Regional Skills
NORTH WEST
Partnerships for Skills

An Roinn Breisoideachais agus Ardoideachais, Taighde, Nuálaíochta agus Eolaíochta
Department of Further and Higher Education, Research, Innovation and Science

CYBER|IRELAND
North-West Chapter

NORTH WEST

Cyber Security Skills Audit Report

December 2022

Regional Skills
NORTH WEST
Partnerships for Skills

Table of Contents

Foreword

Hilary McPartland

Regional Skills Manager

As manager of the North West Regional Skills Forum this report has captured the opportunity for cybersecurity in the North West.

It finds a vibrant ecosystem with great potential to grow. It's the first step in our journey to build this sector to be one of the leaders in our region. I look forward to helping develop the talent and skills needed to support this dynamic sector vital to our economy and future success.

Paul Brady

Senior Director – Enterprise Information Security (Optum)

As both a business stakeholder and chapter lead for Cyber Ireland I am excited to see this report come to fruition.

The report offers clear and sensible direction to promote the growth of cybersecurity in the North West region and I welcome the recommendation that now is the time to invest in cyber talent to take advantage of the opportunities ahead of us.

Tim Kelly - Strategic Head for TCS Threat Management Centres in UKI & Europe

As part of the TCS cyber security leadership team responsible for setting the strategic direction of our threat management centres, I wholly support the report's recommendations to ensure Ireland talent can deliver on the global opportunities in the cyber security sector.

This study rightly identifies the urgent need to accelerate investment to satisfy the demand for security skills. TCS Cyber Security Practice continues to invest in its Threat Management Centres across the globe. We are committed to grow and strengthen our Ireland TMC to service our customer cyber security needs from our global delivery centre in Letterkenny.

Executive Summary

This research project was commissioned to examine the shape of the cybersecurity sector in the North West (NW) region as well as to identify the key skills gaps and challenges that need to be addressed to help the sector grow and flourish.

It also looked to identify the region's strengths which would be attractive to companies seeking a new location for cybersecurity. It was completed through interviews and surveys with a wide range of businesses and stakeholder organisations.

The research found a burgeoning, cyber-friendly ecosystem that could significantly help grow Ireland's cybersecurity sector. The region has two established global cybersecurity operations, both with plans to rapidly grow in the coming few years. It has a new university (Atlantic Technological University) that brings together three institutes of technology, each with a strong record of supporting cybersecurity and industry. The local governments have a strong record of being agile and responsive to drive new business growth as it moved away from traditional industries. New initiatives such as Donegal Digital show the region's continued commitment to supporting entrepreneurial activity and economic growth.

A key finding from the research was the forecast for 220 new cybersecurity jobs in the region in the next few years growing the total cyber jobs by 88%.

These roles span entry to senior-level – with potential to fill many of these with talent from within the region. A key need emerging from this research is to expand much further the region's pool of cyber talent to take full advantage of these opportunities.

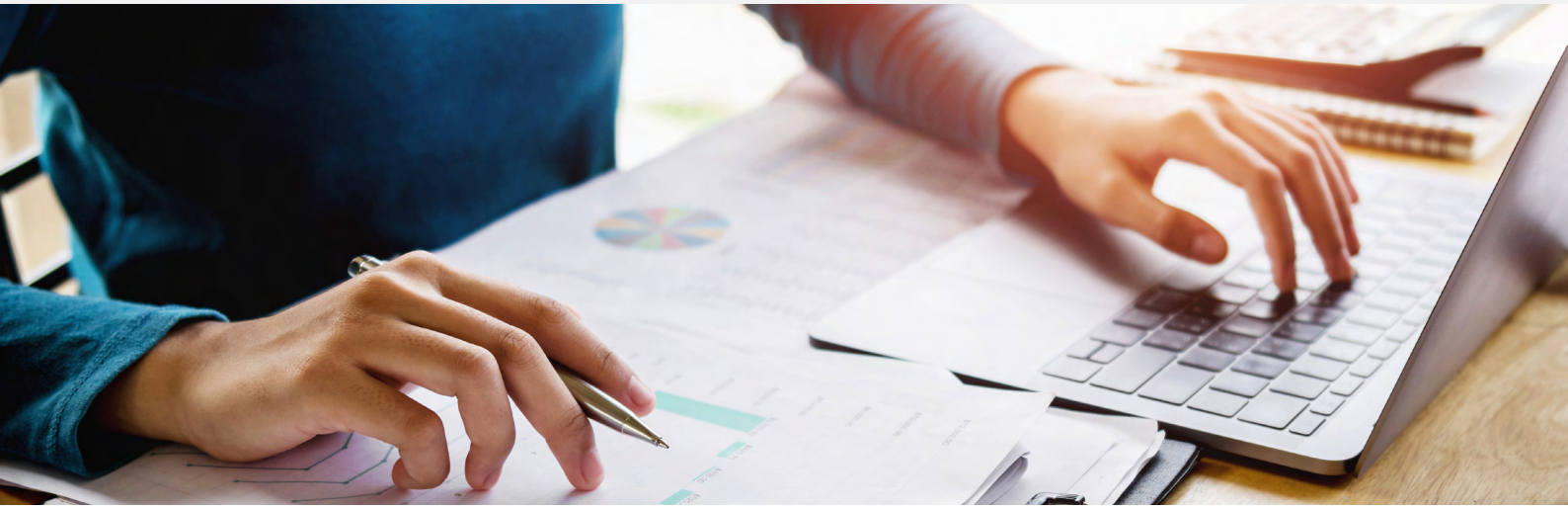
Providing educational and training support to cybersecurity employees, graduates, and other people aspiring to enter the field would aid the sector and the cybersecurity operators seeking to expand. In turn, facilitating this growth will make the region more attractive to new cybersecurity investment.

Another key finding was that many companies outside the cybersecurity field have recognised the need to improve the maturity of their cybersecurity, but that government support is needed to help drive this. A key starting point will be cyber awareness programmes that span across different sectors and levels so that owners, managers and employees understand the fundamentals for a secure business.

The recommendations in this report cover a range of areas – all focused on three underlying themes of: creating a culture of strong cybersecurity, promoting the region's assets to attract new cybersecurity investment, and enhancing the supply of cybersecurity talent within the region – all aimed at taking advantage of the forecasted growth of this sector globally. With a clear intent from the region's large cybersecurity operators to expand, now is the time to bring together all the stakeholders to facilitate the growth of the cybersecurity sector in the North West region.

About the Research Project

This project was commissioned by the North West Regional Skills Forum and Cyber Ireland's North West Chapter.



The primary aims of the research were to identify if there were opportunities for further employment in cybersecurity in the North West region and what the regional stakeholders could do to support these opportunities. More specifically the project sought to develop:

a. A profile of the cybersecurity activities in the region.

b. A synopsis of the current skills needs of employers in the region.

c. An estimate of the future skills needs of employers in the region.

d. An assessment of any mismatch between the demand for skills and the supply of skills.

e. An understanding of the challenges and opportunities facing the Cybersecurity Sector in the region.

f. Recommendations to address the challenges identified in the research.

The research consisted of desktop research, interviews with cybersecurity leaders and stakeholders, and skills audit surveys across a range of different organisations.

RESEARCH METHODOLOGY DETAILS

1. Desk research – explored the latest cyber security issues, trends and challenges at a regional, national and global level. It also covers the latest national initiatives for cyber security and also the current state of educational provision for cyber security in the region.

2. Interviews – involved 26 interviews with people working in, or supporting cybersecurity in the region (15) and with government stakeholders (7) with an interest in supporting the sector. The interviews sought to identify and discuss the extent of:

- Cybersecurity activity in the region.
- Supply and demand issues for cybersecurity resources.

- Future skills requirements for cybersecurity.
- Issues and challenges for this section in the region.

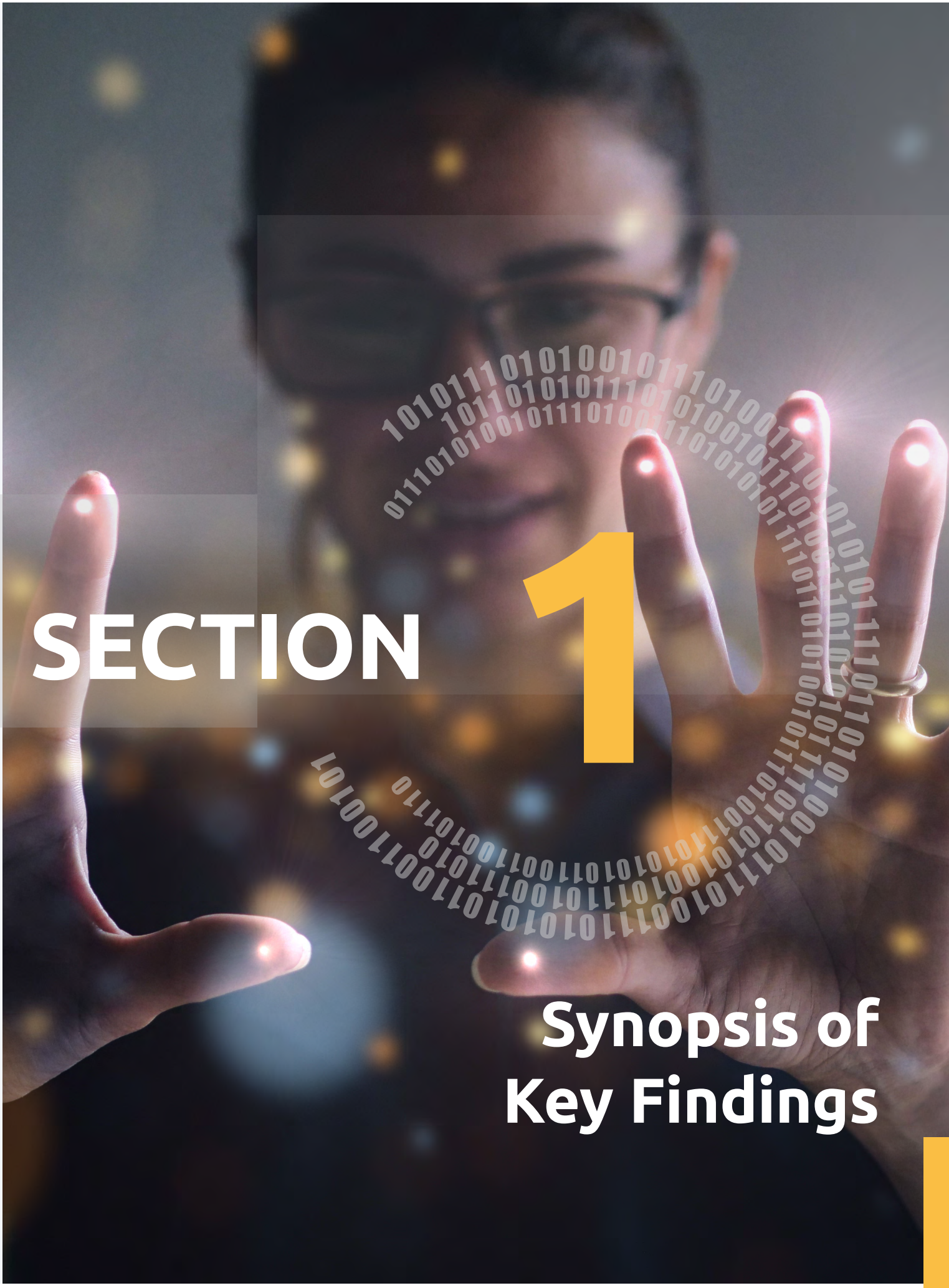
3. Surveys – one group completing a **technical skills audit survey** and a second a **non-technical version**. The data and findings from both groups are presented and discussed throughout the report (see Appendix 1 for the survey response profile).

Throughout the report two groups are frequently referred to as per below:

- The 'cybersecurity operators' – organisations actively offering the market cybersecurity services or a company with a significant internal cyber operation, this group completed the technical skills audit survey.
- The 'other organisations' – businesses not actively providing cybersecurity services to the market or without a cyber operation, this group completed the non-technical skills audit survey.

NOTE ON THE LIMITATIONS OF THE RESEARCH

A key limitation of this research was the relatively low number of survey respondents (25). Although this provided insights into cybersecurity issues and skills needs in the region, it did not provide a statistical representation of the overall business population.



