CYBER | IRELAND

IRELAND'S CYBER SECURITY CLUSTER

Cyber Security Skills Report 2021

National Survey

Authors:

Carmel Somers

Dr Eoin Byrne

About Cyber Ireland

Cyber Ireland brings together **Industry, Academia** and **Government** to represent the needs of the Cyber Security Ecosystem in Ireland. We aim to enhance the Innovation, Growth and Competitiveness of the companies and organisations which are part of the cluster focusing on the following areas:

Building the Community

Talent & Skills

Research & Development

Business Development

For more information:

www.cyberireland.ie

EXECUTIVE SUMMARY

In 2020, a Cyber Security Skills Survey was conducted with **Cyber Ireland** members to provide a better understanding of the current labour market for cyber security skills in Ireland. Over 80 respondents from industry provided data on: Cyber Security Roles & Certifications, Hiring & Retaining of Staff, Skills & Training, and Gender Diversity Programmes. The results have highlighted strengths and identified challenges, including Cyber security skills gaps (people lacking appropriate skills) and skills shortages (a lack of people available to work in cyber security job roles). These shortages are impacting organisations of all sizes (micro, small, medium and large), across a range of sectors, including indigenous and foreign owned companies. To address these challenges, recommendations are made that need to be jointly addressed by industry, academia and government.

A Growth Sector & Skilled Workforce

The cyber security cluster in Ireland will continue to grow, in line with international trends of a growing cyber security market and demand for talent:

- 62% of organisations **plan to hire in 2021**.
- 82% will hire **technical security staff** and 50% will **hire new graduates**.
- Twenty organisations noted they have **70 open cyber security positions** in total
- 81% of organisations have staff with a **general technical degree,** 50% with cyber security **master's degree** and 11% with **PhDs**.

This bodes well for the growth of the cluster but asks questions of whether the Irish labour market has the skills available to meet this growth and take advantage of international opportunities.

Skills Shortages

Cyber security teams are understaffed and there is evidence of a significant skills shortages:

- 41% of organisations **security teams are understaffed** and a further 5% are **significantly understaffed**.

- 48% of the companies have **open or unfilled cyber security roles.**
- For 19% of organisations it takes **six months or more** to fill a cyber security role
- 43% of cyber security **hires are from outside of Ireland** (28% from Europe and 15% outside Europe),
- **Most difficult roles to fill** are: Security- Engineer, Analyst, Architect, Consultant, Specialist.

Skill Gaps (people lacking appropriate skills)

Skills Gaps were identified as a serious challenge impacting industry.

- 77% of the open (unfilled) cyber security roles are **technical cyber security positions**,
- 34% of respondents cite a **lack of technical skills** as the primary reason for open roles not being filled
- To address skills gaps, 65% have **increased staff training**, almost 30% have increased their **reliance on artificial intelligence or automation** and 25% increased their reliance on **certification** to attest to tactual skill mastery.

Upskilling and Training Plans:

There are significant investments in upskilling and training by organisations:

- 72% have conducted an **analysis of their cyber skills needs**.
- 52% have a **formal cyber security training programme**.
- 32% were **dissatisfied or unsure of the effectiveness** of their training programme.
- Almost all organisations (93%) **support** their employees in **furthering their cyber security education and certification**.

Courses & Graduates

New graduates from undergraduate and short-term courses, in particular apprentice programmes, play a vital role in addressing skills shortages and skills gaps if graduates' skills meet the requirements of industry:

- **Graduates' salaries** in cyber security roles are **attractive** with almost a third earning between €25k-€35k and a third earning between €35k - €45K.

- Over a quarter (26%) of organisations believe **graduates are less qualified** than expected and 5% are **poorly qualified**.
- Only 17% of organisations had a staff member with a **cyber security apprenticeship**

Gender Diversity

The cyber security sector is male-dominated in Ireland and organisations are experiencing difficulties in retaining women:

- 27% of organisations have **all male cyber security teams** and 42% have significantly more men than women.
- 27% of organisations have **difficulty in retaining women** in their cyber security team.
- 30% of turnover is due to "**family situation changes** (e.g. children, marriage)"
- 44% of organisations **don't have a diversity programme** to support women weren't aware if such a programme.

The results have highlighted strengths and identified challenges, including Cyber security skills gaps and skills shortages. These shortages are impacting organisations of all sizes (micro, small, medium and large), across a range of sectors including indigenous and foreign owned companies. To address these challenges, recommendations are made that need to be jointly addressed by industry, academia and government.

