Global Cyber Security Outlook [7] and the ISC2 Cyber security Workforce Study [8].

Globally, the Lightcast Spotlight platform suggests that cyber security job postings has more than doubled (2.5 times increase, from 494k posts in 2019 up to 1.23m posts in 2022).

In Ireland, the number of job postings has more than trebled, from 2,004 in 2019 up to 6,707 in 2022. The yearly number of job postings are outlined in the table below, suggesting that the greatest increase in yearly postings occurred between 2019 and 2020, and 2020 and 2021.

TABLE 2:1 NUMBER OF UNIQUE JOB POSTINGS (2019 – 2022)

YEAR	NUMBER OF UNIQUE POSTINGS
2019	2,004
2020	3,322 (+66%)
2021	5,786 (+74%)
2022	6,707 (+15%)

Source: Lightcast Spotlight

Recruitment data available through Lightcast suggests that the demand for cyber security roles in Ireland is increasing at a faster rate than the global figure. The United States' International Trade Administration[9] highlights several of the key factors driving demand in Ireland, including, e.g., an increase in economic crime and fraud in Ireland, Government efforts to increase national cyber resilience and awareness within the private sector, alongside additional demand due to an increase in remote working and digitisation of services.

> *"With so many types and varieties of roles under the Cyber Security umbrella, the demand is ever growing."*
>
> DIVERSIFIED COMPANY WITH A CYBER SECURITY TEAM

[7] Indeed (2019) Global cybersecurity outlook. Available at: https://www.indeed.com/lead/cybersecurity-outlook-2019

[8] ISC2 (2022) 2022 Cybersecurity workforce study. Available at: https://www.isc2.org/Research/Workforce-Study omparator region and proportion of cyber security job posts include: United States (1%), Ireland (0.8%) Germany (0.7%), France (0.6%), UK (0.6%), Netherlands (0.4%), and Poland (4%)

[9] International Trade Administration (2022) Ireland – Country Commercial Guide. Available at: https://www.trade.gov/country-commercial-guides/ireland-cybersecurity

2.2 CYBER SECURITY SALARIES

Lightcast Spotlight suggests that the advertised median cyber security salary in 2022 was €75k, which is aligned to figures presented in previous research undertaken by Cyber Ireland[10] . Lightcast Spotlight also suggests that the median advertised cyber security salary is increasing, up 4% from 2021, and 8% from 2020, suggesting that the profession is creating increasingly high value jobs.

The sector also has a significant salary premium when assessed against the national median wage and is almost double (+ 80%).

The most recently available national median salary is c.€41k[11] , and as reflected by stakeholders this is typically the baseline salary for new entrants into the sector:

> *"Cyber security salaries start in the early forties and can go anywhere upwards. It's like asking how long a piece of string is."*
>
> PROVIDER OF CYBER SECURITY SERVICES

2.3 GEOGRAPHIC VARIATION

The Lightcast Spotlight platform supports analysis of regional job postings at the NUTS 3-level. NUTS 3 boundaries are visualised in the adjacent figure, which also outlines total job postings associated with each region for the year 2022.

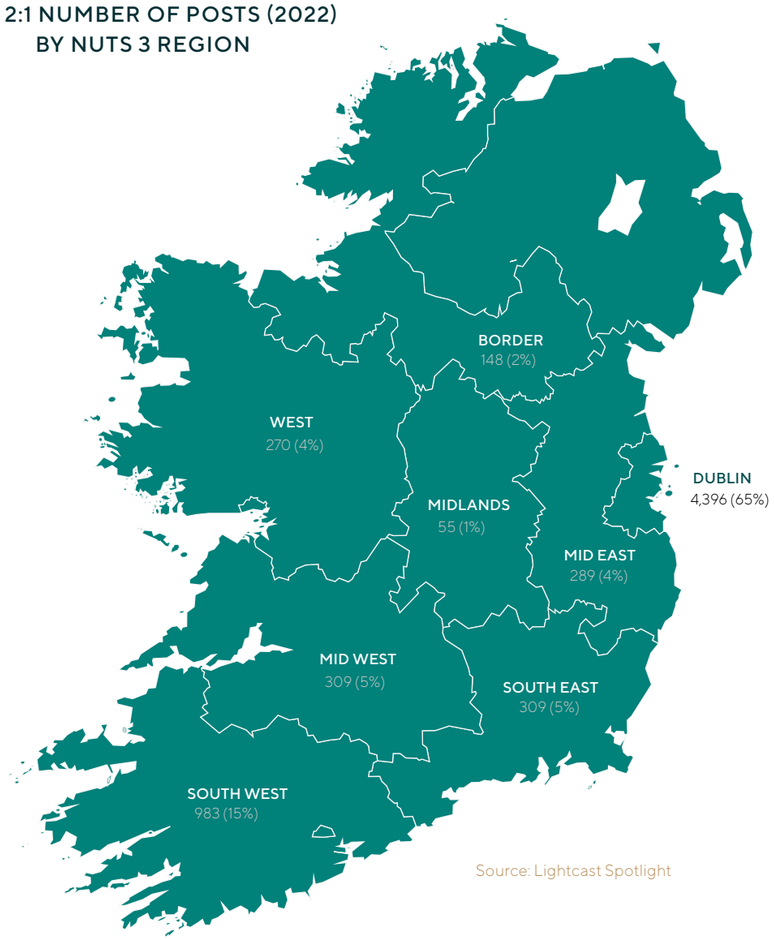
[10] Cyber Ireland (2022) State of the Cyber Security Sector in Ireland. Available at: https://cyberireland.ie/wp-content/uploads/2022/05/State-of-the-Cyber-Security-Sector-in-Ireland-2022-Report.pdf

[11] Central Statistics Office (2020) Earnings Analysis using Administrative Data Sources 2020. Available at: https://www.cso.ie/en/releasesandpublications/ep/p-eaads/earningsanalysisusingadministrativedatasources2020/annualearnings/

Counties included within each NUTS 3 region are as follows:

- Dublin - Dublin
- South - West - Kerry, Cork
- Mid-East - Kildare, Meath, Wicklow, Louth
- Mid-West - Clare, Tipperary, Limerick
- South-East - Carlow, Kilkenny, Wexford, Waterford
- West - Mayo, Roscommon, Galway
- Border - Cavan, Donegal, Leitrim, Monaghan, Sligo
- Midlands - Laois, Longford, Offaly, Westmeath

FIGURE 2:1 NUMBER OF POSTS (2022) BY NUTS 3 REGION



Source: Lightcast Spotlight

Further analysis for each region is outlined in the table below. This analysis suggests that all of Ireland's regions have seen a significant increase in cyber security job postings between 2019 and 2022.

The largest net increase in job postings can be seen in Dublin (2,967 jobs), the South West (715 jobs), the South East (255), Mid-West (224), and Mid-East (217).

This analysis is aligned to the State of the Cyber Security Sector 2022[12] report which identified four concentrated clusters of cyber security businesses in the counties Dublin, Cork, Limerick, and Galway.

Please note that while Dublin has seen the largest net growth in cyber security talent, all other regions have seen a greater increase relative to their baseline, this is indicative of the growing demand for cyber security talent across Ireland.

The analysis also suggests that Dublin and the South West have higher salaries than other regions. This is likely linked with the level of foreign direct investment (FDI) in each region, which typically also brings higher paid jobs.

TABLE 2:2 NUTS 3 SUMMARY TABLE

REGION	REGION POPULATION (2022)	MEDIAN ADVERTISED SALARY (2022)	NUMBER OF JOB POSTINGS (2019)	NUMBER OF JOB POSTINGS (2022)	INCREASE 2019-2022	% OF TOTAL JOBS (2022)[13]	JOB POSTINGS (2022) RELATIVE TO POPULATION
Dublin	1,450,701	€82.7K (n=955)	1,429	4,396	207%	66%	0.3%
South-West	736,489	€67.1K (n=133)	268	983	266%	15%	0.1%
Mid-West	500,524	€59.6K (n=57)	85	309	263%	5%	0.06%
Mid-East	761,858	€61.4K (n=51)	72	289	301%	4%	0.03%
West	483,677	€56.8K (n=56)	58	270	366%	4%	0.06%
South-East	456,228	€56.8K (n=30)	54	309	471%	5%	0.07%
Border	417,260	€56.8K (n=21)	39	148	280%	2%	0.04%
Midlands	316,799	€41.8K (n=18)	2	55	2650%	1%	0.02%
TOTAL	**5,123,536**	**€74.9k (n=1,323)**	**2,004**	**6,707**	**235%**	**-**	**0.1%**

Source: Lightcast Spotlight

[12] Cyber Ireland (2022) State of the Cyber Security Sector in Ireland. Available at: https://cyberireland.ie/wp-content/uploads/2022/05/State-of-the-Cyber-Security-Sector-in-Ireland-2022-Report.pdf

[13] Please note that this figure uses total national posted jobs (6,707) as its denominator. Regional postings total 6,759. It is assumed that this disparity is due to some job postings offering the same role across different regions in Ireland.