SECTION 1

Synopsis of Key Findings

Synopsis of Key Findings

A PROFILE OF THE CYBERSECURITY ACTIVITIES IN THE REGION

The research identified at least 10 organisations offering cybersecurity services within the region. In particular:

- The region has two large, established cybersecurity operators (both in Letterkenny).
    - Tata Consultancy Services via its Global Delivery Centre – which includes cybersecurity (with plans to grow this function by up to 140 new posts).
    - Optum via its global healthcare systems, solutions and services - which includes cybersecurity.
- A new cybersecurity operator, Advantio, has recently announced its plan to create 40 cybersecurity jobs within the region (Sligo) in the next three years.
- There are 7 small IT / cybersecurity service providers in the region with varying intentions to add cybersecurity roles in the near future.
- It is estimated that there are 200 to 250 cybersecurity professionals working in the region.
    - Cyber Ireland's recent sectoral report estimates 7,350 cyber professionals in the ROI. Therefore approximately 3% of these are then based in the NW region.
- There are hiring intentions for approximately 220 new roles in the coming few years, which would bring the number to 470 cybersecurity professionals in the region.

A SYNOPSIS OF THE CURRENT SKILLS NEEDS OF EMPLOYERS IN THE REGION

The technical survey included 39 technical skills areas to evaluate, and the following were identified as the top skills needs (i.e. 20 or more employees require training) for the 'cybersecurity operators':

- Cloud cyber / native security.
- DevSecOps including application security.
- Cyber playbooks.
- Network security.
- Penetration testing.
- Security frameworks.
- Security Operations Centre (SOC).
- Vulnerability management.

Importantly, further development needs were identified for all technical skills areas provided in the survey and Appendix 2 provides a full breakdown of these requirements.

Regarding the skills needs of the 'other organisations', the non-technical survey found that cyber awareness training was the main priority. This can be broken down into two key areas:

1. General employee cyber awareness (including safe remote working practices).
2. Cyber awareness training for the manager/owner (including, for larger organisations, the topics of governance, risk, resilience, data protection and compliance in cybersecurity).

The need for cyber awareness training was confirmed in both the surveys and interviews - and aligns closely to a recent cybersecurity training needs report covering another region.

The research revealed a significant number of companies where IT or other staff with responsibility for cybersecurity which points to a training need to ensure they are kept up to date on the latest developments and techniques in cybersecurity. We have added this broad need below.

- Cybersecurity upskilling for IT staff or other employees (for those covering cybersecurity responsibilities).

The research also brought to light some emerging needs to address:

- Operational Technology (OT) cybersecurity upskilling – the manufacturing sector was highlighted as an important skills development area given the increasing threat level for this sector. Some universities (SETU) and institutions (Cyber Skills) are providing programmes, but a gap remains in terms of targeted, short form training to ensure manufacturing managers, technicians and operatives are quickly upskilled to protect industrial systems and networks.
- Cybersecurity standards – there is an emerging need to have available cybersecurity standards designed with SMEs in mind. It is felt this could play a key role in helping increase cybersecurity maturity for SMEs. With new cyber regulations on the horizon, cybersecurity standards for SMEs are likely to soon be important to the region's (and country's) overall competitiveness.

Cyber awareness training is the top priority for SMEs

AN ESTIMATE OF THE FUTURE SKILLS NEEDS OF EMPLOYERS IN THE REGION

The following needs are drawn from responses to the technical survey concerning future hiring intentions. The following will be key skills areas in demand by regional employers over the next 2 to 3 years:

1. **SOC Analysts L1 (up to 54 posts)** – particularly the provision of training to make new hires job-ready – covering topics such as: active directory, SIEM tools, network traffic analysis, security incident handling, security tools.

2. **IAM Solution Specialist (up to 40 posts)** – the skills and knowledge needed here would include: identity and access architecture, cloud security, cloud migration, zero trust, IAM tools and platforms, authentication protocols, project management, amongst others.

3. **Cloud Security Engineers (up to 35 posts**) – depending on the skill gaps at recruitment, this may include: Linux, programme languages, DevOps, containerization, virtualisation, vendor system training, cloud security, data science for cybersecurity and penetration testing.

4. **SOC Analysts L2/L3 (up to 24 posts)** – the skills needed would focus on: incident responding, digital forensics, malware reverse engineering, advanced malware detection/threat hunting and then threat intelligence tools and techniques.

5. **Vulnerability Assessors (up to 20 posts)** – the skills needed would include: operating systems, programme languages, test design, application security testing techniques, network analysis, security scanning tools, security frameworks and report writing.

6. **Senior Security Consultants (up to 20 posts)** – the skills and knowledge needed would vary depending on the role but may include security architecture, cyber intelligence, vulnerability assessments, cybersecurity platforms and tools, security policy, frameworks and best practices, governance and the consulting competencies.

TCS Cyber Security Practice in Letterkenny currently numbers 160+, growing to 300 in the medium term. Top skills in demand include cloud security, identity / access management, cyber resilience, and managed detection / response services. Our cybersecurity customers are prioritising identity security using 'identity as perimeter', and that accelerates deep and wide security skills demand in cloud, multi-cloud, and hybrid cloud environments across all the cloud platforms. This impacts related demand for skills supporting security strategies such as zero trust networking, and cloud native developments in threat detection, response, and recovery.

The above represents the main future skills needs of employers aligned to planned recruitment plans captured in the Technical Survey (see Appendix 3 for details).

AN ASSESSMENT OF ANY MISMATCH BETWEEN THE DEMAND FOR SKILLS AND THE SUPPLY OF SKILLS

The region looks set to increase cybersecurity roles by up to 220 new posts over the next few years and this presents talent supply issues. Interviews uncovered differing views on the supply of talent in the region; some participants report that the supply is “quite good” while others disagreed. This diversity of views may reflect the different recruitment plans and practices as well as the type and experience of employees required. The survey found some companies are recruiting predominantly from within the region, while others are recruiting mostly from outside Ireland. However, it is clear that the regional supply of cybersecurity professionals is not meeting the needs of respondents. The data collected indicates companies are recruiting just 30% of cybersecurity employees from within the region. The following looks at the supply and demand question in more detail based on current recruitment (hiring intention) demand.

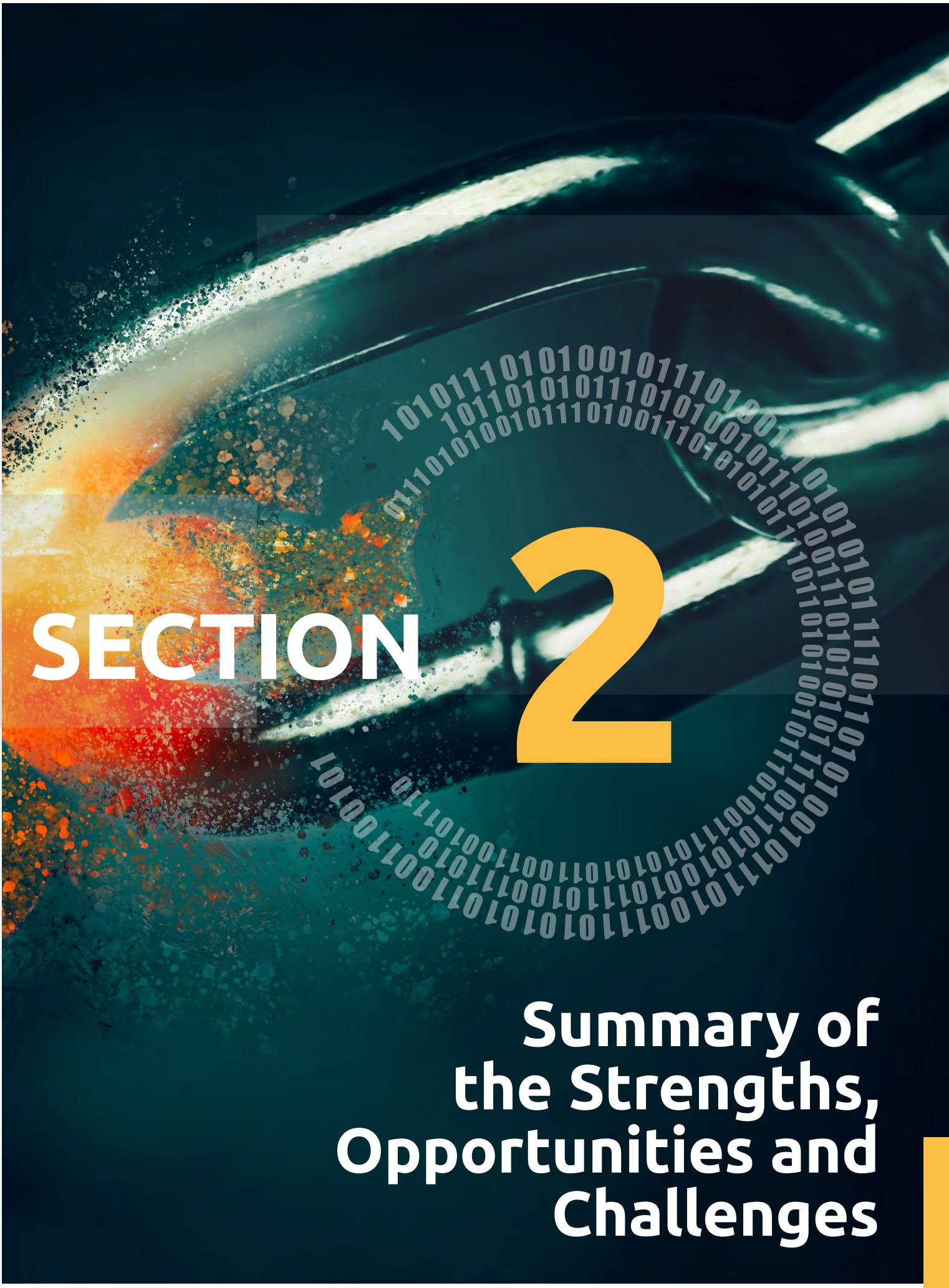
Entry Level roles – the research finds demand for entry level employees (SOC Analyst L1 and Technical Support) of up to 61 new posts in the coming few years. Graduate data from the Higher Education

Authority (HEA) reports the region producing 218 ITC undergraduates in 2020, indicating a strong potential supply of talent for these roles [ii] . However, views from respondents on graduate recruitment vary from 'they fit right in' to 'they take about 9 months to be job-ready'. If this is a substantive issue, education and industry stakeholders should work together to identify actual skills gaps and how these might be best addressed.

Second Tier roles – the research finds a sizeable portion of the planned new jobs (29) are second tier roles such as junior penetration testers, SOC Analysts L2 or junior cyber consultants. HEA's data for 2020 reported 93 ICT postgraduates for the region, with a good portion (no specific data available here) likely to include people with a cybersecurity specialty given the number of these degree programmes available in the region (see Section 3 - Education Ecosystem). This suggests that there is likely to be a potential supply of talent from within the region for a good portion of these 19 roles.

Senior roles – there is a significant talent supply issue for the 130 more senior level new cybersecurity posts planned for the region. For these roles, recruiting companies will need to focus more on attracting new talent from outside the region. Cyber Ireland calculates the total cybersecurity talent pool in Ireland to be around 7,350 which indicates, at the national level, a talent pool capable of filling many of these positions (with the right attraction campaign and job offer).

Just 30% of cybersecurity employees are recruited from within the region



SECTION 2

Summary of the Strengths, Opportunities and Challenges

Strengths, Opportunities & Challenges

This section draws upon the desktop, quantitative and qualitative research activities to identify the key Strengths, Opportunities and Challenges for the cybersecurity sector within the region.

STRENGTHS

- **Education** – the recently launched Atlantic Technology University (ATU) provides a significant strength in terms of the depth of cybersecurity programmes it can offer now and in the future. It brings together previous LYIT, IT Sligo and GMIT programmes and expertise along with their strong track records of collaborating with industry.
- **Lower Cost Base in Region** – the relative lower housing and office costs as well as the lower average salaries compared to other parts of the country could help attract employers to consider investing in the region. For potential employees, the lower cost of living in the region will need to clearly outweigh higher salaries outside the region. Cyber Ireland's sectoral report found competition for cybersecurity employees is a key barrier to growth. However, recent inflation and the escalating housing crisis should increase the attractiveness of working in the region for many cybersecurity professionals.
- **Established Anchor Clients** – the cybersecurity sector in the region has two key anchor clients based in Letterkenny (global companies with large cybersecurity operations), both with plans to grow their cybersecurity functions. The launch of Tata Consultancy Services' Global Delivery Centre offers an attraction opportunity for many potential employees. Optum's growing cybersecurity team and its history in the region are also an attractive part of this emerging cluster. The establishment of these large anchor clients demonstrates to potential investors that the region is an attractive and proven option.
- **Access to Nearby Clusters** – the North West region has access to and strong ties with Northern Ireland (NI) which has a strong cybersecurity cluster in Belfast (86 cybersecurity company offices) alongside Queen's University's CSIT (The Centre for Secure Information Technologies). This offers a nearby talent pool and expertise that may help contribute to the region's growth.

To the south, there is a cybersecurity cluster in Galway (with 39 cybersecurity company offices) where GMIT (now part of ATU) has delivered highly successful cybersecurity skills programmes in partnership with HPE and ITAG (Innovation Technology Atlantic Gateway). These relationships and good practices can be drawn upon more readily now given the recent move of GMIT into ATU.

OPPORTUNITIES

The cybersecurity industry is **set to grow** – with **10% average annual growth worldwide** in spend estimated up to 2026 [iv] . Ireland is in a good position to benefit from this with a high presence of global cybersecurity firms in the country [v] . Cyber Ireland estimates cybersecurity jobs nationally will more than double to 17,000 by 2030. As cybersecurity organisations look to set up or expand, more will look beyond the major business centres in Ireland due to high wages and the critical housing shortage (e.g. State Street's set up of a global cybersecurity unit in Kilkenny with up to 400 jobs expected). Within this context, the following are a number of important opportunities identified from this research project.

- **Cybersecurity Job Growth** – there is a clear opportunity to facilitate job growth for up to **220 new cybersecurity roles** in the coming few years. This would take the number of cybersecurity employees in the region to approximately 470 by end of 2024. With the average cybersecurity salary currently at €75,000, this would contribute significantly to the local economy, as well as nationally [vi] . Furthermore, using a projected 10% compound job growth figure (from Cyber Ireland's national job growth projections) and apply it to the 2024 job figure of 470, then cybersecurity jobs in the region **could reach 830 by 2030**. Supporting the growth of these high value / high wage jobs is an important priority for the region.
- **Cybersecurity as an Enabler of Business Growth** – as the cyber threat level increases for all businesses, strong cybersecurity is now viewed by many as an enabler of growth. Building a culture of strong cybersecurity in the region will contribute to future economic growth – by both protecting businesses and building a reputation as a secure place to do business. Establishing and promoting good cybersecurity practices across all sectors is central to this. Supporting both the global anchor clients and the local cybersecurity operators will help create this culture change by ensuring there is the necessary cybersecurity expertise and services available.
- **A North West University** – the launch of Atlantic Technological University (ATU) this year (amalgamating LYIT, IT Sligo, and GMIT) provides the sector an opportunity to harness greater research capabilities within each of the founding institutions – bringing together their different strengths within cybersecurity. Now is an ideal time for a working group to look anew at the current research projects and capabilities and identify long term goals that could support the growth of the cybersecurity sector in the region.
- **Growing the Graduate Talent Pool** – related to above point, there has been a history of collaboration between industry and higher education in the region in terms of shaping degree programmes that support industry requirements. This research project has highlighted that there is a new wave of job growth in the cybersecurity sector expected, pointing to the need to review the higher education programmes for cybersecurity to ensure close alignment with the future job and skills demand.

- **Collaboration with Other Clusters** – the NW's cybersecurity sector is within close proximity to other cyber clusters in the country. Belfast's cyber cluster has Queen's University's CSIT which conducts research into connected devices, ICS, AI applications and is designated an Academic Centre of Excellence in Cyber Security Research. In Galway's cybersecurity cluster, ITAG have supported the cybersecurity sector for many years with HPE as an anchor client. Looking beyond cybersecurity, the region has two tech networks, ICT FinTech (Donegal) and Tech North West (Sligo & Leitrim) with a strong interest in cybersecurity. The different expertise and support available from this wider network should be utilised into to help contribute to the sector's growth.
- **Current Momentum** – recent announcements concerning Tata Consultancy Services' Global Delivery Centre and Advantio's planned cybersecurity operation for Sligo sends a message to other businesses that the region is an attractive place to set up. There is an opportunity to build on this momentum to attract new interest and investors to the region. These investments help reinforce the business case and provide assurance for other investors that the region is a good location option.

CHALLENGES

There are a number of challenges raised by respondents in the course of the research.

- **Weak Local Demand for Cybersecurity Services** – in terms of growing the sector at the local/regional level, the research found low demand for cybersecurity services locally. The findings also indicate that there is weak local demand for investing in cybersecurity systems, solutions and/or training. For the regional cybersecurity operators seeking to expand, this presents a limitation with these companies in a 'wait and see' position.

Many cybersecurity operators suggest growth will need to be stimulated through awareness campaigns and/or subsidy support schemes to stimulate demand.

- **Small Regional Talent Pool** – while some respondents feel the regional talent pool is sufficient, others face a challenge attracting the cybersecurity talent they need – describing it as an obstacle to the achievement of business goals. This challenge is reflected in the survey data which shows that companies are having to source much of their cyber talent from outside the region. The recent uptake in remote working offers employers an opportunity to attract new talent but it also presents a risk of losing experienced talent to higher paying jobs from outside the region. The ability to attract new talent to the region as a key issue to address in order to support the expected cybersecurity job growth.
- **Competition for Investment** – this sector is competitive with the region naturally facing competition from other regions and countries for investment however MNCs continue to be attracted to Ireland for its talent, access to Europe and its cost of doing business. Providing the right education and training and offering support to incumbent cybersecurity operators will be important to ensure they stay competitive globally and the employees are engaged and enabled to perform. In turn, this ecosystem of support will help entice new cyber investment to the region.

SECTION 3

Desk Research

Desk Research

LATEST CYBER TRENDS, ISSUES AND CHALLENGES

Cyber Talent In Ireland

The State of the Cyber Security in Ireland report (2022) from Cyber Ireland found 489 cybersecurity firms operating in the ROI – with a considerable proportion of these large sized firms (44%) and most of these of foreign origin (89%). Ireland has many of the leading cybersecurity organisations and a number of Security Operation Centres operating here. This shows the success in attracting MNC cybersecurity firms to Ireland, with others likely to view this as an attractive location. Dublin, Cork, Galway and Limerick were identified as the main locations, with Donegal (along with Clare, Kildare, Waterford and Louth) identified as locations of note (i.e. areas with 10 or more cybersecurity firms).

The Cyber Ireland sectoral report estimated that there are 7,350 cybersecurity professionals in Ireland and a further 30,000 people with cyber related skills [vii] . The Cyber Security Skills Report 2021 (National Survey) provides an important benchmark and state of play for cybersecurity in Ireland. [viii]

The report highlights:

- Significant skills gaps and skills shortages faced by most organisations.
- Long lead times between a vacancy and a hire (over six months or more).
- Anticipated increases in hiring for cybersecurity roles.
- Increased cybersecurity training to address skills gaps/shortages.
- A move towards AI and automation to manage low complexity cybersecurity work.
- Graduates are often entering cyber roles without the expected skills.

These findings align to other cyber industry reports, and it recommended that organisations move to remote working and innovative learning options to make progress on the skills gaps. It also suggests the need for a European career framework for cyber, cyber apprenticeships and greater investment in diversity programmes to attract more women into the field.

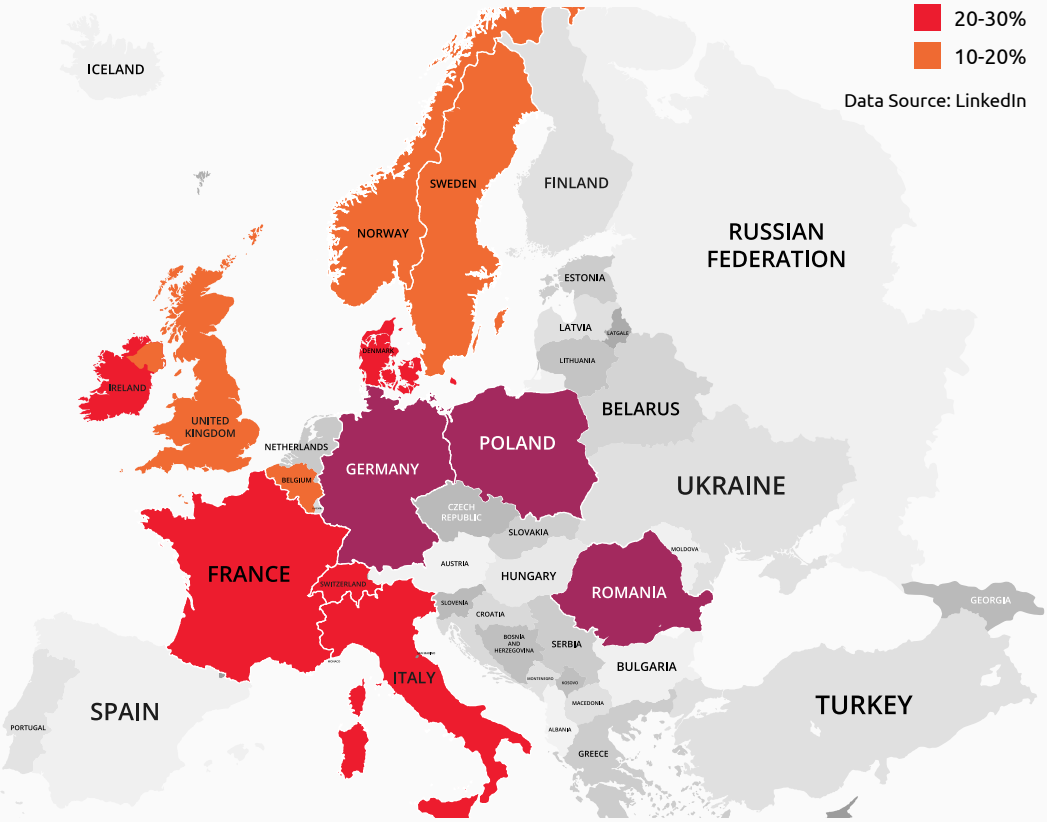
Demand For Cyber Skills

The Expert Group on Future Skills Needs Forecasting Future Demand for High-Level ICT Skills in Ireland report (2019) highlighted that cybersecurity is set to be a key concern for economies and businesses for the foreseeable future as new technologies, market, and societal/consumer trends expand the attack surface for cyber criminals. This is creating demand for offensive cybersecurity systems and services capable of dealing with the growing number of known and unknown threats.

A cybersecurity skills development initiative from Microsoft used LinkedIn data to identify demand for cybersecurity skills globally and found Ireland's demand is growing by 21% year-on-year (see diagram on next page). [ix] In contrast, Cyber Ireland uses, in its sectoral report, a 10% compounded annual economic growth rate to estimate industry, and therefore job growth, which perhaps provides a more realistic job growth ratio.

Demand For Cybersecurity Has increased By 22% over the past year

COUNTRY	PAST YR GROWTH
Belgium	17%
Denmark	21%
France	23%
Germany	32%
Ireland	21%
Italy	24%
Norway	17%
Poland	36%
Romania	31%
Sweeden	18%
Switzerland	21%
United Kingdom	18%



Of note, Microsoft created an online business intelligence tool with this data to also show gender participant ratios within the cybersecurity profession, for Ireland it estimated it to be 21% female to 79% male.

CYBER THREAT TRENDS

The World Economic Forum (WEF)'s Cybersecurity Outlook 2022 proposes that a fundamental driver of increasing cybersecurity threats is the move to e-commerce and the growth in online shopping. [x] Cyber criminals are taking advantage of this and are adopting new technologies to launch more sophisticated attacks in this space, and this is increasingly being directed by criminal (Mafia linked) organisations. It highlights that the dark web is now facilitating the growth of 'hacking as a service' with the easy purchase of hacking software for anyone with an interest.

The WEF found that, on average, companies take **280 days** to identify and respond to a cyber-attack. There is an intensifying race between cybersecurity professionals and criminals to patch (or exploit) the vulnerabilities found in common software. It also found an increasing concern about the cybersecurity of supply chains and organisations are seeking to build cyber resilience (i.e. incident response and recovery systems) underlined by a growing acceptance that cyber defences will not fully protect them from cyber-attacks.

Grant Thornton's eye opening **Economic Cost of Cyber report (2020)** estimated that cybercrime had cost the Irish economy €9.6 billion (up from €630 million in 2014). [xi] This rise is due to increased attacks across all vectors but also driven in particular by the Covid pandemic and the increased remote working. It found the costs associated with ransomware had doubled from €1 billion to €2 billion during that time. A recent report from DataPac revealed that **37% of SMEs experienced a cyber-attack** in 2021 and 86% of business owners are now concerned about being a target of a cyber-crime. [xii]

The **SonicWall Cyber Threat Report (2022)** showed a significant increase in cyber-attacks with ransomware at the top of the list (up 105% on 2020). [xiii] It reported known common vulnerabilities in software reached a new high in 2021, and with digital transformation expanding, the range of software tools companies use looks set to rise again in 2022. It finds cyber-attacks are becoming much more 'ruthless' in targeting infrastructure and key supply chains.