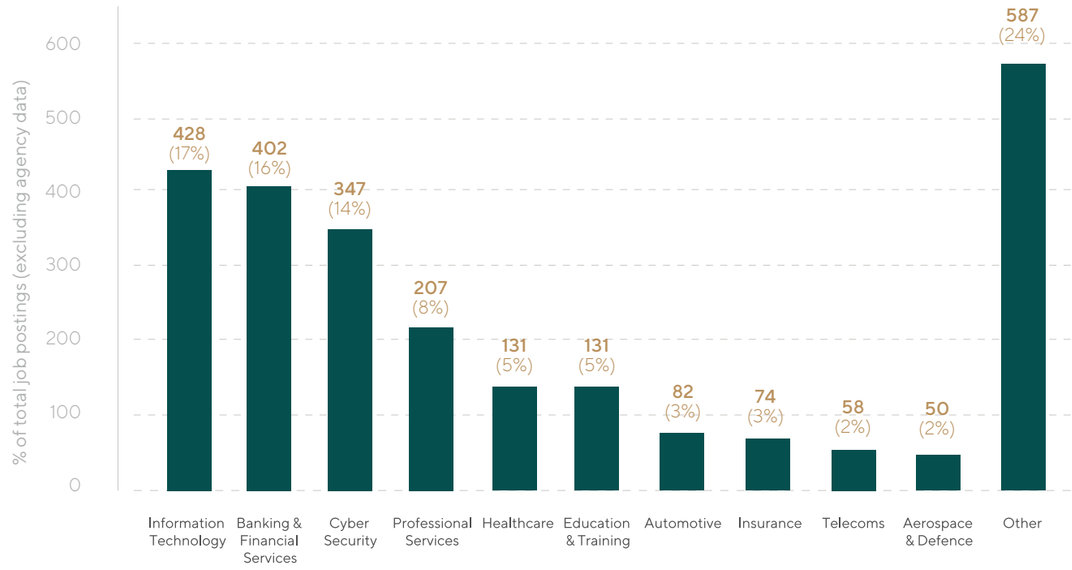
2.4 SECTORAL DEMAND FOR CYBER SECURITY STAFF

To understand which sectors have the highest demand for cyber security services, the research team have reviewed and classified recruiting firms into 12 sector groups.

This analysis suggests that in 2022, c.34% (n=1,265 job postings) of all recruitment was through a recruitment agency, with the remaining 66% of job postings coming from one of the other eleven sector groups.

An analysis of recruiting sectors (excluding recruitment agencies) is presented below.
Please note that this analysis uses the data export provided by Lightcast, and focuses on recruitment activity in 2022 only:

FIGURE 2:2 SECTOR OF RECRUITING FIRM (2022)



Source: Lightcast data export (2022)

The analysis of Lightcast data for 2022 suggests that 17% of recruitment is being undertaken by firms in the Information Technology sector, 16% in the Banking and Financial Services sector. A further 14% was undertaken directly by firms dedicated to the provision of cyber security services, and 8% by professional service providers.

This analysis is in line with identified market trends:

> *"Historically we work with a lot of finance organisations and the big four."*
>
> **RECRUITMENT FIRM**
>
> *"The life sciences, public healthcare and financial services sectors also represent strong end-user sub-segments for the cyber security sector in Ireland."*
>
> **INTERNATIONAL TRADE ADMINISTRATION**
>
> *"The banking sector has experienced a significant increase in demand for technology professionals due to demand in cyber security and a need for further upgrading of software applications."*
>
> **MORGAN MCKINLEY EMPLOYMENT MONITOR[14]**

2.4.1 FACTORS DRIVING SECTORAL DEMAND OF CYBER SECURITY STAFF

Government and industry regulation has been noted as a key driver for cyber security demand[15], with both available literature[16] and stakeholders noting how this is influencing specific sectors, e.g., finance. Stakeholders suggest that this regulation is driving demand for cyber security talent, and is a factor in protecting the cyber security sector from the wider uncertainty faced by the tech sector:

[14] Morgan McKinley (2023) Employment Monitor Q2 2023. Available at: https://d2gkwf0gauw8z0.cloudfront.net/sites/default/files/2023-07/8346-MMK-IE-JL_Ireland-Employment-Monitor_Q2-2023.pdf

[15] Cybersecurity and Infrastructure Security Agency (2018) Cybersecurity Careers of the Future. Available at: https://niccs.cisa.gov/sites/default/files/documents/pdf/cybersecurity%20careers%20of%20the%20future.pdf?trackDocs=cybersecurity%20careers%20of%20the%20future.pdf

[16] Carnegie Endowment for International Peace (2021) The European Union, Cybersecurity, and the Financial Sector: A Primer. Available at: https://carnegieendowment.org/files/Krueger_Brauchle_Cybersecurity_legislation.pdf

> *"Large financial services are facing increased regulatory and audit scrutiny."*
>
> **DIVERSIFIED COMPANY WITH A CYBER SECURITY TEAM**
>
> *"We're not seeing cyber security as an area targeted [for redundancies within the wider tech sector], and this is likely due to increased regulatory demand."*
>
> **PROVIDER OF CYBER SECURITY SERVICES**

Other factors as to why financial firms are recruiting for cyber security experts are outlined by the United States' International Trade Administration, which highlights Ireland's growing digital economy and the increase in economic crime and fraud as a factor driving recruitment:

> *"Cybercrime is considered the most disruptive economic crime facing the business community... With its large $50bn digital economy, Ireland is increasingly encountering cyber security threats... Cybercrime remains the most prevalent type of fraud committed in Ireland and is three times more disruptive than the global norm."*
>
> **UNITED STATES' INTERNATIONAL TRADE ADMINISTRATION**

03
Cyber security roles, skills, and certifications

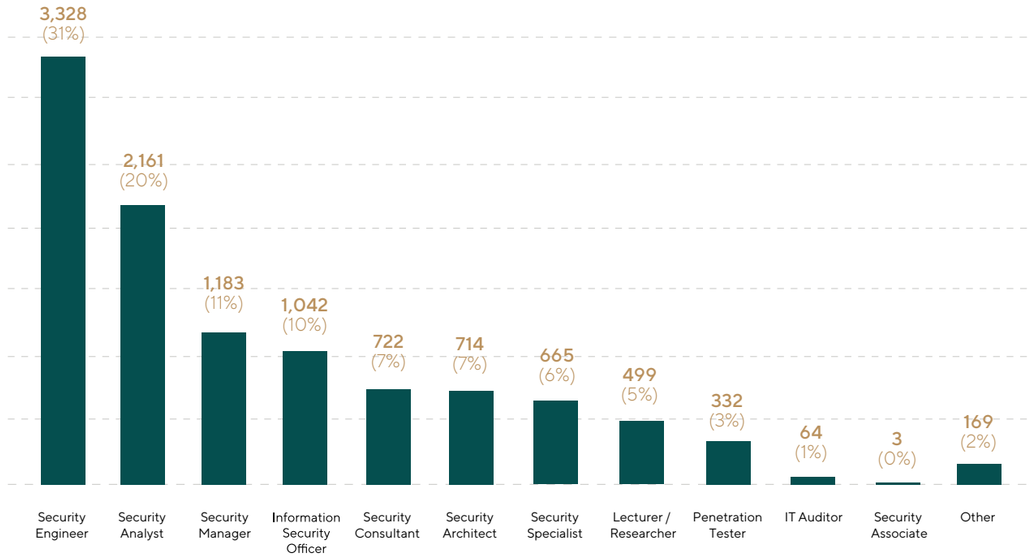
This section of the report provides an overview of the key roles included in job postings, and the skills associated with the top three roles. This analysis draws primarily from the data extract of 10,832 jobs provided by Lightcast, and the European Union Agency for Cyber Security's (ENISA) European Cyber Security Framework (ECSF). Please note, as with the section above, an analysis of trends and emerging demand is presented in Section 5 of this report.

3.1 ADVERTISED JOB ROLES

The analysis below provides an outline of advertised roles identified by Lightcast. Please note that the research team has undertaken some additional cleaning and classification of this data to support analysis.

The figure below provides an overview of job roles advertised between 2019 and 2022.

FIGURE 3:1 JOB PROFILE CLASSIFICATIONS



Source: Lightcast data extract (n=10,882)

This data suggests that nearly two-thirds of all advertised job roles were for the top three categories, security engineer (31%), security analyst (20%), or security managers roles (11%). This is aligned to demand in the UK market [17], which also suggests that these three roles accounted for 67% of all job posts between January and December 2021.

[17] Department for Digital, Culture, Media, and Sport (2022) Cyber security skills in the UK labour market 2022. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1072767/Cyber_security_skills_in_the_UK_labour_market_2022_-_findings_report.pdf .

This analysis also aligns to Morgan McKinley's Employment Monitor for quarter 2, 2023[18] :

> *"Cybersecurity Engineers continue to be in high demand due to the increasing importance of protecting digital assets."*
>
> **MORGAN MCKINLEY EMPLOYMENT MONITOR**

Demand for engineer and analyst roles is likely linked to the existing demand for technical cyber security staff in Ireland, whereas the high percentage of security manager roles is likely reflective of companies recruiting for leadership roles within their cyber security teams. The figure above is aligned to the perspective of sector stakeholders who note:

> *"We see the main shortage is for engineering roles."*
>
> **PROVIDER OF CYBER SECURITY SERVICES**

> *"Most common roles would be Security Operation Center (SOC) Analysts and Information Security Analysts."*
>
> **DIVERSIFIED COMPANY WITH A CYBER SECURITY TEAM**

> *"Finding people for project management roles is hard, there's low numbers."*
>
> **PROVIDER OF CYBER SECURITY SERVICES**

Source: Cyber Ireland, Perspective Economics

[18] Morgan McKinley (2023) Employment Monitor Q2 2023. Available at: https://d2gkwf0gauw8z0.cloudfront.net/sites/default/files/2023-07/8346-MMK-IE-JL_Ireland-Employment-Monitor_Q2-2023.pdf

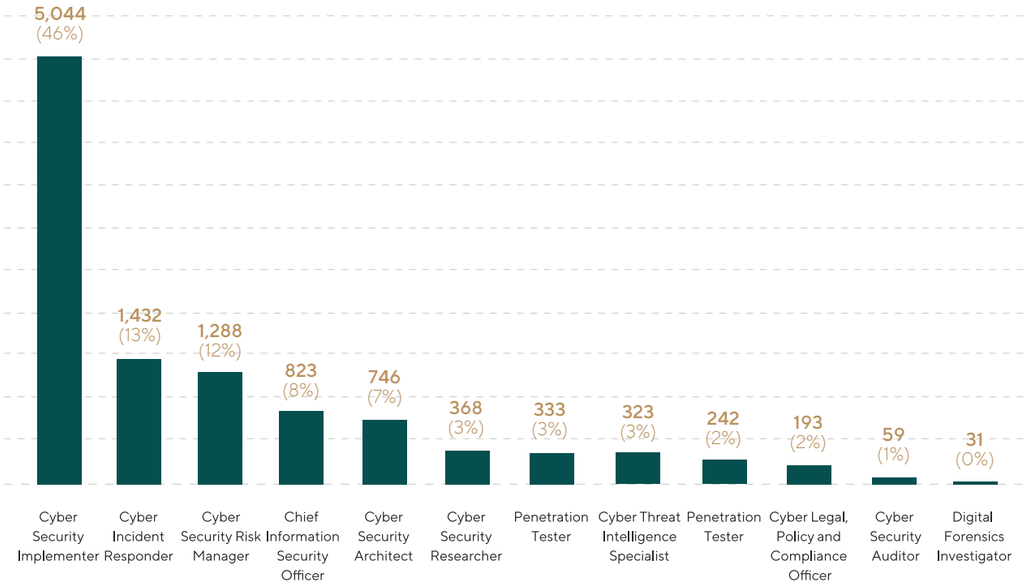
3.2 TECHNICAL SKILLS IN DEMAND

The research team has undertaken further classification of job roles against ENISA's European Cyber Security Framework (ECSF) to determine the key skillset associated with in demand cyber security roles.