The **Cisco Security Outcomes 2021** Report found that organisations with the strongest security outcomes had invested in the following five key drivers (25 in all were tested); a proactive tech refresh strategy, well integrated technology, strong incident response capabilities, accurate threat detection and prompt disaster recovery. [xiv] This argues that companies need to maintain the investment in up-to-date IT and security technologies and have robust processes needed for detection, response and recovery. This report helps raise a question about the size of the challenge for SMEs in terms of keeping pace with the investment required to keep their businesses secure.

The **Bullet Proof 2021 Annual Report** offered different insights after it conducted a Pen-test/retest exercise and found a quarter of critical vulnerabilities originally identified across their customer base had not been fixed at retest six months later. In another exercise, it put a honeypot (fake) server onto the internet, and it was scanned within milliseconds by malicious actors using automated software. It notes the huge growth in Cloud IT services since the Covid pandemic but raises the issue that this can lead to a false sense of security (even with a shared responsibility model).

Micro Trend's Towards a New Momentum (2022) report makes clear that cyber threats will become increasingly sophisticated in the coming years. In particular, the increased adoption of Cloud SaaS applications will expand the threat landscape: ransomware attacks will move focus from endpoints to servers; the race for zero day exploits will intensify as an increasing number of vulnerabilities are found; 'commodity' ransomware as a service will increasingly target SMEs; hackers will target 'smart' car data; supply chains will remain a key battleground especially as companies look to reconfigure these of late.

Companies and cyber leaders are feeling the pressure as reported in the **EY's Global Information Security Survey 2021**. 77% of the 1,000 CISOs questioned reported a notable increase in cyber-attacks in 2021 and that cybersecurity is now becoming a regular board agenda item. It highlighted three key challenges facing CISOs: underfunding, spiralling regulation and declining influence at the strategic level.

CONCLUSIONS

Recent cybersecurity reports show that the threat landscape is continuing to evolve – driven lately by geopolitical events, as well as technological trends and advancements. Many reports point to large organisations adapting their security posture in response – incorporating newer approaches like zero trust, cyber resilience and security by design. [xv] However, an important issue to draw from these reports is whether the often overlooked SMEs can keep pace with these requirements and challenges – especially important as they are increasingly the focus of cyber-attacks.

LEGAL AND GOVERNMENTAL TRENDS

The 2020 HSE cyber-attack by criminals using Conti ransomware effectively shut down much of the HSE's IT system for a number of months and cost the taxpayer an estimated €100 million to date to recover and repair the damage. [xvi] This common type of cyber-attack caused significant disruption to the HSE's operations and patients' healthcare and was a wakeup call for everyone across the country. [xvii] Since then the Irish government published the **Public Sector Baseline Security Standards (November 2021)** which all public sector bodies now need to achieve. [xviii] However, feedback from this research suggests that many current cybersecurity standards are often beyond the scope of many SMEs, and that one catering to reality of these organisations would help.

The UK government has started supported an initiative to maintain cybersecurity standards with the Cyber Essentials certification programme and so far over 24,000 organisations have completed the programme. [xix] Companies seeking to be a supplier with the UK government must now hold a **Cyber Essentials** certificate, showing a good example of the government working to secure its 'supply chain'. Similar processes also exist in the US and elsewhere.

Relevant to the HSE attack and based on the European Commission's 2020 Cybersecurity Strategy in the Digital Decade, the commission is now updating the **Network and Information Security Directive (NIS)** to create NIS2 which "will impose new requirements on "essential" and "important" service providers in critical sectors, including reporting cyber attacks, implementing security policies, scrutinising the security of suppliers, and proper use of encryption technology. [xx] NIS2 will grant governments more power to enforce the law such as halting operational activities.

Irish government's Public Sector Baseline Security Standards were launched in November 2021

Similarly in the US, President Biden signed a new law called **The Cyber Incident Reporting for Critical Infrastructure Act** on March 15, 2022, making the reporting of a cyber incident and ransomware payments a legal requirement for critical infrastructure owners and operators. [xxi] Companies now have to provide detailed information of the incident within 72 hours (or face penalties).

CONCLUSIONS

The above examples are a snapshot of the increase in cybersecurity legislation and standards being enacted globally. Many governments are fully recognising and prioritising what may be considered an implicit state of cyber warfare against certain state supported actors and criminal organisations. Organisations are facing both increasing threat levels as well as more demanding regulations and standards, particularly if they are part of a critical infrastructure. From this it can be envisioned that the cybersecurity reporting and audits may become routine for most organisations as are financial ones. Cybersecurity looks set to continue to be a strategic challenge and priority investment area for most businesses.

EDUCATION ECOSYSTEM FOR CYBERSECURITY

Atlantic Technological University

The North West region's new university Atlantic Technological University (ATU) has a full range of degree, diploma and certificate level courses covering cybersecurity. These include:

ATU Donegal

- Bachelor of Science in Cybersecurity and Digital Forensic Level 7 & Level 8 Honours.
- Master of Science in Cybersecurity Level 9.
- Master of Science in Cybersecurity Research Level 9.

ATU Sligo

- Bachelor of Science in Computer Networks and Cyber Security Level 7 / 8 Honours.

Nearby at **ATU's Mayo campus** there is a full range of programme options:

- Certificate in Data Cybersecurity Level 7.
- Certificate in Network Cybersecurity Level 7.
- Bachelor of Science in Network Cybersecurity Level 7.
- Higher Diploma in Science in Cybersecurity Risk and Compliance Level 8.
- Master of Science in Cybersecurity Operations Level 9.
- Certificate in Cybersecurity Operations Level 9.
- Online: Certificate or Bachelor of Science in Computer Networks and Cloud Infrastructure Level 8.

Springboard+

In 2022 Springboard continues to offer a comprehensive programme of partially or fully subsidised university programmes aimed at both employees and job seekers focused on cybersecurity:

- ATU Donegal – Postgraduate Diploma in Computing in Cybersecurity.
- ATU Sligo – Certificate in Computer Networks and Cloud Infrastructure (L8).
- ATU Galway – Postgraduate Diploma in Cybersecurity and Software Development.
- CCT College Dublin Diploma in Networking and Systems Security (L7).
- City Education Group – Special Purpose Award in Cyber Security (L7).
- South East Technological University – Higher Diploma in Computer Science.
- TU Dublin – B.Sc. Enterprise Cloud Computing (with Security & Cloud Certifications, L7 add-on).

CYBER SECURITY PROFESSIONAL ACADEMIES

Cyber Skills

Cyber Skills was set up to deliver a range of university level diplomas, certificates and accredited course in cybersecurity. These include:

- Certificate in Secure Network Operations.
- Certificate in Secure Software Development.
- Certificate in Secure Systems Architecture.
- Certificate in Cybersecurity for Business.
- Certificate in Cyber Security Standards and Risks.
- Professional Diploma in OT Security Operations Specialist.

Cyber Skills also offer micro-credential courses covering:

- Secure Systems Architecture.
- Practical Cryptography.
- Log Files and Event Analysis.
- Security Assurance.
- Secure Network Services.
- Cyber Security for Business.
- Secure Network Systems.
- Information Security Architecture.
- Cryptography & Protocols.
- Secure Software Development.
- Cybersecurity Standards & Risk.

Advance Centre

The Advance Centre (Professional Education for Digital Transformation) is a multi-university (UCD, ATU Sligo and TU Dublin) partnership that offers a number of accredited targeted cybersecurity modular and full degree programmes delivered in a blended learning format.

- MSc in Cyber Security.
- Graduate Certificate in Cyber Security.
- Leadership in Cyber Security (module).
- Applied Cryptography (module).
- Risk Assessments and Standards (module).
- Secure Software Engineering (module).
- Information Security (module).
- Cyber Security Law (module).

Both Cyber Skills and the Advance Centre reflect a trend in higher education to offer targeted programmes aimed at helping people upskill/reskill within shorter time frames, as well as prepare IT professionals for a managerial and technical career in Cybersecurity. These types of initiatives can cater to the need to provide 'last mile' training for university graduates to top up practical skills or knowledge gaps on different work-related topics with cybersecurity.

Northern Ireland

In North Ireland (NI) there are a number of education and training cybersecurity programmes on offer from Queen's University Belfast.

- Applied Cyber Security (Master of Science).
- Applied Cyber Security Certificate, Postgraduate.
- Applied Cyber Security with Professional Internship (Master of Science).

The NI government also offer a number of upskill training programmes:

- Cyber Security Academy – a 2 month training programme supported by KPMG.
- Cyber Gateway Aptitude Programme – online cyber labs.

Apprenticeships

A number of apprenticeship programmes are now available for cybersecurity in the ROI:

- In the North West, the Mayo, Sligo & Leitrim Education and Training Board (MSLETB) offer a two year Cybersecurity Apprenticeship programme with training and job placement leading to a Level 6 Advanced Certificate and a number of CompTIA certificates in cybersecurity (also available are Network Engineering and Software Development apprenticeship streams).
- University of Limerick's Cybersecurity Practitioner Programme (NFQ Level 8).

The ongoing skills shortage within cybersecurity suggests that these programmes will need to continue and maintain close alignment with employer investment in entry level, graduate and early career cybersecurity jobs.

CONCLUSION

At the university level, cybersecurity education is now very well served for people seeking to enter or upskill in this area, with over 40 university degrees available (see Cyber Ireland's for a full list of programmes: httpss// cyberireland.ie/course-finder). Greater emphasis may be needed on making available a full range of training options for cybersecurity employees, particularly for those who need to quickly upskill in specific skills areas but are not able to take a longer form degree, diploma or certificate option. The Cyber Skills Development Strategy 2021 report from it@cork Skillnet provides a review of the cybersecurity training providers to this end. [xxiii]

ECONOMIC PROFILE FOR THE NORTH WEST REGION

Business Demographics

Based on 2019 Central Statistics Office (CSO) data below, the counties in the North West region have a higher proportion of employees working in Micro, Small and Medium sized businesses compared to the national average. The Active Enterprise also points to higher proportions in Micro and Small enterprises.

		DONEGAL	SLIGO	LEITRIM	NATIONALLY
	Employees	32,835	11,885	5,466	**1,590,578**
Micro	Under 10	26%	25%	34%	**17%**
Small	10-49	36%	NA	NA	**24%**
Medium	50-249	25%	28%	18%	**22%**
Large	250+	13%	NA	NA	**37%**
2019	**Active Enterprises**	7,978	3,109	1,892	**272,531**
Micro	Under 10	90.8%	91.8%	93.8%	**91.4%**
Small	10-49	8.0%	7.0%	5.5%	**7.0%**
Medium	50-249	1.1%	NA	NA	**1.3%**
Large	250+	0.1%	NA	NA	**0.3%**

Note: some data points not available due to CSO confidentiality rules.

Incomes and Housing in the NW Region

As a potential place for investment, average incomes and housing costs are favourable compared to other regions (recognising that salaries usually driven by industry/sectoral factors). The latest available CSO income data (2019) captures 'earned income' and reveals that the average earnings in the North West region are lower than many regions (see following tables). In particular, average incomes in Donegal are 41% less than those in Dublin. [xxiv]

This may be positive for employers but less so for employees – unless the lower cost of living and ease of access to housing make up the difference for a lower salary. Recent data from Cyber Shark shows that salaries for entry level Cyber Security Analysts are high, at €44,000 gross per annum, about 9% above the national average of salaries. [xxv]

While salaries in the region may be lower, those for cybersecurity salaries are less likely to be so given the demand. The following tables provide ranked information concerning earned incomes and housing prices for the different regions (by county) in the country.