The ECSF is a result of work conducted by ENISA's Ad-Hoc Working Group on the European Cyber Security Skills Framework, which is made up of experts representing various views.

The developed framework combines insight from existing frameworks, market research, and expert insight, offering a standardised terminology that aims to bridge the gap between the cyber security professional workplaces and the learning environment[19]. The summary below presents Lightcast job roles classified against ECSF categories:

FIGURE 3:2 ECSF JOB PROFILE CLASSIFICATIONS



Source: Lightcast data extract, ECSF

[19] ENISA (2022) European Cyber security Skills Framework (ECSF). Available at: https://www.enisa.europa.eu/topics/education/european-cyber security-skills-framework

This analysis suggests that cyber security implementer is the most sought-after job role, included in 46% of all job postings since 2019. This is followed by cyber incident responder (13%), and cyber risk manager (12%). Collectively, these roles account for 71% of all job postings. This highlights that while there is a growing demand for cyber security staff in general, a concentrated effort to meet the skill needs within these three roles will likely have significant impact on growing the sector nationally.

The main tasks, skills, and competencies associated with the three most common ECSF job roles are outlined below, in more detail in the appendix, and in full here.

Please note, that while the analysis provided by Lightcast has classified jobs roles against the ECSF, alternative frameworks[20] such as the NICE Framework are also commonly used.

The applicability of both frameworks to Ireland's cyber security market should be considered in future research designed to explore labour market competencies.

3.2.1 SKILLS PROFILE: CYBER SECURITY IMPLEMENTER

The cyber security implementer[21] typically has several responsibilities including the development, implementation, and maintenance of cyber security products; support to product users and customers; the configuration and reporting relating to systems, services, and products; and close collaboration with wider IT and OT personnel on cyber security-related issues.

Key skills associated with this role include the ability to integrate cyber security solutions into an organisation's infrastructure and the configuration of solutions in accordance with an organisation's security policy; the ability to assess the security and performance of solutions; and the ability to develop code, scripts, and programmes. Identified soft skills include ability to communicate, present and report to relevant stakeholders, and collaboration with other team members and colleagues.

3.2.2 SKILLS PROFILE: CYBER INCIDENT RESPONDER

The main tasks associated with the cyber incident responder[22] role includes the development, maintenance and assessment of an Incident Response Plan; the development, implementation and assessment of procedures related to incident handling; the identification, analysis, mitigation and communication of cyber security incidents; the assessment and management of technical vulnerabilities; the measurement of cyber security incidents detection and response effectiveness; the evaluation of the resilience of the cyber security controls and mitigation actions taken after a cyber security or data breach incident; the adoption and development of incident handling testing techniques; the ability to establish procedures for incident results analysis and incident handling reporting; and document incident results analysis and incident handling actions. Identified soft skills include cooperation with Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs), and cooperation with key personnel for reporting of security incidents according to applicable legal frameworks.

Key technical skills include the ability to practice all technical, functional, and operational aspects of cyber security incident handling and response; to collect, analyse and correlate cyber threat information originating from multiple sources; to work on operating systems, servers, clouds, and relevant infrastructures; to work under pressure; to communicate, present and report to relevant stakeholders; and to manage and analyse log files.

[20] National Institute of Standards and Technology (2023) NICE Framework Competency Areas: Introduction and Proposed List. Available at: https://www.nist.gov/system/files/documents/2023/06/14/NICEFramework_CompetencyAreas_List.pdf[21] Alternative job titles for this role include: Information Security Risk Analyst, Cyber security Risk Assurance Consultant, Cyber security Risk Assessor, Cyber security Impact Analyst, Cyber Risk Manager

[21] Alternative job titles for this role include: Information Security Implementer, Cyber security Solutions Expert, Cyber security Developer, Cyber security Engineer, Development, Security & Operations (DevSecOps) Engineer

[22] Alternative job titles for this role include: Cyber Incident Handler, Cyber Crisis Expert, Incident Response Engineer, Security Operations Center (SOC) Analyst, Cyber Fighter /Defender, Security Operation Analyst (SOC Analyst), Cyber security SIEM Manager

> *"Incident handling is always a key skill to have and will be a huge factor for hiring."*
>
> DIVERSIFIED COMPANY WITH A CYBER SECURITY TEAM

3.2.3 SKILLS PROFILE: CYBER SECURITY RISK MANAGER

The main tasks of a cyber security risk manager[23] include the: development of an organisation's cyber security risk management strategy; management of an inventory of organisation's assets; identification and assessment of cyber security-related threats and vulnerabilities of ICT systems; identification of threat landscape including attackers' profiles and estimation of attacks' potential; assessment of cyber security risks and the ability to propose the most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy; monitoring of effectiveness of cyber security controls and risk levels; ensuring that all cyber security risks remain at an acceptable level for the organisation's assets; and development, maintenance, reporting, and communication of the complete risk management cycle.

Key skills associated with the role include the ability to: implement cyber security risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards; analyse and consolidate organisation's quality and risk management practices; enable business assets owners, executives and other stakeholders to make risk informed decisions to manage and mitigate risks; build a cyber security risk-aware environment; communicate, present and report to relevant stakeholders; and propose and manage risk-sharing options.

[23] Alternative job titles for this role include: Information Security Risk Analyst, Cyber security Risk Assurance Consultant, Cyber security Risk Assessor, Cyber security Impact Analyst, Cyber Risk Manager

3.3 CYBER SECURITY SKILL DEVELOPMENT STRATEGY IN IRELAND

Ireland's National Cyber Security Strategy[24] was published in December 2019 and includes a wide range of objectives designed to increase resilience, to improve the national response to cyber security threats, to improve national infrastructure, and to increase international collaboration. The importance of skill development within the sector is noted by stakeholders:

> *"The NCSC published their mid-term review [of the National Cyber Security Strategy] in June, within which skills was identified as a key ask within the sector. "*
>
> GOVERNMENT REPRESENTATIVE

The National Cyber Security Strategy's mid-term review[25] offers insight into key measures undertaken, or in development, to support the skill's pipeline in Ireland:

- Continued development and deployment of second and third level training in computer science and cyber security, supporting the work of Skillnets Ireland in developing training programmes for all educational levels and supporting SOLAS initiatives for ICT apprenticeship programmes in cyber security.
- Science Foundation Ireland's (SFI) promotion of cyber security as a career option in schools and colleges by means of their Smart Futures Programme.
- Science Foundation Ireland, Department of Business, Enterprise, and Innovation (DBEI) and Department of the Environment, Climate, and Communications (DCCAE) to explore the feasibility through the SFI Research Centre Programme, the Research Centre Spoke programme or other enterprise partnership programmes to fund a significant initiative in Cyber Security Research.
- The ongoing development of a centralised repository of educational and apprenticeship courses in cybersecurity at all levels and throughout the country, and use of this data to develop materials for schools, guidance counsellors and others to raise awareness of careers in cyber security and learning pathways.

[24] National Cyber Security Centre (2019) National Cyber Security Strategy. Available at: https://www.ncsc.gov.ie/strategy/

[25] Department of the Environment Climate and Communications (2023) National Cyber Security Strategy 2019-2024 Mid-Term Review. Available at: https://www.gov.ie/pdf/?file=https://assets.gov.ie/261971/356d743c-b154-4a5f-b7ae-eb6714c2d011.pdf#page=null

- Market analysis for cyber skills to better understand supply and demand, the effectiveness of current interventions and priorities for future policy and strategy.
- The development of the Irish cyber security research community to develop its capacity with a view to delivering a significant initiative in Cyber Security Research.

> *"While considerable progress has been made since 2019, stakeholders highlighted challenges with hiring and retaining staff with critical skill sets... The Measures will build upon the existing collaborative relationships between the NCSC, Department of Education, Department of Further and Higher Education, Research, Innovation and Skills, Science Foundation Ireland, Technology Ireland ICT Skillnets, SOLAS, Cyber Ireland, and the educational and research institutions."*
>
> NATIONAL CYBER SECURITY STRATEGY MID-TERM REVIEW

3.4 OVERVIEW OF CYBER SECURITY COURSES

Cyber Ireland has previously identified 69 cyber security courses[26] in Ireland that support cyber security skill development at different levels of experience. These courses must be accredited under the National Framework of Qualifications (NFQ) with courses including at least 15 credits of cyber security. Industry certifications and non-accredited courses, while valuable and in demand, are not included.

- 35 courses are aimed at bachelor or master's level entry;
- 30 are designed to upskill existing IT professionals that want to specialise in cyber security; and
- 4 courses are at the apprenticeship level, facilitating on the job learning.

[26] Cyber Ireland (2023) Course finder. Available at: https://cyberireland.ie/course-finder/https://www.gov.ie/pdf/?file=https:///261971/356d743c-b154-4a5f-b7ae-eb6714c2d011.pdf#page=null

Course length, and approach to study are also flexible:

- 57% of courses are no longer than a year;
- 54% offer a blended or online approach to learning; and
- 42% of all courses are offered on a part-time basis.

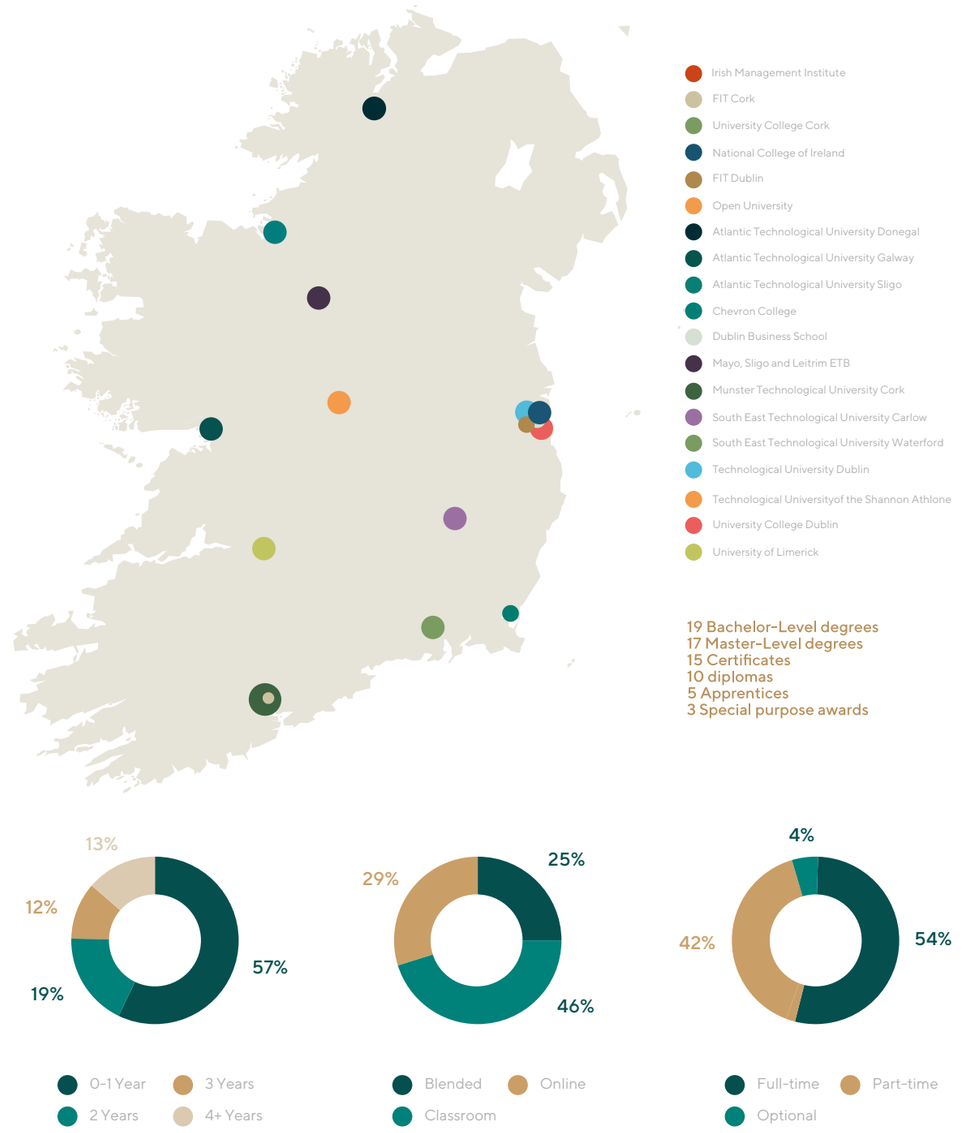
This suggests that Ireland has a strong foundation of graduate-level training, alongside transitional training to support entry from diverse pathways.

> *"Local colleges do a great job of preparing entry level candidates."*
>
> **DIVERSIFIED COMPANY WITH A CYBER SECURITY TEAM**

To support the development of a sustainable talent pipeline the content of these courses should be reviewed against the current industry demand, building on existing relationships between Cyber Ireland, government, industry, and academia to ensure high quality and consistent training is available throughout the country:

> *"We work closely with colleges... Some conversion courses are really good, such as the courses provided through the National University... [but] we have seen some courses elsewhere that don't seem to specialise enough for our offering."*
>
> **PROVIDER OF CYBER SECURITY SERVICES**

FIGURE 3:3 CYBER SECURITY TRAINING PROVIDERS IN IRELAND



Source: Cyber Ireland

Please note that stakeholders also highlight the value of recruiting talent from sectors with a similar skillset to cyber security.

3.5 LEVEL OF EXPERIENCE IN DEMAND

Cyber Ireland's Skills Report [27] (2021) offers insight into the current skill pipeline, suggesting that 41% of cyber security teams are understaffed, and that 48% of firms have an open or unfilled role. Of the open and unfulfilled roles tracked in Cyber Ireland's survey, 77% were for technical positions. Over a third of survey respondents (34%) suggest that lack of technical talent was the primary reason for open roles not being filled.

This finding has been tested with sector stakeholders, who have suggested that this barrier in recruitment is linked with the availability of experienced hires in Ireland:

> *"Mid to senior levels are most in demand... more experienced hires are always an issue."*
>
> DIVERSIFIED COMPANY WITH A CYBER SECURITY TEAM

> *"Experienced hires are hard to find, there can be a lot of applicants and we're specific about what we want at this level."*
>
> PROVIDER OF CYBER SECURITY SERVICES

> *"We are always looking for people who can lead... but they're rare and likely already embedded into a role elsewhere."*
>
> PROVIDER OF CYBER SECURITY SERVICES

> *"A masters in cyber security is heavily sought after with a few years' experience, but the cyber security masters has only been available for a few years."*
>
> RECRUITMENT FIRM

[27] Cyber Ireland (2021) Cyber Security Skills Report 2021. Available at: https://cyberireland.ie/wp-content/uploads/2021/02/Cyber-Ireland-Skills-Report-2021.pdf

3.6 CERTIFICATIONS IN DEMAND

The Cyber security skills in the UK labour market (2023)[28] report offers insight into the value of certification among recruiting firms. This study suggests that 45% of firms surveyed have staff with a specialist degree in cyber security, and 38% have a more general degree in a related discipline, e.g., IT. In contrast, 74% of firms employ staff that have received a technical qualification or certified training relating to cyber security, noting that requested certifications are typically linked with a specific career pathway or specialism.

Aligned to the above study, stakeholders suggest that in demand certifications in Ireland are largely derived from career pathways:

> *"Cyber security is such a broad area. In terms of certification, we would look for something broad, e.g., CISSP, and then dependent on the role we would ask for a certification in something specific, e.g., for cloud roles we would seek a cloud certification, or the same for penetration testing."*
>
> PROVIDER OF CYBER SECURITY SERVICES

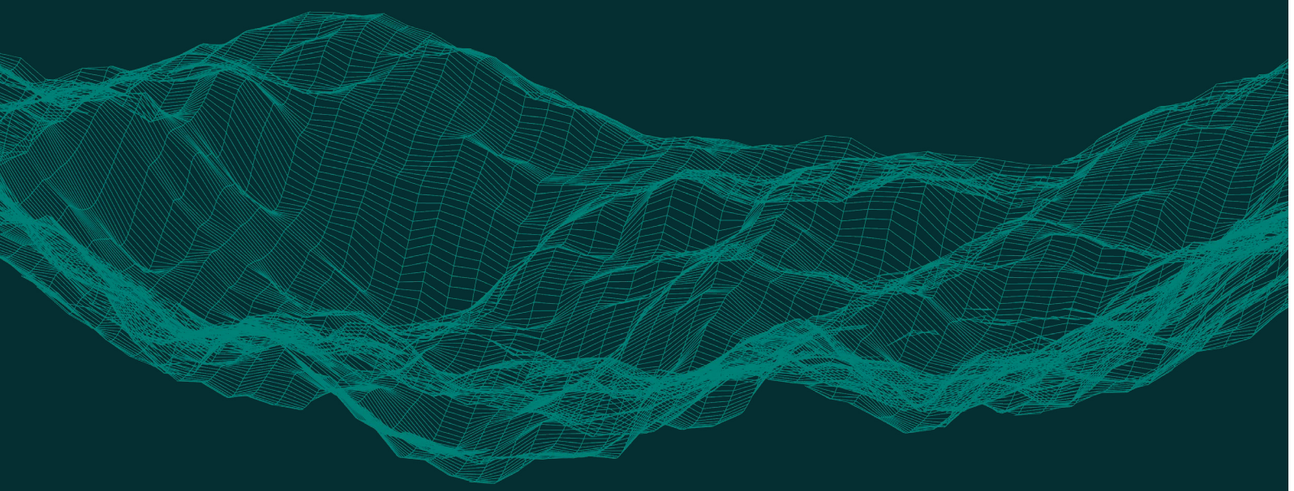
> *"A lot of people come in from infosec, and that's when degrees can come into play – specifically the master's in cyber security is asked for a lot."*
>
> RECRUITMENT FIRM

> *"SANS certs are always considered to be the highest level and most decorated."*
>
> DIVERSIFIED COMPANY WITH A CYBER SECURITY TEAM

[28] DSIT (2023) Cyber security skills in the UK labour market. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1173325/Cyber_security_skills_in_the_UK_labour_market_2023.pdf

04
Global Benchmarking

This section provides an overview of cyber security demand across comparator markets, including the United States, Germany, France, the UK, the Netherlands, and Poland.