Average incomes in Donegal are 41% less than those in Dublin

The CSO data (2022) for average house prices indicate that the region is very favourable, with Donegal house prices, for example, 70% lower than Dublin's on average (see table below). [xxvi]

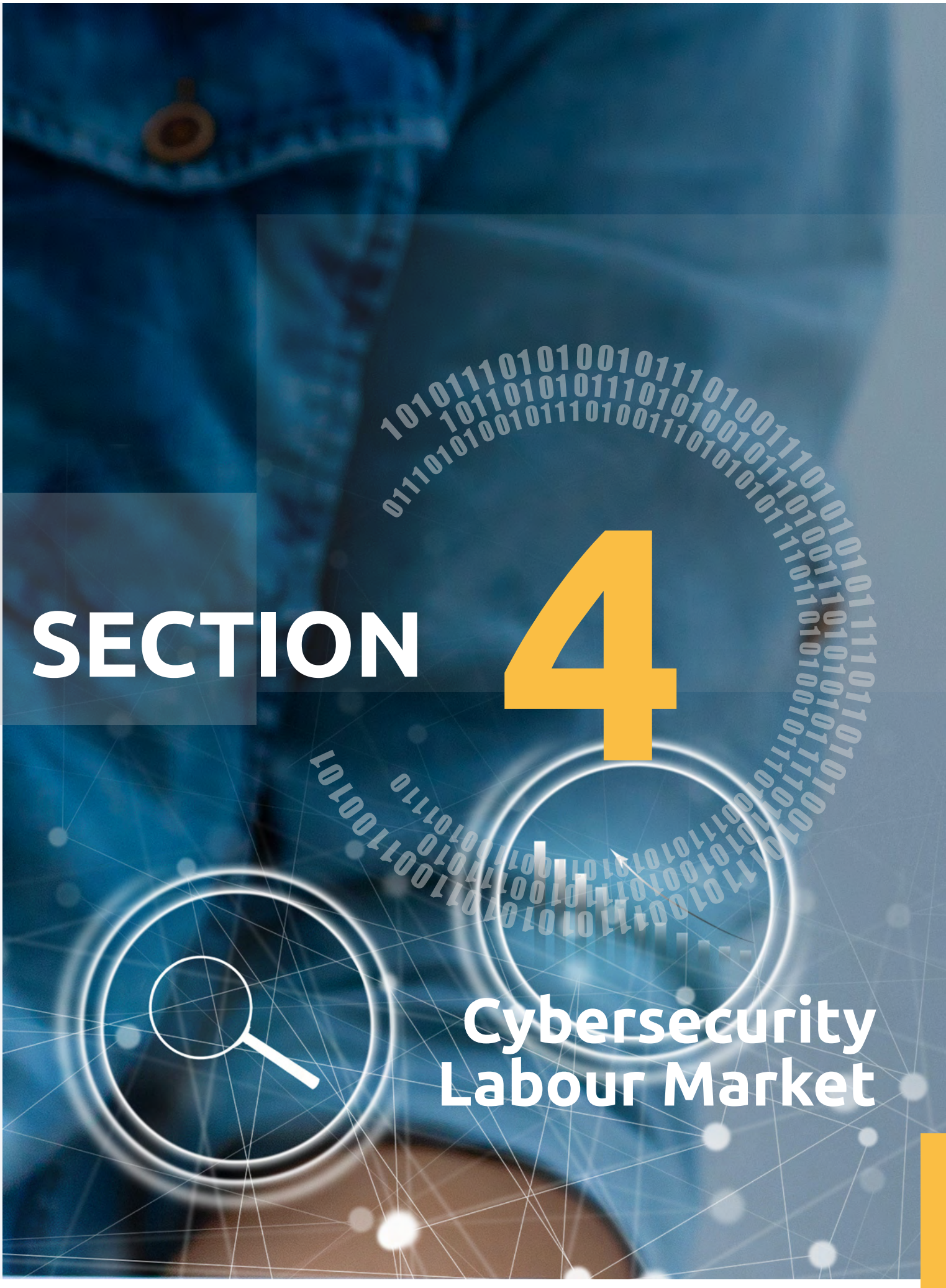
COUNTY	AVE. INCOME PER PERSON 2019	COUNTY	AVE. HOUSE PRICE 2022
Dublin	38,903	Dublin	507,070
Limerick	34,751	Wicklow	434,763
Kildare	34,089	Kildare	344,920
Cork	32,551	Meath	310,344
Wicklow	32,399	Cork County	290,277
Meath	32,001	Kilkenny	255,594
Galway	28,750	Louth	253,279
Waterford	28,655	Waterford County	250,806
Clare	28,592	Galway County	249,766
Louth	28,156	Limerick County	244,453
Carlow	28,032	Wexford	229,414
Kilkenny	27,845	Kerry	220,965
Sligo	27,632	Westmeath	219,092
Kerry	27,161	Laois	217,466
Wexford	26,569	Carlow	216,708
Tipperary	26,503	Clare	214,756
Leitrim	26,153	Offaly	201,813
Monaghan	25,872	Tipperary	192,233
Roscommon	25,847	Monaghan	189,810
Cavan	25,795	Sligo	188,272
Mayo	25,698	Cavan	176,906
Westmeath	24,140	Mayo	174,214
Laois	23,163	Roscommon	155,933
Donegal	23,036	Donegal	154,594
Offaly	22,749	Leitrim	151,599
Longford	22,127	Longford	146,671

Additionally housing stock (Donegal in particular) and regional vacancy rates (across all three counties) compare quite favourable with other parts of Ireland. [xxvii]

RELATIONSHIP TO NORTHERN IRELAND

The Common Travel Area provides ease of access to Northern Ireland and in Belfast there are a number of leading cybersecurity operators (e.g. Avanade, Citi, Cygilant, KPMG, NTT, Rapid7, Synopsis, etc.)[xxviii] Cyber Ireland's sectoral report estimates that there are 2,300 cybersecurity professionals in NI. [xxix]

Belfast is home to the Centre for Secure Information Technologies (CSIT) located in Queen's University – it is focused on innovation and commercialisation of secure information technologies and also specialises in OT/cyber physical security (potentially of help to secure Ireland's manufacturing sector). Commuter distances might not be viable for many so attracting cyber professionals from here may require relocation support and/or a remote or hybrid work option.



SECTION 4

Cybersecurity Labour Market

Cybersecurity Labour Market

Researchers at **Threat Connect** found UK cybersecurity staff turnover to be 20% in 2021 and staff were facing high levels of stress due to increasing threat levels and work demands. [xxx]

Cyber Ireland's national survey found staff turnover for employees with 1 to 3 years of experience to be 50%, pointing to higher turnover rates in Ireland than the UK. The high turnover emphasises the need for companies to keep a strong focus on staff engagement and retention.

The IDA Ireland **Labour Market Pulse** (Edition 5, February 2022) reported a large uptake in remote working of late with one in five jobs postings now offering remote working, up from one in seven one year ago. The uptake of remote working offers the region a way to attract new employees to the region but also poses a risk of losing employees to roles outside. Companies will likely need to consider more just than remote working to attract new talent to the region.

Cyber Shark's **Cyber Security Irish National Survey** identified average salaries for Dublin, Cork and the Rest of Ireland (ROI). It found a clear, but not overly large, differences in cybersecurity salaries between ROI and Dublin/Cork which were 10% to 15% higher. [xxxii] It also reported that cyber professionals are moving jobs for an 18% uplift in salary confirming that salary pressure and staff retention are current issues for most cybersecurity companies.

Cyber Ireland's survey found Irish salaries were 7% higher than the UK's and 35% higher than Northern Ireland's (table below). This presents an opportunity to attract new employees from the UK/NI to Ireland and the North West region.

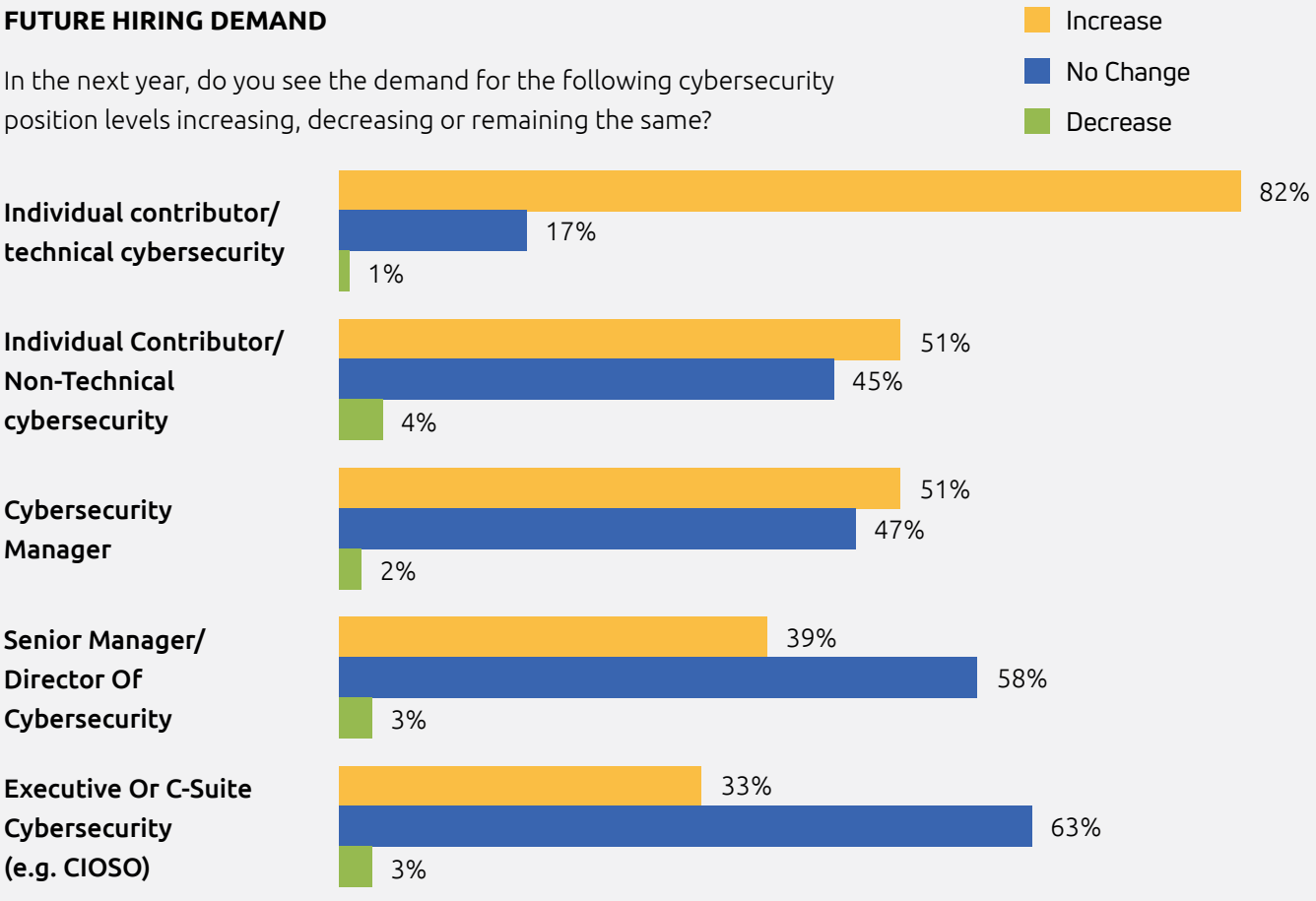
REGION	NO. OF FIRMS (PER100K NATIONAL POPULATION	NO. OF EMPLOYEES	SECTOR REVENUE	SECTOR GVA	AVERAGE SALARY
Ireland	489(9.7) [12]	7,351	€2.1bn	€1.1bn	€75k
Northern Ireland [13]	104(6) [14]	2,299	Not Estimated	£161m (€190m)	£48k (€55k)
UK [15]	1,838(2.7) [16]	52,727	£10.1bn (€11.9bn)	£5.3bn (€6.3bn)	£60k (€70k) [17]

Source: Perspective Economics, Cyber Ireland

A Harvey Nash's **Digital Leadership Report 2021** found that cybersecurity experts are the number one digital skill shortage encountered, with half of the global respondents planning to cross-skill existing staff to address this gap. [xxxiii] **ISACA's State of Cybersecurity 2022** report focuses on talent management in cybersecurity globally and found 82% of the 2,031 respondents are expecting increased hiring demand for cybersecurity professionals (see chart below).

FUTURE HIRING DEMAND

In the next year, do you see the demand for the following cybersecurity position levels increasing, decreasing or remaining the same?



ISACA have reported a tension between employers/ employees over return to office directives which are impacting on the retention of cybersecurity staff – with a **20% increase in resignations** of mid career cyber employees between 2020 and 2021. [xxxiv]

This coupled with the growth in cybersecurity positions is leading to large increases in unfilled and time to fill recruitment rates for staff. It also found that 52% of the organisations list an IT degree as essential for entry level cyber positions but only 27% respondents felt university graduates were well prepared for the cybersecurity challenges companies were facing.

Research from ISC^2 provides some good news with more people viewing the sector as an attractive career option, particularly with the prospects for above average salaries, rapid progression and interesting, fast-paced, purpose driven work. It argues that the tide might be turning in terms of attracting enough talent into cybersecurity. [xxxv] However, it found that although people are becoming more aware of cybersecurity as an attractive career option – it is often much later compared to other career paths, often after they have made key educational choices.