4.1 GLOBAL BENCHMARKING: NUMBER OF JOB POSTINGS

The research team reviewed the number of job postings across identified comparator regions. This analysis is set out below:

TABLE 4.1 NATIONAL CYBER SECURITY JOB POSTING COMPARISON FOR 2022

COUNTRY	CYBER SECURITY POSTS	ALL ADVERTISED ROLES	% OF GLOBAL CYBER SECURITY ROLES	% OF ALL JOBS NATIONALLY
Global	1.23m	161.38m	-	0.8%
United States	515,077	55.95m	42%	1%
Ireland	6,707	858,546	0.5%	0.8%
Germany	90,073	13.75m	7%	0.7%
France	72,459	11.76m	6%	0.6%
UK	51,386	8.3m	4%	0.6%
Netherlands	12,477	3.39m	1%	0.4%
Poland	10,332	2.86m	1%	0.4%

Source: Lightcast Spotlight (2022 data)

Globally, Lightcast has identified 1.23m cyber security job postings in 2022, accounting for just under 1% of total job postings. The United States has a significant role in driving global demand, accounting for 42% of all advertised job roles in 2022 (n = 515,077). US-headquartered firms also have a significant role in driving demand in Ireland. This has been previously identified in Cyber Ireland's State of the Cyber Security sector report[29], which suggests that 28% of all cyber security firms in Ireland are headquartered in the United States, and that 55% of all employment is driven by FDI from the United States.

[29] Cyber Ireland (2022) State of the Cyber Security Sector in Ireland. Available at: https://cyberireland.ie/wp-content/uploads/2022/05/State-of-the-Cyber-Security-Sector-in-Ireland-2022-Report.pdf

Of all comparator regions Ireland makes up the smallest proportion of total cyber security job posts globally (n = 6,707, 0.5%). The sector is however strategic at the national level, with cyber security job postings accounting for 0.8% of Ireland's total job postings, which is higher than all comparator regions other than the United States. Stakeholders also note the strategic value of establishing a base of operation in Ireland:

> *"There's good word of mouth in the global industry around the quality in Ireland, and how we're able to build out teams."*
>
> PROVIDER OF CYBER SECURITY SERVICES

4.2 GLOBAL BENCHMARKING: SALARY COMPARISON

The median advertised cyber security salary was also compared with the national median salary for each country. This analysis is set out below:

TABLE 4.2 NATIONAL CYBER SECURITY SALARY COMPARISON FOR 2022

COUNTRY	CYBER SECURITY POSTS	CYBER SECURITY MEDIAN SALARY	NATIONAL-LEVEL MEDIAN SALARY[30]	SALARY PREMIUM
Global	1.23m	€81.3k	€35.3k	130%
United States	515,077	€103k	€42.8k	140%
France	6,707	€54.5k	€22.9k[31]	138%
Ireland	90,073	€74.9k	€35.3k	112%
Poland	72,459	€20.2k	€10.9k	84%
UK	51,386	€56.4k	€34k	66%
Netherlands	12,477	€49k	€33.1k	47%

Source: Lightcast Spotlight (2022 data)

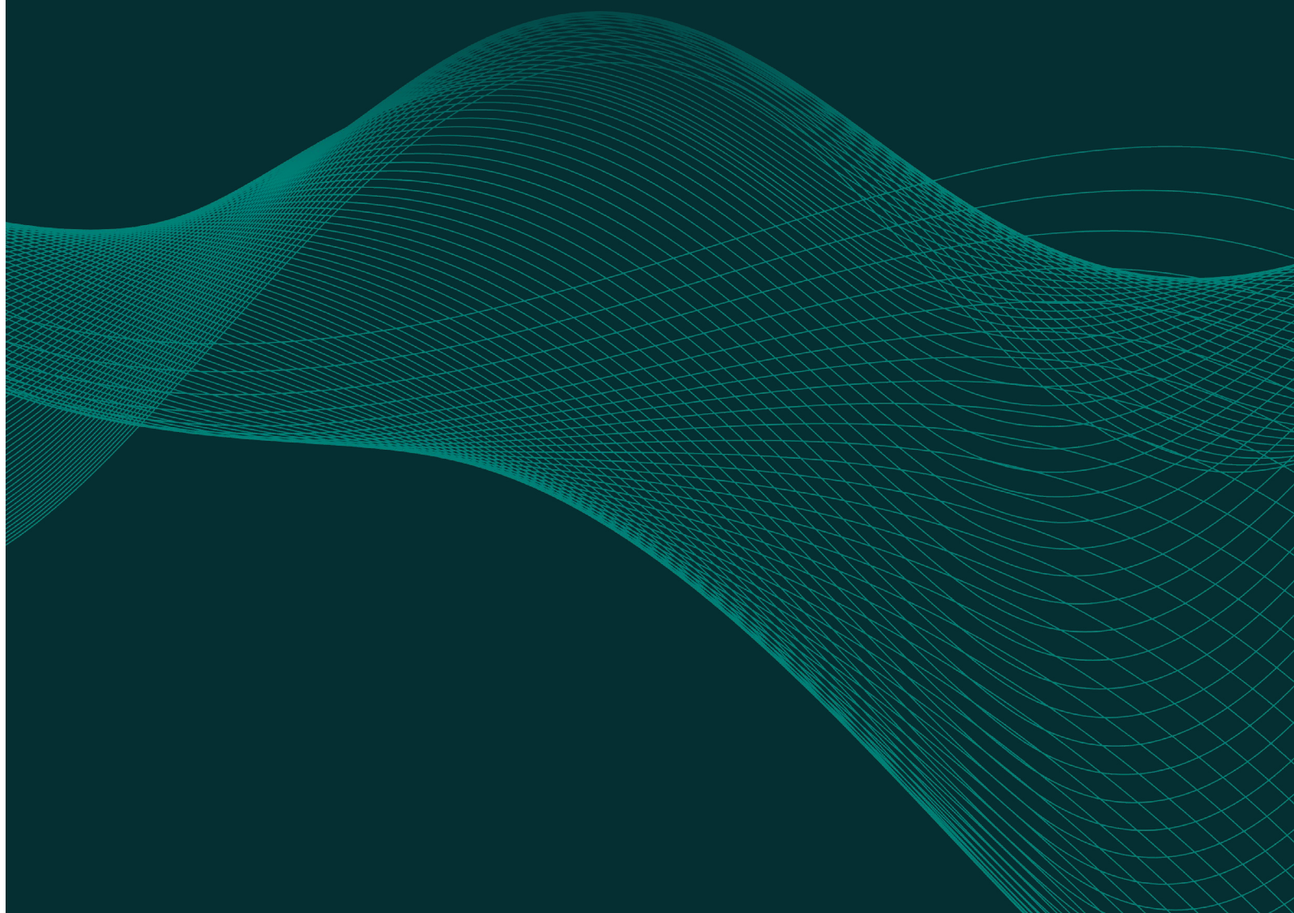
Ireland has the second highest median salary of comparator regions after only the United States. It also suggests that the salary premium is higher than most other comparator countries. This is indicative of the strategic value of the cyber security sector to Ireland, supporting higher value jobs.

[30] Please note that for the purpose of comparison the national salary used in this section has been derived from the advertised median salary on the Lightcast platform and not from official national statistics.

[31] Limited sample size

05
Future trends and considerations

This section provides a summary of wider desk research and considerations from stakeholder consultations relating to demand within the sector, barriers faced by the sector, and the future direction of growth and opportunity.



5.1 GLOBAL DEMAND FOR CYBER SECURITY TALENT

The global demand for cyber security talent is well documented, with recent workforce studies[32] suggesting that the global labour market now encompasses a record 4.7m people, an increase of c.464k workers from the previous year. Despite this impressive increase in the workforce globally, the global deficit in talent has also grown more than twice as much as the workforce.

The current global gap in the workforce is c.3.4m cyber security professionals, an increase of 26% from 2021's figures. Specifically, within Europe, there is a deficit of c.317k cyber security professionals, with ISC² estimating that this figure has increased 60% since the previous iteration of their research.

The ISC² report suggests that this deficit in the workforce is felt strongest by cyber security professionals, with 70% suggesting that their organisation does not have enough cyber security staff to be effective, with the gap in the workforce having an impact on the fundamental functions of the profession, such as risk assessment, oversight, and critical systems patching. Key sectors impacted by the deficit in cyber security professionals globally include aerospace, government, education, insurance, and transport.

5.2 NATIONAL DEMAND FOR CYBER SECURITY TALENT

Nationally, the yearly increase in job vacancies suggests that the demand was greatest between 2019 and 2020 (+66% job postings), and 2020 and 2021 (+74%); and while demand increased between 2021 and 2022, the increase was significantly lower (+15%). This suggests that, whilst there are signs of growth, there is a potentially slowing market. This trend was tested with stakeholders, who offer valuable insight into the current and future trends impacting Ireland's cyber security sector, which are summarised in the sections below:

5.2.1 UNCERTAINTY IN THE WIDER MARKET

The Morgan McKinley Quarterly Employment Monitor for quarter 2 2023 suggests that there has been a fall in professional job vacancies[33].

Stakeholders engaged as part of the current research have reflected on the current market, noting how market uncertainty has had an impact on attrition and mobility of cyber security talent between firms, also suggesting that firms are more cautious with recruitment currently.

[32] ISC2 (2022) 2022 Cybersecurity workforce study. Available at: https://www.isc2.org/Research/Workforce-Study

[33] Morgan McKinley (2023) Quarterly Employment Monitor. Available at: https://www.morganmckinley.com/ie/article/quarterly-employment-monitor-sharp-fall-in-professional-job-vacancies

> *"It [2023] has been a strange year. There have been a lot of people let go [in the wider tech industry] and as part of that we've seen some people redeployed to cyber security. We're still super busy and attrition is down... People don't feel as mobile [however] which is not creating a space for other people to come in... We're not seeing security as an area for lay-offs."*
>
> PROVIDER OF CYBER SECURITY SERVICES
>
> *"Up until October 2022 we were very active, but we started seeing a lot of potential roles collapsing or being put on hold until January... [It seems] that this was directly due to budget availability."*
>
> RECRUITMENT FIRM
>
> *"There's less noise in the recruitment world. Before people were less risk adverse."*
>
> PROVIDER OF CYBER SECURITY SERVICES

As noted elsewhere in the report, regulation has been identified as a key driver for recruitment in the sector, limiting the impact of wider tech layoffs to cyber security professionals. This is reflected in Morgan McKinley's Q2 trends, which has noted an increase of demand for cyber security talent in the banking and financial sector, also suggesting that cyber security engineers were among the most in-demand roles more generally.

5.2.2 IMPLICATIONS OF COVID-19

The analysis conducted as part of this study suggest that while demand for cyber security talent is still increasing in Ireland, it is slower than during the pandemic. Stakeholders have suggested that the slowdown in recruitment is linked with the market correcting itself following increased demand during the COVID-19 pandemic:

> *"During the pandemic, hiring for cyber security was through the roof, but now firms are more cautious about hiring... There is also the salary and expectation from candidates. Last year you could demand €80k for four years' experience, but its peeled right back. So maybe there's a disconnect now between candidates and companies, where companies are now being more realistic."*
>
> RECRUITMENT FIRM

Despite this slowdown in market activity, recruiters suggest that market activity is once again increasing:

> *"It's opening up again now... the roles are out there but its slow moving at the minute... There was probably an element of over hiring, and at the moment there's still cautiousness and budget cutting... but things are levelling out."*
>
> RECRUITMENT FIRM

5.2.3 THE NEED TO PRIORITISE CYBER SECURITY AMONG FIRMS IN IRELAND

The desk review suggests that the risk of cyber security attacks can have significant implications to revenue and operations across sectors. The ISC[2] study suggests that 70% of workers globally do not think their organisation is appropriately staffed, and more than half of those surveyed would suggest that this puts their organisation at a moderate or extreme risk of cyber-attacks.

The Hiscox Cyber Readiness Report (2022)[34] offers insight into risk and costs to businesses in relation to cyber security attacks. It suggests that Ireland has paid out ransoms more regularly than other countries, paying five times or more to recover data. The report also suggests that the incidents of cyber-attacks have increased 10% in Ireland, which is above average of benchmarked regions, and that the median cost of cyber-attacks has also increased at a faster rate than most comparators.

This analysis suggests that many businesses in Ireland have limited awareness or have not prioritised cyber security within their organisations. This is reflective of the National Cyber Security Centre and the National Cyber Crime Bureau public alert in August 2022 to SMEs about the increased threat of ransomware attacks on SMEs, alongside measures set out in the National Cyber Security Strategy mid-term review:

- Develop a voluntary cyber security standard for Irish SMEs aligned with relevant international standards.
- Implement a financial support programme for SMEs and other societal stakeholders, in accordance with EU provisions, to improve cybersecurity resilience and facilitate innovation.

NATIONAL CYBER SECURITY STRATEGY, MID-TERM REVIEW MEASURES

[34] Hiscox Group (2022) Cyber Readiness Report. Available at: https://www.hiscoxgroup.com/sites/group/files/documents/2022-05/22054%20-%20Hiscox%20Cyber%20Readiness%20Report%202022-EN_0.pdf

To encourage cyber security good practice the Government could adopt cyber security certification, similar to, e.g., the UK's Cyber Essentials[35]. Cyber Essentials requires select Government contractors handling data to be certified and establishes a minimum standard for cyber security processes in the private sector.

5.2.4 EMBEDDING CYBER SECURITY BEST PRACTICE IN GOVERNMENT

It is important to acknowledge the work undertaken by the Government in recent years to increase cyber security awareness and resilience in Ireland. Most recently, this includes the guidelines developed by the National Cyber Security Centre, Grant Thornton, and wider stakeholders to establish best practice for cyber security public procurement[36], illustrating how the developing regulatory landscape is shaping Ireland's commitment to secured public services:

> *"These guidelines aim to reinforce the Cyber Security Baseline Standards and current and future EU legislative proposals including the Network and Information Security (NIS) Directive and the NIS directive revision (NIS2) and the EU Cyber Security Act Regulation. The publication also considers ongoing EU legislative proposals including the Cyber Resilience Act."*
>
> DEPARTMENT OF THE ENVIRONMENT, CLIMATE AND COMMUNICATIONS

[35] National Cyber Security Centre (2023) About Cyber Essentials. Available at: https://www.ncsc.gov.uk/cyberessentials/overview

[36] Department of the Environment, Climate and Communications (2023) Guidelines on Cyber Security Specifications published. Available at: https://www.gov.ie/en/press-release/5d4b0-guidelines-on-cyber-security-specifications-published/

Other activity across Government includes the National Cyber Risk Assessment (2022)[37], which examines the systematic cyber risks faced by the State's critical services and makes three core recommendations focused on strengthening legislative provisions to embed cyber security measures into products and services at the outset, ensuring that dependencies can be managed across the supply chain, and mapping all essential and important state entities.

This proactive engagement to increase cyber resilience will have implications for both Government and supplier organisations, and the skills required to meet this new demand. This has been highlighted by stakeholders in relation to the Digital Operational Resilience Act (DORA) and the impact that this will have on the financial sector, and the NIS2 Directive and the impact that this will have on the OT specialism:

> *"With DORA, there is a need for implementation by 2025. I see [demand] for this a lot, though it will not be called a "DORA" role, but cyber risk, information risk, or analyst, etc.... On the other side there is the OT environment and in particular the NIS2 Directive... [This requires] OT roles... there's no large pool of talent and it's an incredibly niche area. As a result, we're bringing in people from England and India. At the minute it's the biggest demand."*
>
> RECRUITMENT FIRM

> *"We work with national infrastructure who are preparing for NIS2. This requires OT skills, particularly for utilities and manufacturing. But it's not just OT, NIS2 is driving a need for cyber security across IT systems as well."*
>
> PROVIDER OF CYBER SECURITY SERVICES

[37] Rialtas na hÉireann | Government of Ireland (2022) National Cyber Risk Assessment. Available at: https://www.gov.ie/en/publication/5a871-national-cyber-risk-assessment-2022/

The role of NIS2 is also highlighted in the National Cyber Security Strategy mid-term review, which notes the importance of the directive in shaping Ireland's future cyber security strategy:

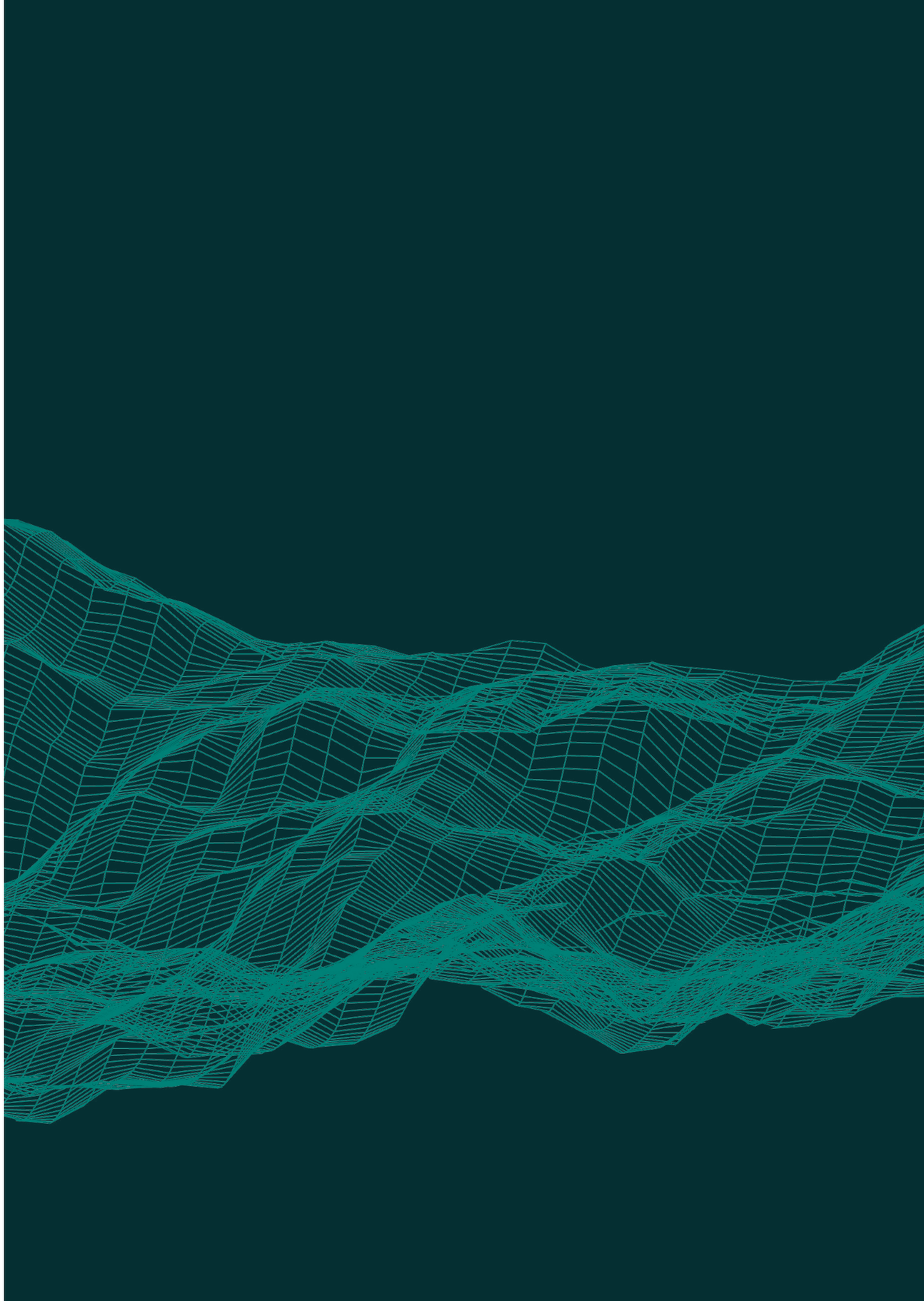
> *"The NIS2 Directive referenced earlier includes provisions for national cyber security strategies, including a number of areas Member States are required to consider when drafting their national strategy. The relevant article will be transposed into Irish law as part of the transposition of the Directive, and so it will inform the process of developing the successor strategy for the period from 2024 onwards."*
>
> NATIONAL CYBER SECURITY STRATEGY MID-TERM REVIEW

The role of regulation in shaping demand should therefore not be overlooked, and Cyber Ireland should engage partners to identify key areas of regulation, and the skills required to meet the demand that they create.