CONCLUSIONS

The cybersecurity talent shortage, staff turnover, and high wages continue to affect the sector – hindering many organisations' ability to defend against cyber threats. Organisations will have to put more investment into recruitment, training and retention initiatives as the demand for cyber staff continues to outstrip supply. For the NW region's employers, they will also need to focus on creating attractive employee / work-life experiences with salaries that compare well to the other regions in Ireland.

Just 27% of companies feel university graduates are well prepared to face cybersecurity challenges

CYBERSECURITY TALENT DEMAND IN THE NW REGION

Job Post Demand

After tracking job postings over the past year on a leading job site, the current demand for cyber employees in the NW region is currently low with 1.2% of the total cyber jobs posted.* However, the start of State Street's cybersecurity centre in Kilkenny shows the impact that one or two anchor clients can make to demand (see below), where Donegal can be expected to move up to a similar position in the next few years.

CYBER JOB POSTING – (% OF TOTAL / COUNT)		
Dublin	67.9%	2804
Cork	11.1%	460
Limerick	9.4%	110
Kilkenny*	2.7%	94
Galway	2.3%	80
Waterford	1.9%	39
Clare	0.9%	29
Donegal	0.7%	26
Carlow	0.6%	21
Sligo	0.5%	13
Kildare	0.3%	9
Roscommon	0.2%	9
Louth	0.2%	8
Kerry	0.2%	7
Tipperary	0.2%	7
Mayo	0.2%	5
Wicklow	0.1%	5
Meath	0.1%	4
Cavan	0.1%	3
Offaly	0.1%	2
Westmeath	0.0%	2
Wexford	0.0%	2
Leitrim	0.0%	1
Longford	0.0%	1
		4,131

* Note: not all employers use this job board site or for all jobs, so the above statistics are not fully representative of all the jobs posted for cybersecurity.

Talent Pool Exercise

In this exercise the two most common 'job types' in cybersecurity (analysts and engineers) were searched using LinkedIn's Sales Navigator to assess the talent pool. The search portal identified a wide range of job titles that span under each and provides an indication of the number of professionals with these titles within a locality.

The summary below compares the NW region to County Dublin and nationally and shows that between 3 to 4% of the country's cybersecurity analysts and engineer professionals registered on LinkedIn are located in the NW region. This highlights the relative size of the NW cyber talent pool and shows the wider talent pool available in Ireland to support the planned job growth in the region in the next few years.

SALES NAVIGATOR EXERCISE – RESULTS (JOBS AND NUMBER OF PEOPLE WITH JOB TITLE)	NW COUNTIES	COUNTY DUBLIN	NATIONAL
Cyber Security Analyst (covering 16 roles): Security Analyst, Information Security Analyst, Senior Security Analyst, Information Technology Security Analyst, Network Security Analyst, Senior Information Security Analyst, System Security Analyst, Security Researcher, Data Security Analyst, Information Assurance Analyst, Senior Information Technology Security Analyst, Senior Information Assurance Analyst, Senior Network Security Analyst, Computer Forensic Analyst, Malware Analyst, Security Operations Centre Analyst	**29**	**333**	**771**
Cyber Security Engineer (covering 20 roles): Network Security Engineer, Security Architect, Information Security Engineer, Security Technician, Senior Network Security Engineer, Information Technology Security Engineer, Senior Security Architect, Cryptologic Technician, Information Assurance Engineer, Senior Information Security Engineer, Information Security Architect, Network Security Architect, Firewall Engineer, Information Technology Security Architect, Security Solutions Architect, Information System Security Engineer, Senior Information Assurance Engineer, Enterprise Security Architect, System Network Security Engineer, Security Operations Centre Architect	**18**	**217**	**451**

CYBERSECURITY FIRMS OPERATING IN THE NW REGION

The research found within the NW region a small number of established firms specialising in cybersecurity; the following is an illustration of these:

CYBERSECURITY COMPANIES IN THE REGION	LOCATIONS	FOCUS
Advantio – consulting and managed services	Sligo	Diversified
Anuview – specialised cybersecurity systems	Sligo/Dublin	Dedicated
CyberRiskAware – online training	Donegal	Dedicated
CyberSecure365 – consulting and managed services	Donegal	Dedicated
Commsec – consulting and managed services	N. Roscommon	Dedicated
Cyberworks – consulting and specialised services	Donegal/Galway	Diversified
ITUS Secure Technologies – full IT consulting and services	Donegal/Dublin	Dedicated
Optum – consulting and managed services for healthcare	Donegal	Diversified
Secora Consulting – cyber consulting and penetration testing	Donegal	Dedicated
Tata Consultancy Services – full IT consulting and services	Donegal	Diversified
Trojan IT – full IT consulting and services	Roscommon	Diversified

The research findings show that the larger cybersecurity operators have clear plans to grow the number of cyber roles in the region while most of the other providers are in a 'wait and see' position – depending on an increase in local demand for cybersecurity services before they expand their cybersecurity teams.

SECTION 5

Summary of the Qualitative Research

Summary of the Qualitative Research

Background

The interviews typically lasted 1.5 hours and examined the following themes:

- Supply and Demand of Cyber Talent.
- Cybersecurity - Future Skills Requirements.
- Cybersecurity Challenges and Opportunities for the North West Region.

26 people, primarily cybersecurity managers, experts or stakeholders involved in the sector, were interviewed offering up a wide variety of views across the themes covered below.

Supply and Demand of Cyber Talent

Most of the people interviewed felt the regional supply of cyber talent is not meeting demand and a focus on expanding the supply is needed to grow the sector. Some commented that the apprenticeship model was not working and/or that graduates were not 'job ready'. Others, in contrast, felt the talent pool and supply of graduates was "quite good". One interviewee highlighted remote working as a risk in terms of drawing local talent away to firms outside the region.

Future Skill Requirements

Most participants were not in a position to precisely define or quantify answers concerning future skills requirements and, for the few that did, these varied widely in terms of the requirements. These ranged from OT security to chaos engineering. However, the one requirement that many agreed upon was the need for cyber awareness for SMEs.

Opportunities and Challenges for the North West Region

This theme drew the most comments. A majority believed there is an opportunity in the region to grow the cybersecurity sector, but they had wide ranging views on what the challenges are. These included government support for cyber, lack of cyber awareness/fundamentals, inaccessible cybersecurity standards, limited networking between organisations regarding cybersecurity, and weak local demand for cybersecurity.

A few pointed to the need to restructure education – moving to something much shorter than a four year degree.

Conclusions

The interviews find that while many see an opportunity to grow the cybersecurity sector, they also point to significant obstacles that need to be addressed regionally to facilitate this growth. In particular, the need to expand the regional supply of talent, improve the understanding and maturity of cybersecurity in the region, and then measures to stimulate local demand for cybersecurity.

SECTION 6

Summary of the Quantitative Research

Summary of the Quantitative Research

Background

The quantitative research surveyed organisations on the following thematic areas for cybersecurity:

- Issues and Challenges.
- Resources.
- Recruitment.
- Skills Development Needs.
- Opportunities for the North West Region.

Over a hundred organisations in the region were directly contacted to participate with 45 indicating willingness to participate. The NW Regional Skills team conducted an engagement exercise over several months to identify, invite, encourage and remind companies to participate in the survey. Of the 45 invited, 25 organisations responded (a 56% response rate). This response provided enough data to report but is not statistically representative of the region's business population.

Two versions of the cyber security skills audit survey were developed:

- A technical survey for organisations with a regional team/operation working in cybersecurity.
- A non-technical survey for those organisations without a cybersecurity team/operation.

SOC1 Analysts, IAM Specialists and Cloud Security Engineers are in high demand

Technical Survey – Key Findings

This survey focused on identifying the technical issues and challenges companies were facing as well as the growth roles and the technical skills gaps to address. There were five survey respondents; all were directors or managers working in cybersecurity. The key findings were:

- There is a clear intention to expand the number of cybersecurity jobs within the region, upwards to 220 SOC1 Analysts, IAM Specialists and Cloud Security Engineers.
- Recruitment is a key challenge to future job growth and support from stakeholders in the region is key to help address this in the short term (e.g. attracting new talent to the region) and longer term (e.g. increasing the supply of local talent).
- Respondents have quite different recruitment strategies and practices (from recruiting primarily within the region to recruiting primarily from overseas) when hiring for cybersecurity roles.
- There are a wide range of technical skills development needs, even among the five respondents, and a further prioritisation exercise is needed to identify which will require external support. This breadth of the training needs reflects the complexity of this sector and the variety of roles and responsibilities within it.
- In terms of interpersonal skills, the responses reveal a range of different requirements however Leadership Development was core across all the cybersecurity operators.

See Appendix 4 for details on the survey findings.

Non-Technical Survey – Key Findings

This survey emphasised cyber preparedness and the challenges and skills gaps that need to be addressed for this. There were 20 respondents for this survey ranging from micro sized to large organisations. Respondents tended to be general or operational managers with some responsibility for cybersecurity.

The key findings were:

- There is a recognition of a growing threat level – most respondents had an incident plan in place and, as of yet, only a few had encountered a serious cyber-attack.
- Respondents felt cybersecurity is a 'somewhat important' consideration for their customers when they are purchasing from them.
- Almost all felt that cyber awareness training (for both employees and managers) was the main skills need and the main area to help organisations defend against cyber threats.
- 15 of the 20 respondents answered that they had no dedicated cybersecurity resources indicating that cybersecurity is often managed as part of a wider role in SMEs.
- Just two respondents were planning to recruit someone with cybersecurity skills in the coming year to enhance and maintain their security.

See Appendix 5 for further details on the survey findings.

Conclusions

Both the surveys provided some key insights and areas to focus on to grow the cybersecurity sector in the region. First, further support is required to improve cybersecurity awareness and maturity of the SME businesses in the region, which is an important prerequisite to grow this sector at the local level. Secondly, the cybersecurity operators are intent on significantly expanding the number of cybersecurity jobs in the region but targeted support from the education ecosystem is needed to help grow the region's talent pool and address the recruitment challenges they are facing. The Recommendation section provides a range of proposals to address these areas.

SECTION 7.

Recommendations

Recommendations

This section provides the Recommendations that have emerged from the research project into three overarching themes:

- **PROMOTING THE NW REGION'S CYBERSECURITY SECTOR** – pursuing the opportunity to grow the cybersecurity sector in the region into a leadership position that attracts FDI and contributes to region's economic growth.
- **CREATING A STRONG CYBERSECURITY CULTURE** – building a strong cybersecurity culture across all sectors and organisations in the region so that the overall business environment has a formidable reputation as one of the safest and securest regions to do business.
- **BUILDING A CYBER TALENT PIPELINE** – creating a clear and targeted focus on developing cybersecurity talent in the region to support and sustain the growth of the sector.

The recommendations are based on findings from the interviews, surveys and desktop research and also the further discussions with the research stakeholders.

PROMOTING THE NW REGION'S CYBERSECURITY SECTOR

- **Regional Promotion Showcase** – to build awareness of and interest in the benefits of operating in the region, a promotion showcase for cybersecurity is needed to help attract new investors and FDI. Working with IDA North West, this showcase would show the region as a stand-out place for locating cybersecurity operations (as well as for living and working in) along with the business case to do so. A stakeholder working group will be needed to define each of the elements (business, government, employee, education and community) and, importantly, formulate a clear vision and strategic plan that shows how the stakeholders are working together to build the region into a leader in cybersecurity.
- **Regional Talent Attraction Campaign** - this is needed in the short term to bring in outside talent to fill some of the more senior cyber vacancies. A 'Come Work in the North West' style campaign and tool-kit could attract new cyber talent to the region (building on initiatives from the Western

Development Commission). This attraction campaign would include individual and business case studies about the growing cyber sector in the region and the benefits of working here. Recruiting organisations and agencies would then make use of this material to support their own recruitment activities.

- **A Review of Cybersecurity Research Projects in the Region** – with the goal of developing a regional research strategy for cybersecurity, it is proposed that a review by academic researchers and industry representatives is undertaken to examine the current focus of research and identify any future areas (regionally and nationally) that could be addressed by the region's academic institutions. Industry would help by contributing potential research topics that could lead to value-adding innovations. A well-developed cybersecurity research strategy for the region would then be an important part of the business case for locating future operations in the NW.