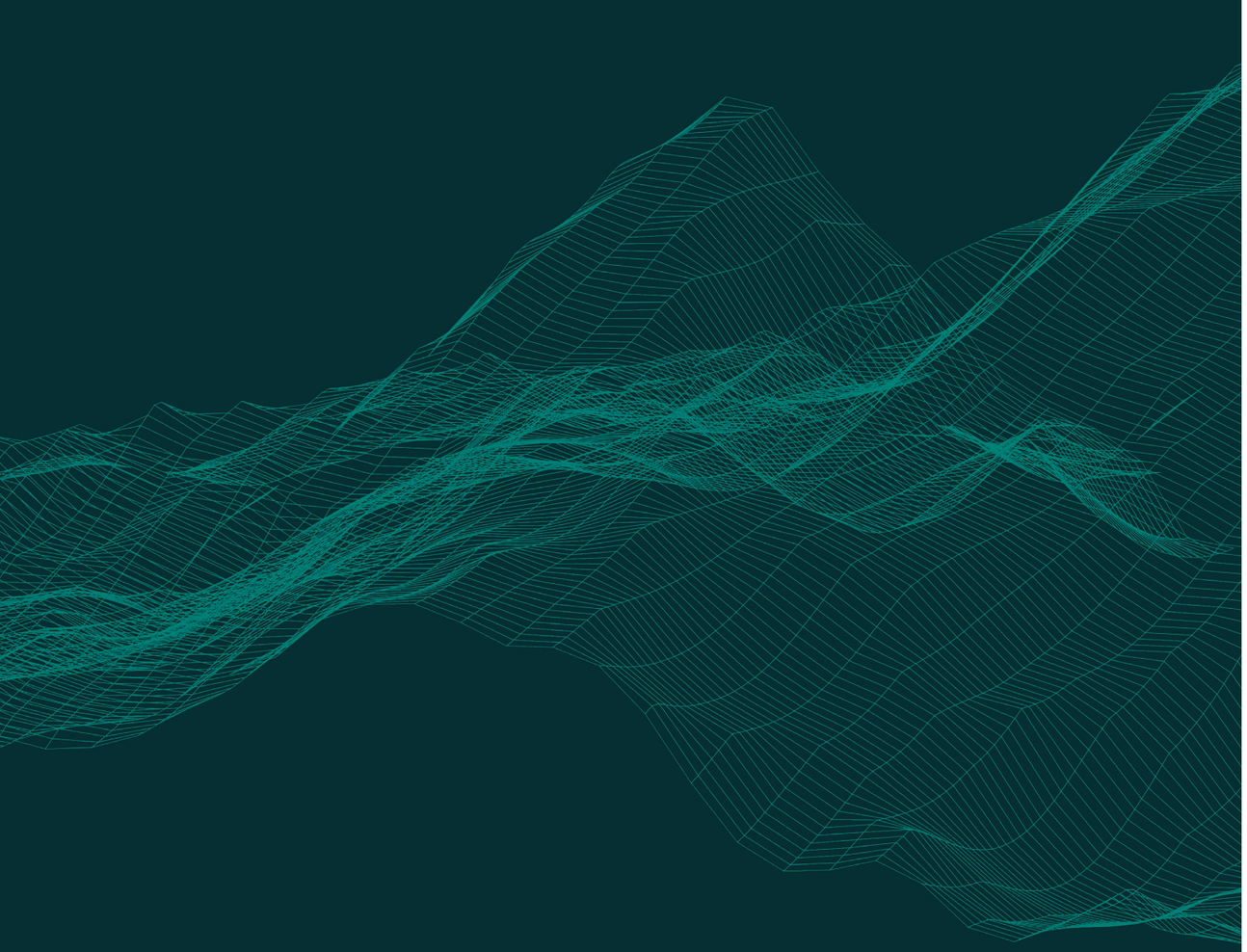
5.2.5 EMBEDDING CYBER SECURITY LEARNING ACROSS SOCIETY

Stakeholders have noted the importance of increasing awareness of cyber security among the general public, as well as Government. With more risk, and increasingly digitised services there is a need to extend the understanding of cyber security and digital risk across society more generally, as noted by stakeholders:

> *"While there are still not enough cyber security staff, it's the general population that schemes should be targeting. No one [in wider society] mentions cyber security... [We should] do more at the second and third level... It's the general education and looking beyond immediate demand to longer term resilience."*
>
> PROVIDER OF CYBER SECURITY SERVICES



06
Key Findings and Recommendations



This section provides a summary of key findings and recommendations:

6.1 KEY FINDINGS

PIPELINE AND DEMAND

- The State of the Cyber Security Sector 2022 report identified 7,351 private sector professionals working in the cyber security sector, with the potential for 17,000 private sector jobs by 2030.
- To meet this demand, the sector would need to recruit an additional c.1,000 workers each year.

Number of vacancies

- In 2022, there were 6,707 unique job postings for cyber security professionals in Ireland – demand more than trebling from 2019.

SECTOR SALARY

- Ireland's median cyber security salary for 2022 (€75k) was almost twice the official median salary for Ireland (€41k, 2020).
- Ireland's median cyber security salary has seen yearly growth, increasing 4% from 2021 and 8% from 2020. Salaries are highest in Dublin and the South West.

REGIONAL DEMAND

- All of Ireland's regions have seen a significant increase in cyber security job postings between 2019 and 2022. The regions with the highest demand in 2022 include Dublin (4,396 posts), the South-West (983), the Mid-West (309), and the Mid-East (289).
- The largest net increase in job postings can be seen in Dublin (2,967 jobs), the South West (715 jobs), the South East (255), Mid-West (224), and Mid-East (217), yet relative to their baseline, all regional job postings have increased at a faster rate than Dublin.

SECTORAL DEMAND

- Lightcast suggests that c.34% of all online vacancies are advertised via a third-party recruitment agency.
- Excluding recruiters, sectors with the highest levels of demand include Information Technology sector (17%), the Financial Services sector (16%) and cyber security (14%).

JOB ROLES AND TECHNICAL SKILLS

71% of job posts were in one of three categories:

- Cyber security implementers[38] (46% of job roles) handle product development, integration, and maintenance. They need skills in solution integration, security assessment, coding, and communication.
- Cyber incident responders[39] (13%) create and assess Incident Response Plans, handle incidents, manage vulnerabilities, measure response effectiveness, and document actions. Key skills encompass technical handling, threat analysis, system operation, pressure handling, communication, and log analysis.
- Cyber security risk managers[40] (12%) develop risk strategies, manage asset inventory, assess threats, propose risk treatments, monitor controls, and ensure risk levels are acceptable. Skills involve framework implementation, compliance, risk analysis, stakeholder communication, and risk-sharing.

[38] Alternative job titles for this role include: Information Security Implementer, Cyber security Solutions Expert, Cyber security Developer, Cyber security Engineer, Development, Security & Operations (DevSecOps) Engineer

[39] Alternative job titles for this role include: Cyber Incident Handler, Cyber Crisis Expert, Incident Response Engineer, Security Operations Center (SOC) Analyst, Cyber Fighter /Defender, Security Operation Analyst (SOC Analyst), Cyber security SIEM Manager

[40] Alternative job titles for this role include: Information Security Risk Analyst, Cyber security Risk Assurance Consultant, Cyber security Risk Assessor, Cyber security Impact Analyst, Cyber Risk Manager

GLOBAL BENCHMARKING

- Cyber security job posts make up 0.8% of all job posts in Ireland, which is a higher proportion of national job posts of any comparator region other than the United States[41]. This suggests that in proportion to the available labour force, Ireland has a significant demand for cyber security skills.
- The cyber security salary premium is also significant in Ireland, behind only the United States and France[42].

FACTORS IMPACTING NATIONAL DEMAND

- The increase in national job vacancies was most notable between 2019 and 2021, slowing in 2022. Stakeholders attribute this slowdown in recruitment to wider market uncertainty and correction for over hiring during the COVID-19 pandemic.
- Businesses in Ireland have paid out ransoms more regularly than other European countries, paying five times or more to recover data. This suggests industry could better incorporate cyber security into their business practices. Growing awareness in this area, and increased regulatory requirements have both been noted as factors contributing to the growing demand for cyber security.
- There is a need to incorporate cyber security practices and improve understanding across wider society. Stakeholders suggest that this should include increased engagement with students in primary and secondary education, and the inclusion of cyber security modules in more general IT courses at the university level, and in courses that will likely lead to employment in sectors that are currently hiring for cyber security roles (e.g. finance).
- Mid to senior level roles have been noted as most in demand by stakeholders, and in demand skills are driven by industry-specific regulation, e.g., OT-specialists as a result of the NIS2 directive, and the role of the Digital Operational Resilience Act (DORA) on the financial services sector.

[41] Comparator region and proportion of cyber security job posts include: United States (1%), Ireland (0.8%) Germany (0.7%), France (0.6%), UK (0.6%), Netherlands (0.4%), and Poland (4%)

[42] Comparator region salary premiums include: United States (140%), France (138%), Ireland (112%), Poland (84%), UK (66%), and the Netherlands (47%)

RECOMMENDATIONS

Recommendations developed as a result of this research are grouped across three main themes, outlined below:

UNDERSTANDING THE SKILL PIPELINE

While this study provides an assessment of the current level of demand for cyber security talent, additional research should be undertaken to determine the current skill supply in Ireland. Recommendations relevant to supply-side skills assessment include:

Evaluation of the supply-side skills in Ireland's cyber security market: The cyber security sector study completed in 2022 identified c.7,351 cyber security employees across 489 organisations in Ireland. Further research to identify what skills are readily available in the labour market, and where the perceived shortfall exists will support Cyber Ireland and its partners' understanding of the market, to be used to inform the development of existing and future training and education schemes.

Assess the applicability of the ENISA's European Cybersecurity Skills Framework to Ireland's private sector and education market: This research has used the ECSF skills profiles to classify job postings. The ECSF has been developed to establish a common terminology for the cyber security sector within the EU. Future research should assess the applicability of the ECSF in Ireland's market context, alongside its alternatives, e.g., the NICE Framework. The incorporation of existing frameworks into sector planning will support skill tracking and policy design.

Assess cyber security regulatory requirements and what this means for future skills demand: Stakeholders have noted how regulation is a significant driver for cyber security employment. Cyber Ireland should work collaboratively with industry and Government to identify the current and future regulatory requirements likely to influence demand for cyber security talent. This includes, e.g., demand brought on by NIS2, CRA, and DORA. This can help inform future workforce planning, and potentially support the development of entry-level pathways such as cyber security apprenticeships focused on areas such as OT and regulatory compliance.

SUPPORTING EDUCATION & SKILL DEVELOPMENT

Evaluation of education and training pathways to determine entry-level competencies: Cyber Ireland have identified 69 cyber security courses in Ireland. Future research that explores the volume of students completing these courses, the competencies they develop, and their career progression will present a clear picture of Ireland's cyber security talent pipeline and the entry-level skillsets available to the market. It will also support Cyber Ireland and partners in assessing to what extent available courses are meeting the current skills demand in the market.

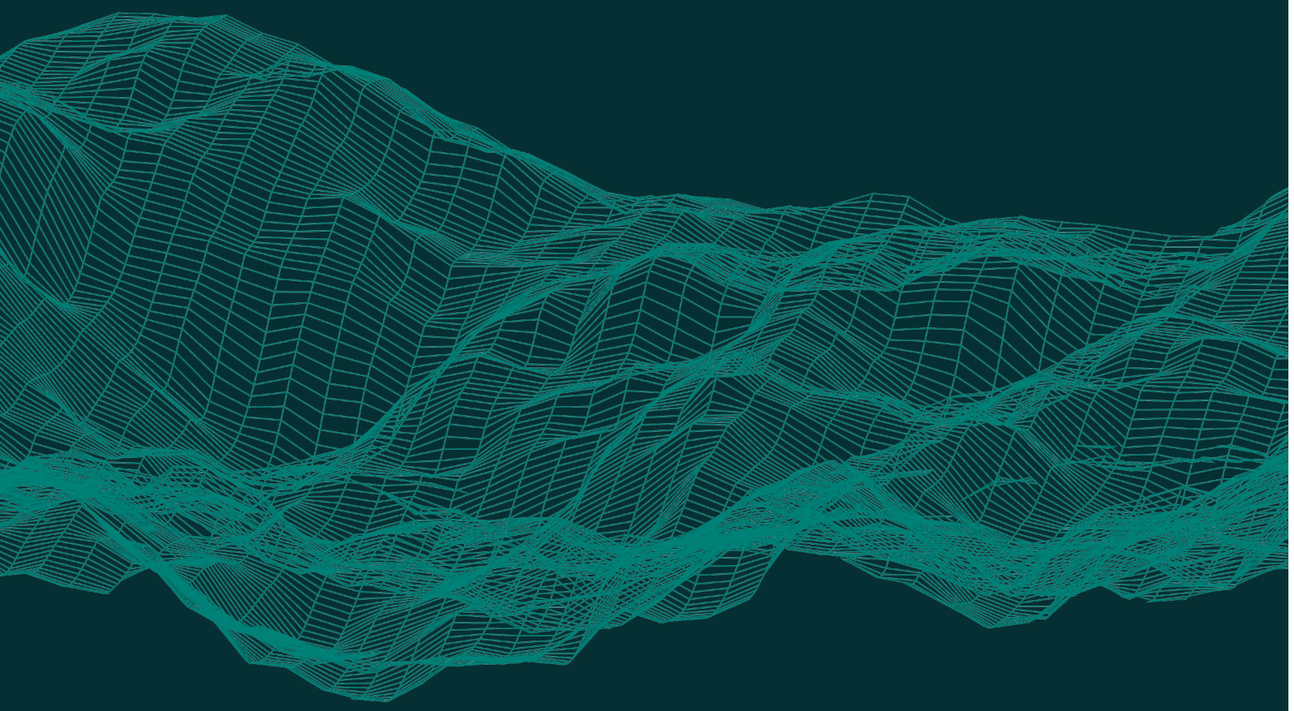
Increase awareness and education at primary and post primary level through a nationally funded, coordinated scheme: Cyber Ireland should continue to work collaboratively with Government to develop a national scheme to facilitate sectoral awareness among young people. This scheme should build on and incorporate learning from smaller scale schemes that have previously been active in Ireland, e.g., Cyberwise, CyberFutures and Schools Capture The Flag (CTF) Events.

SUPPORTING CYBER SECURITY RESILIENCE WITHIN THE PRIVATE SECTOR

Establish a baseline security standard for cyber security practice through certification: While available literature suggests that businesses are becoming more aware of the risks associated with poor cyber security measures, the adoption of certification, similar to the UK's Cyber Essentials Certification, will have significant impact on the cyber security resilience of Ireland's private sector, also creating further opportunities to support entry-level employment.. This could also be embedded within public procurement processes to ensure private contractors are meeting minimum cyber security standards.

Schemes to support cyber security employment in strategic sectors: Cyber Ireland should engage with recruiting firms within strategic sectors (e.g., IT and finance) to identify skills demand and to establish career development pathways. This could include upskilling and transition of existing staff with similar skillsets into cyber security roles. Examples of similar schemes include the UK's Department for Science, Innovation and Technology's Upskill in Cyber programme, delivered in partnership with the SANS Institute.

07
Appendix



SKILLS PROFILE: CYBER SECURITY IMPLEMENTER

Alternative titles:

Information Security Implementer, Cyber Security Solutions Expert, Cyber Security Developer, and Cyber Security Engineer Development, Security & Operations (DevSecOps) Engineer.

Main tasks:

- Develop, implement, maintain, upgrade, test cyber security products.
- Provide cyber security-related support to users and customers.
- Integrate cyber security solutions and ensure their sound operation.
- Securely configure systems, services, and products.
- Maintain and upgrade the security of systems, services, and products.
- Implement cyber security procedures and controls.
- Monitor and assure the performance of the implemented cyber security controls.
- Document and report on the security of systems, services, and products.
- Work close with the IT/OT personnel on cyber security-related actions.
- Implement, apply, and manage patches to products to address technical vulnerabilities.

Key skills:

- Communicate, present and report to relevant stakeholders.
- Integrate cyber security solutions to the organisation's infrastructure.
- Integrate cyber security solutions and ensure their sound operation.
- Configure solutions according to the organisation's security policy.
- Assess the security and performance of solutions.
- Develop code, scripts, and programmes.
- Identify and solve cyber security-related issues.
- Collaborate with other team members and colleagues.

Source: ECSF

SKILLS PROFILE: CYBER INCIDENT RESPONDER

Alternative titles:

Cyber Incident Handler, Cyber Crisis Expert, Incident Response Engineer, Security Operations Center (SOC) Analyst, Cyber Fighter /Defender, Security Operation Analyst (SOC Analyst), and Cyber Security SIEM Manager.

Main tasks:

- Contribute to the development, maintenance, and assessment of the Incident Response Plan.
- Develop, implement, and assess procedures related to incident handling.
- Assess and manage technical vulnerabilities.
- Measure cyber security incidents detection and response effectiveness.
- Evaluate the resilience of the cyber security controls and mitigation actions taken after a cyber security or data breach incident.
- Adopt and develop incident handling testing techniques.
- Establish procedures for incident results analysis and incident handling reporting.
- Document incident results analysis and incident handling actions.
- Cooperate with Secure Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs).
- Cooperate with key personnel for reporting of security incidents according to applicable legal framework

Key Skills:

- Practice all technical, functional, and operational aspects of cyber security incident handling and response.
- Collect, analyse, and correlate cyber threat information originating from multiple sources.
- Work on operating systems, servers, clouds, and relevant infrastructures.
- Work under pressure.
- Communicate, present and report to relevant stakeholders.
- Manage and analyse log files.

Source: ECSF

SKILLS PROFILE: CYBER SECURITY RISK MANAGER

Alternative titles:

Information Security Risk Analyst, Cyber Security Risk Assurance Consultant, Cyber Security Risk Assessor, Cyber Security Impact Analyst, Cyber Risk Manager

Main tasks:

- Develop an organisation's cyber security risk management strategy.
- Manage an inventory of organisation's assets.
- Identify and assess cyber security-related threats and vulnerabilities of ICT systems.
- Identification of threat landscape including attackers' profiles and estimation of attacks' potential.
- Assess cyber security risks and propose most appropriate risk treatment options, including security controls and risk mitigation and avoidance that best address the organisation's strategy.
- Monitor effectiveness of cyber security controls and risk levels.
- Ensure that all cyber security risks remain at an acceptable level for the organisation's assets.
- Develop, maintain, report, and communicate complete risk management cycle.

Key Skills:

- Implement cyber security risk management frameworks, methodologies and guidelines and ensure compliance with regulations and standards.
- Analyse and consolidate organisation's quality and risk management practices.
- Enable business assets owners, executives, and other stakeholders to make risk informed decisions to manage and mitigate risks.
- Identification of threat landscape including attackers' profiles and estimation of attacks' potential.
- Build a cyber security risk-aware environment.
- Communicate, present and report to relevant stakeholders.
- Propose and manage risk-sharing options.

Source: ECSF

CYBER | IRELAND
IRELAND'S CYBER SECURITY CLUSTER

Perspective Economics