CREATING A STRONG CYBERSECURITY CULTURE

- **Promoting SME Support for Cyber Awareness** - to encourage a proactive approach and enhanced cybersecurity in SMEs in the region it is proposed that an awareness campaign is developed that provides compelling case and clear direction to funding support(s) available to help improve their cybersecurity. For example, Enterprise Ireland offers support via its Digital Transition Fund to conduct an initial cybersecurity needs assessment. This initiative will be a key step to start building a strong cybersecurity culture in the region.
- **SME Cyber Training for Owners/Managers** – following on the previous recommendation, the research highlights the need for targeted cyber awareness interventions that are easy to access and deploy and cover the cyber essentials needed for owners/managers/employees of SMEs. This will include cyber awareness fundamentals and also more advanced options such as vulnerability or maturity assessments. A modular approach will ensure busy owners/managers can take on board the information in a manageable way.
- **Enhancing the NW Cyber Community** – to enhance the sharing of knowledge and best practices in the region it is recommended that a dedicated resource is created to organise and facilitate knowledge sharing, expert talks, meet ups, virtual community and resource tools (both within and across regions). Working with the Cyber Ireland NW chapter and its members there is scope for regional cybersecurity conferences and events to raise cyber awareness across all businesses, schools and the public. This investment will improve cybersecurity awareness and standards and highlight the region as an active and growing cluster.
- **Cybersecurity Standards for SMEs** – to offer SMEs an accessible and feasible route towards achieving a baseline of cybersecurity it is proposed that there are cybersecurity standards are developed catering specifically to SMEs in Ireland. This would involve developing and promoting baseline standards across the region (and nationally) with clear guidance and support on how to achieve these. These standards would focus on offering a pathway to enhanced cybersecurity.

BUILDING A CYBER TALENT PIPELINE

- **Job Readiness Courses for Graduates** – to attract graduates and ensure they are 'job- ready' for cybersecurity work it is recommended that a short form (e.g. 4–6 weeks), practical programme is developed for those seeking entry level role(s) in cybersecurity e.g. SOC1 L1 Analysts. This programme would bring new talent into the sector and support the expected job growth of the key employers in the region. It could be developed into a NW Cyber Graduate programme supported by regional cybersecurity employers delivering ongoing education and skill development for participants into their first few years in the field.
- **Cyber Cross Skilling / Upskilling** - the research found that responsibility for cybersecurity is often part of a dual role (e.g. IT, operations, management, administration, etc.) in SME organisations. To ensure these employees are equipped to handle cybersecurity responsibilities, it is suggested that a targeted programme of courses is available so that these employees are kept skilled in the latest systems, tools, techniques and policies needed to maintain strong cybersecurity. This programme would also facilitate IT employees who want to move into cybersecurity roles. Support from regional Skillnets, ETBs, along with educational institutes like ATU, would ensure broad access and an offering catering to all requirements.
- **University Cyber Career Guidance and Mentoring** – this would target university students in the region particularly those in second year who are considering, or have decided upon, a cyber career. This initiative would deliver career guidance (talks, materials, recruitment events, etc.) across all the educational institutions as well as offer mentoring advice from cyber professionals working in the region. This initiative might include cybersecurity events like Capture the Flag to bring to life a cybersecurity career for students.
- **Targeted Cybersecurity Apprenticeship-type Programme** – to help expand the talent pool for entry level roles it is proposed a targeted, role focused programme is developed with educational and industry partners. This would utilise / build upon the Cyber Apprenticeship offered by the Mayo Sligo and Leitrim ETB, working closely with the region's cybersecurity operators on the curriculum and sequencing that enables both job placement and future progression in the field.
- **Stakeholder Engagement and Co-ordination Strategy** – to ensure there is alignment, coverage and synergies between the different cybersecurity programmes and initiatives put forward for the region, it is proposed that an overarching co-ordination, engagement and sourcing role is required. As this aligns with the objectives of the Regional Skills Forum, it is proposed that Regional Skills North West liaises with the education and training providers (ATU, MSLETB and the relevant Skillnets), employers and other stakeholders (e.g. Cyber Ireland, Cyber Skills, etc.) to bring together a comprehensive offering needed to deliver all education and upskilling requirements to current and aspiring cybersecurity professionals in the region.
- **School Outreach Programme** - to build awareness and attract the next generation of cybersecurity professionals it is recommended that a school outreach programme is created that promotes cyber careers and cyber awareness (both for students and educators). This programme would leverage the different educational outreach currently available (e.g. Cyber Futures, CyberSafe and Webwise) as well as address any needs and gaps that arise after consultation with and delivery within schools.

- **Manufacturing/OT Cybersecurity Training** - to ensure the manufacturing sector in the region and beyond is equipped to address the increasing cybersecurity risks for infrastructure and manufacturing operations, a specific cybersecurity operational technology (OT) upskill programme is developed for firms in these sectors. This would entail both short and long form courses to cover the different roles and responsibilities within these manufacturing environments developed in partnership with the educational and research institutions supporting this sector.
- **Cybersecurity Employment Activation Training** - to help bring into cybersecurity new talent and increase the overall talent pool, it is suggested that the current employee activation programmes continue to be offered and promoted within the region. Support from Skillnet Ireland and Springboard will be key, and any future programmes may be aligned to industry needs to ensure there is a path into cybersecurity for people new to the field.

Case Study

A CASE STUDY ON CLUSTER COLLABORATION

The following case study highlights how a collaborative approach between industry and the educational community can produce compelling results.

HPE in Galway

HPE has been operating in Ireland for over 50 years and has become one of the leading cybersecurity employers in Ireland. The Galway site is now home to the European hub for cybersecurity, called the Cyber Defence Centre. It protects HPE and its customers from cyber threats using emerging Machine Learning and AI technologies.

Over the past decade HPE in Galway has set up a number of talent initiatives to build its cybersecurity capabilities. It works closely with universities (GMIT now ATU) to help inform and sponsor various degree programmes including:

- Certificate in Data Cybersecurity (L7).
- Certificate in Cybersecurity Operations (L9).
- Master of Science in Cyber Security (L9).

Other internal talent attraction, development and retention initiatives in HPE have included:

- A twelve month a job rotation programme.
- A return to work programme.
- Diversity initiatives in talent (e.g. recruits from IT and non-IT backgrounds).
- Cyber outreach programme e.g. Girl Guides initiative.
- Three month internships.
- Bootcamps (three months) for new graduates / early career.
- Participation in an ITAG Skillnet mentorship programmes.

HPE have invested significantly in a range of internal and external talent initiatives and partnerships to help build the cybersecurity talent pool in the county and country.

HPE have recently announced 150 news jobs in Ireland (including in cybersecurity) coming under their 'Edge to Office' initiative which will allow for a mix of flexible working / flexible locations opening opportunities to applicants across the country.

References:

https://www.irishexaminer.com/lifestyle/arid-30951579.html

https://www.siliconrepublic.com/enterprise/cybersecurity-ireland-galway-shannon-companies

https://www.gmit.ie/news/gmit-announces-suite-of-new-cybersecurity-courses-in-response-to-skills-shortage

https://kildare-nationalist.ie/2021/03/31/hewlett-packard-enterprise-announces-150-new-high-tech-jobs/

https://kildare-nationalist.ie/2021/03/31/hewlett-packard-announces-150-jobs-with-flexible-locations-in-ireland/


SECTION
8
Appendices

Appendix 1 – Overall Survey Response Profile

OVERALL RESPONSE PROFILE (FOR BOTH SURVEY GROUPS)

What are the origins of your organisation?

Indigenous Irish	20	Foreign owned	5

What responsibilities do you have for cybersecurity within your organisation? (select those that apply)

No direct responsibility for cybersecurity	6
Cybersecurity strategy	3
Cybersecurity operations	4
Cybersecurity recruitment	0
Cybersecurity training	0
Combination of above	12

What industry is your organisation in? Please select one:

Agriculture (1)	
Construction (2)	
Cybersecurity Vendor (3)	2
Defence (4)	
Financial/Insurance Services (5)	1
Food and Drink (6)	
Healthcare (private sector) (7)	1
Healthcare (public sector) (8)	
Heavy Engineering/Manufacturing (9)	4
Information and Communication Technology/Telecommunications (10)	5
Medical Technology (11)	
Non-Profit (12)	
Pharmaceutical (13)	
Police (14)	
Professional Services (15)	4
Public Services (16)	1
Retail/Wholesale (17)	3
Transportation (18)	
Utilities (19)	
Other (please specify) (20): Education x 2 - E-commerce/web development - Software	

What is the size of your organisation?

Micro (1 to 10 employees) (1)	7
Small (11 to 49 employees) (2)	5
Medium (50 to 249 employees) (3)	6
Large (250 plus employees) (4)	7

Appendix 2 – Technical Skill Development Requirements

Based on your selected development needs in the previous question, approximately how many employees would you expect to undertake training in the skillset area(s)?	Number of employees
AI automation for cybersecurity	10
Asset protection measures	5
Business Continuity / Cyber Resilience	5
Cloud cyber / native security	**30**
Conducting security audits	5
Containerisation	15
Cyber playbooks	**20**
Cyber risk governance	15
Cybersecurity regulations	15
Data Loss Prevention	10
Data Protection / PII / SPI	10
DevSecOps including application security	**25**
Digital forensics	10
Domain specific security e.g. devices	15
Incident response / handling	10
Interpreting malicious code	10
IoT security	10
Linux systems	5
Major incident response planning	10
Malware investigation	10
Managing open source vulnerability	10
Mobile application security	5
Network security	**20**
OT / ICT / SCADA security	10
Penetration testing	**20**
Regulatory compliance	10
Remote working/endpoint security	10
Routing	10
Security architecture	15
Security assessments (e.g. SOC2/Type 2)	10
Security auditing	10
Security frameworks	**20**
Security Operations Centre (SOC)	**20**
Security standards e.g. ISO27001, etc.	10
Supply chain security	5
Systems architecture	10
Threat intelligence	10
User behaviour & activity monitoring	5
Vulnerability management	**20**

Appendix 3 – Current Cyber Roles and Hiring Intentions

Current Roles / Hiring Intentions	Current number of roles	Number of posts to hire in coming few years
Head of Cybersecurity (1)	4	0
Cybersecurity Team Leader (2)	12	0
Cybersecurity Manager (e.g. Head of SOC) (3)	5	0
Cyber Learning & Development Manager (4)	0	1
Cybersecurity Awareness Educator (5)	3	0
SOC Analysts L1 (6)	11	54
SOC Analysts L2 (7)	5	17
SOC Analysts L3 (8)	1	7
Security Architect (9)	3	0
Security Engineer (10)	30+	5
Junior Penetration Tester (11)	11	10
Senior Penetration Tester (12)	9	2
Senior Security Consultants (13)	13	20
Junior Security Consultants (14)	12+	2
Risk and Compliance Officers (15)	7	0
Technical Support / Support Desk (16)	22+	4
Threat Hunting / Intelligence Specialist (17)	5	0
Vulnerability Analysts / Assessor (18)	10	20
Digital Forensic Specialist (19)	0	0
OT Security Engineer (20)	1	0
IoT Security Engineer (21)	1	0
Incident Response Specialist (22)	5	0
DevSecOps Engineer (23)	10	0
Cloud Security Engineer (24)	1	35
IAM Solution Specialist (25)	12	40
IT Governance & Audit (26)	7	0
Security Officers (27)	0	3
Total	**200+**	**220**

Appendix 4 - Technical Survey Summary of Findings

Respondent Profile Breakdown (N5)	
Micro (1 to 10 employees) x 2	Indigenous Irish
Medium (50 to 249 employees) x 1	Foreign owned
Large (250 plus employees) x 2	Foreign owned

SUMMARY OF FINDINGS

This survey was completed by three large, diversified organisations (two with significant cyber resources) and two by smaller cybersecurity consultancies. Together, respondents represent approximately 200 cyber professionals working in the region.

Issues And Challenges

- The top issue respondents felt they needed to focus on (from a list of 18 provided) is cyber risk governance and regulatory compliance (3 of the 5 respondents). This aligns with findings from the desktop research which finds cyber regulation is increasing and becoming a key challenge.
- Two of the five respondents felt cybersecurity was critical for its customers, one rated it important, and two just slightly important.
- Overall, the key issues and challenges for this group tended to be management orientated rather than technical, which may reflect their senior position or a confidence in the company's capabilities to tackle technical challenges.

Resourcing And Recruitment

- Four of the five respondents have an intention to hire additional cybersecurity employees over the coming year or two upwards to 220 new posts (see appendix 3).
- Four respondents reported that the challenge of recruiting was having an impact on the achievement of business goals.
- Notable was the lack of consensus of any particular role being challenging to fill, with each selecting different roles as difficult for varied reasons.
- Respondents are accessing a variety of talent pools (e.g. internal, regional, national, etc.) to help fill positions.
    - The differences are stark in some cases – one respondent recruits almost all its cyber employees from within the region or nearby (Northern Ireland), while another sources about 60% of its cyber employees from outside Ireland.
    - With many similar roles, this difference is worth researching further in terms of their differing needs, expectations and recruitment practices.
- Most respondents use the regional educational institutes to help source employees, but a few noted some technical skill gaps encountered here among graduate recruits.
- There was strong consensus on the value of cyber certificates – with the respondents identifying 12 cybersecurity certificates essential or desirable when recruiting someone (see table on next page).

In Demand Certificates (not ranked)	
1	CCNA (Cisco Certified Network Associate)
2	CCNP (Cisco Certified Network Professional)
3	CCSP (Certified Cloud Security Professional)
4	CEH (Certified Ethical Hacker)
5	CEPT (Certified Expert Penetration Tester)
6	CISA (Certified Information System Auditor)
7	CISM (Certified Information Security Manager)
8	CISSP (Certified Information Systems Security Professional)
9	CompTIA Network+
10	CompTIA Security+
11	GPEN (GIAC Penetration Tester Certificate)
12	OSCP (Offensive Security Certified Professional)

- In terms of gender diversity the results generally reflect the average male/female IT employee ratio statistic of 20%; one company was well above, two were on par and two are slightly below [xxxvi]
- In terms of ethnic/cultural diversity data there was limited information available except to note that three of the five cybersecurity operators were recruiting employees from across the EU, and one employer was recruiting almost half of their cyber employees from outside the EU; this indicates that the current cybersecurity workforce in the region is likely to be highly diverse.
- Two of the five respondents had a diversity programme available to their cybersecurity employees, and given the above point, supporting these programmes is likely to play a positive role in attracting, engaging and retaining cyber employees.

Skills Development Needs

- Just two of the five respondents indicated that they had completed a Training Needs Analysis in the past year (this reflects the low uptake of this practice found in survey reports elsewhere). [xxxvii]
- When presented with 39 technical skills areas to evaluate for training needs, the respondents identified needs across all of these with the top two being Cloud Security and DevSecOps.
- When presented with a menu of transversal/soft skills, four respondents identified an extensive set of development needs, pointing to the growing need for cyber professionals to have more than technical skills to effectively manage incidents and protect their customers.
- A clear consensus from all respondents was the need for Leadership Development.
- In terms of training delivery, respondents indicated that online learning would be a key/ central part of any learning delivery mix.
- Four of the five respondents indicated that certificate linked training was either important or essential.

Opportunities for the North West Region

- All considered it important to grow the sector in the region and four have plans to expand the scale and scope of their cybersecurity function in the region.
- The main impediment to growth is the lack of technically skilled candidates in the labour market.
    - The survey data finds potential key recruitment issues for a number of high demand roles in particular: SOC1 Analysts, IAM Solution Specialists and Cloud Security Engineers.

- In terms of what further support is needed from the wider employer and educational community, the respondents suggested help on a number of fronts:
  - Advice to help compete against the remote working job offers available elsewhere.
  - Increase the number of people entering the sector.
  - Offering more upskilling programmes.
  - More support for recruitment campaigns to bring new talent to the NW region.
- Respondents put forward a number of different strengths of the region:
  - A track record in producing good graduates.
  - Proximity to Northern Ireland (CSIT).
  - Established companies in the region with cybersecurity teams.
  - Low cost of living, attractive work/life balance available.
  - Large employment opportunities and talent that can be developed.

Summary

The respondents indicated a clear intent to expand the cybersecurity sector within the region (with 220 projected new roles in the medium term), with many highlighting the number and type of specific cybersecurity professionals they plan to employ.

Recruitment is the main challenge for future job growth and an area where regional stakeholders need to work together to help address, both for the short term (attracting new talent to the region) and longer term (increasing the supply of local talent).

The extensive range of skills development needs were identified from just five respondents; the likely next steps to involve a prioritisation exercise followed by scoping with educational stakeholders to help address these.

Appendix 5 - Non-Technical Survey Summary of Findings

The following comments and charts highlight the key findings from the non–technical quantitative survey. Twenty companies responded to this survey.

Respondent Profile Breakdown	
Micro (1 to 10 employees)	5
Small (11 to 49 employees)	5
Medium (50 to 249 employees)	5
Large (250 plus employees)	5
Total	**20**

Issues and Challenges

- A high proportion of companies (17 of the 20 surveyed) have a cybersecurity plan in place to manage incidents, indicating most have given this risk some consideration.
- All report that there has been an increase in the cyber-threat level, with 15 reporting a significant increase in the threat level, indicating that most now see the threat to cybersecurity as a reality (and not something that happens elsewhere).
- A minority (8) feel their cybersecurity is critical or important for winning or retaining customers while nine respondents feel it is only slightly important, indicating this issue is just starting to filter down into customer expectations of suppliers.
- 17 respondents indicate they have not yet faced a serious cyber incident, however, almost all identified a need to improve their cybersecurity, with a majority (11) indicating a need to undertake a major upgrade, indicating that companies are starting to recognise the need for an uplift in investment into cybersecurity.

Skills Development Needs

- The majority (16) of respondents were planning on providing cyber awareness training to employees while eight respondents identified cybersecurity training for managers as a need. These are training needs that are likely to be applicable across almost all sectors in the region and corresponds to findings in other similar cyber reports.
- However, only half had a definite cybersecurity training plan in place for the coming year, indicating a lack of preparedness from some to tackle the people factor that underpins most cybersecurity risks.

Resourcing and Recruitment

Most respondents (15 of 20) manage their cybersecurity internally to some degree (i.e. 4 do so in conjunction with a outsource partner), indicating that many organisations need skilled internal resource(s) to manage this issue.

- However, only 3 (of the 15) had a dedicated cybersecurity resource (either part or full time), indicating there is a resource/skill gap for cybersecurity in many organisations or, at best, it is bundled into a wider mix of responsibilities for people in these organisations.
- Of the 12 organisations who manage their cybersecurity internally but lack a dedicated resource, half plan to either hire or train someone to address this in the coming year; the other half plan to contract out any new services/skills they might need.

OPPORTUNITIES FOR THE NORTH WEST REGION

When asked about the cybersecurity opportunities for the region, respondents pointed to offering more solutions and services in the region such as audits, awareness training, vulnerability assessments, turnkey system solutions for SMEs and general risk awareness for businesses. Many respondents indicated they would benefit from being part of a business support network to work collaboratively together to tackle cybersecurity threats.

CONCLUSION

This survey has highlighted that most organisations (particularly SMEs) in the region do not have a dedicated full-time cybersecurity resource – so targeted awareness and upskilling training to those employees with this responsibility (e.g. dual role employees) will be critical to improving cybersecurity within the region.

References

[i] Collaboratory, Cyber Security Training Needs & Skills Gap Analysis in the Fingal Region, Report 2021-22, Dr. Ayuna Murphy (Technology University Dublin/Collaboratory).

[ii] Higher Education Authority (www.hea.ie), Statistics page (https://hea.ie/statistics/data-for-download-and-visualisations/access-our-data/access-our-data-graduates/).

[iii] Cyber Ireland, State of the Cyber Security Sector in Ireland, 2022.

[iv] Cyber Ireland, State of the Cyber Security Sector in Ireland, 2022.

[v] Gartner, Forecast: Information Security and Risk Management, Worldwide, 2020-2026, 1Q22 Update.

[vi] Morgan McKinley, cyber security role salary calculator: https://www.morganmckinley.com/ie/irelandsalary-guide-calculator.

[vii] Cyber Ireland, Ireland's Cyber Security Cluster, Cyber Security Skills Report 2021, National Survey, Carmel Somers and Dr. Eoin Byrne.

[viii] Cyber Ireland, Ireland's Cyber Security Cluster, Cyber Security Skills Report 2021, National Survey, Carmel Somers and Dr. Eoin Byrne.

[ix] Microsoft Official Blog, Closing the cybersecurity skills gap – Microsoft expands efforts to 23 countries, Mar 23, 2022, Kate Behncken, https://blogs.microsoft.com/blog/2022/03/23/closing-the-cybersecurity-skills-gap-microsoft-expands-efforts-to-23-countries/.

[x] World Economic Forum, Global Cybersecurity Outlook 2022, Insight Report, January 2022.

[xi] Grant Thornton, The Economic Cost of Cybercrime report, Ireland 2020,

[xii] Irish Tech News, Datapac survey reveals nearly 90,000 Irish SMEs have had data stolen in the last year Ronan Leonard March 31, 2022, (https://irishtechnews.ie/datapac-survey-reveals-nearly-90000-irish-smes-have-had-data-stolen-in-the-last-year/).

[xiii] SonicWall Cyber Threat Report, Cyber Threat Intelligence for Navigating the Unknowns of Tomorrow, 2022.

[xiv] Cisco Secure, Security Outcomes Study, Volume 2, Maximising the Top Five Security Practices.

[xv] EY, Cybersecurity: How do you rise above the waves of a perfect storm?, https://www.ey.com/en_gl/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm, July 21, 2021.

[xvi] Silicon Republic, What are the future cybersecurity needs in Ireland?, Dr. Lubna Dhirani and Dr Tom Newe, (April 13, 2022), https://www.siliconrepublic.com/careers/cybersecurity-skills-needs-ireland-ul.

[xvii] PWC, Conti Cyber attack on the HSE, Independent Post Incident Review, HSE Board, Dec. 3, 2021.

[xviii] Department of Environment, Climate and Communications, Public Sector Cyber Security Baseline Standards, November 2021.

[xix] Bullet Proof, Annual Cyber Security Industry Report, 2022.

[xx] Politico, Europe's gambit to fight off cyberattacks, https://www.politico.eu/article/europe-gambit-fight-off-cyberattacks/.

[xxi] Rapid7, New US Law to Require Cyber Incident Reports (March 10, 2022), https://www.rapid7.com/blog/post/2022/03/10/new-us-laws-to-require-cyber-incident-reports/.

[xxii] Collaboratory, Cyber Security Training Needs & Skills Gap Analysis in the Fingal Region, Report 2021-22, Dr. Ayuna Murphy (Technology University Dublin/Collaboratory).

[xxiii] it@cork Skillnet, Cybersecurity Skills Development Strategy report, May 2021.

[xxiv] Central Statistics Office, Estimates of Household Income (CIA02), Total Income Per Person, last updated (02/17/2022). https://ws.cso.ie/public/api.restful/PxStat.Data.Cube_API.ReadDataset/CIA02/XLSX/2007/en.

[xxv] https://www.jobted.ie/salary/cyber-security.

[xxvi] Central Statistics Office (CSO), Rolling 12 Month Market-based Household Purchases of Residential Dwellings (HPM07 Moving 12 Month Mean Sale Price – Executions. Last updated (02/16/2022), https://ws.cso.ie/public/api.restful/PxStat.Data.Cube_API.ReadDataset/HPM07/XLSX/2007/en.

[xxvii] CSO, Housing data (2022), https://www.cso.ie/en/releasesandpublications/ep/p-cpr/censusofpopulation2022-preliminaryresults/housing/.

[xxviii] Northern Ireland Cyber Security Snapshot Report 2021, CSIT and Perspective Economics, 2021.

[xxix] Cyber Ireland, Ireland's Cyber Security Cluster, Cyber Security Skills Report 2021, National Survey, Carmel Somers, Dr. Eoin Byrne.

[xxx] ThreatConnect, Cyber Security Under Threat (white paper), 2022 .

[xxxi] Cyber Ireland, Ireland's Cyber Security Cluster, Cyber Security Skills Report 2021, National Survey, Carmel Somers, Dr. Eoin Byrne.

[xxxii] CyberShark Recruitment, Cyber Security Irish Salary Survey, 2022.

[xxxiii] Harvey Nash Group, Velocity - Digital Leadership Report 2021, in collaboration with Cionet.

[xxxiv] ISACA, State of Cybersecurity 2022 (Global Update on the Workforce Efforts, Resources and Cyberoperations), 2022.

[xxxv] ISC^2, The 2020 (ISC2) Cybersecurity Perceptions Study, 2020.

[xxxvi] Women in Tech (www.womenintech.co.uk), https://technation.io/insights/diversity-and-inclusion-in-uk-tech-companies/.

[xxxvii] Collaboratory (Cybersecurity Hub at TU Dublin), Cyber Security Training Needs & Skill Gap Analysis in the Fingal Region-Report 2021-22, Dr. Ayuna Murphy.