Recommendations

The following recommendations have been set out to address the challenges identified through this research:

1. Addressing cyber security skills shortages (a lack of people available to work in cyber security job roles):
   a) **Short-Term:** Organisations are encouraged to adopt **remote working** practices to: a) increase staff retention and b) recruit internationally for technical skill shortages that can't be met locally.
   b) **Medium Term:** Facilitate **industry upskilling** with new and flexible learning pathways through short-term courses leveraging **micro-credentials** and **online learning**.
   c) **Long-Term:** Grow the overall pool of cyber security professionals in Ireland through initiatives to **attract children, students and adults** into cyber security careers.
2. A **Cyber Security Skills Gaps Analysis** is required to identify current and future skill gaps of industry and ensure the continued growth of the sector. The research should include a training needs analysis of industry.
3. Development of a **Cyber Security Career Framework** for Europe to standardise roles, competencies, and skills for individuals, employers and training providers in cyber security.
4. Organisations to **evaluate their internal training plans** and the degree to which it is meeting the needs of the security team and the broader organisation.
5. Increase adoption of the **Cyber Security Apprenticeship programme** to address skills shortages and assessment of the challenges for industry in taking on apprenticeships.
6. Further investigation to ascertain are enough **entry level cyber security roles** available and what **skills graduates are lacking** for entry level roles.
7. Support the **attraction, retention and advancement of women** in cyber security with a **Diversity Survey** to assess equity, inclusion and diversity in the cyber sector in Ireland.

This survey is a starting point to benchmark the cyber security skills landscape in Ireland. However, a larger, more in-depth study is required, expanding to include companies outside

of the cyber security cluster to give a full picture of the cyber security needs of organisations across all sectors of the economy. This further research should be conducted by a suitable national organisation and funded appropriately.

INTRODUCTION

Cyber Security Cluster & Talent

Cyber security is critical for all sectors of our economy and is inextricably linked with our national security and the smooth functioning of society. It impacts far beyond 'tech' companies. From healthcare, power grids and telecoms to retail industry and SMEs, every industry faces cyber security threats. This is further compounded due to the impact of COVID-19 with companies moving to remote working overnight and all facets of society becoming increasingly dependent on digital technologies. At a national level, ensuring a ready supply of cyber security skills is critical to protecting critical national infrastructure, government, businesses and citizens alike. Meeting this demand requires not only the training of new entrants but the encouragement of cross training and upskilling from professionals in ICT and other relevant sectors.

The cyber security industry employs over **7,000 people** in Ireland, and it is estimated that almost **30,000 professionals** have Cyber security related skills. Ireland has become a global location for cyber security MNCs, including five of the top ten worldwide security software companies, as well as cyber security operations centres (SOCs) and teams across a diverse range of sectors including ICT, financial services, telecoms, manufacturing and healthcare. The top factor for companies in locating their cyber business in Ireland is access to **specialised skills**[1]**.** Several cyber security MNC operations began in Ireland through the acquisition of indigenous companies, and there is a vibrant and growing indigenous sector exporting internationally. It is critical to have a strong pool of cyber security talent to support indigenous cyber security companies to scale, innovate and compete globally.

International Skills Shortages

Internationally there are reports of a severe shortage of cyber security professionals with estimates of a global shortfall between 1.8 and 3.5 million security professionals within five

[1] See: https://www2.deloitte.com/ie/en/pages/risk/articles/cyber-opportunity-analysis-report.html

years (EY's Global Information Security Survey 2018-2019[2] & Cyber Ventures[3]). According to international research, organisations are experiencing skills shortages, are struggling with skills gaps and access to talent. This is impacting organisations of all sizes and sectors, even the most well-resourced sectors and organisations are struggling to recruit the expertise they need.

- ***EY's (2018) Global Information Security Survey 2018-19***[3] reports that 30% of organisations are struggling with cyber security skills shortages (placing the issue ahead of budgetary constraints, cited by 25%). The situation is particularly acute in smaller organisations.
- ***ISC²'s (2018) Cybersecurity Workforce Study***[4] indicated 63% of organisations reporting a skills shortage, with a third of these categorising it as significant.
- ***Enterprise Security Group's annual survey***[5] of the challenges facing IT professionals has consistently cited a 'problematic shortage' of cyber security skills as its top challenge, with a year-on-year increase in the issue.
- ***Stott and May's (2020) Cyber Security in Focus***[6] reveals that leaders are still struggling with the skills gap and access to talent; 76% of respondents believe there is a shortage of cybersecurity skills in their company and there is no improvement from the previous study in 2019.
- A ten-year longitudinal study carried out by **the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA) (2020)**[7] of professionals reveal that cybersecurity skills continue to deteriorate for the fourth year in a row, affecting over 70% of organisations and putting their operations at risk.
- Furthermore, the technology sector is male-dominated and reports estimate the percentage of women in the cyber security industry is now 24%, a marked increase

[2] EY (2018), Global Information Security Survey 2018 – 2019, https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/GISS-2018-19-low-res.pdf
[3] See: https://cybersecurityventures.com/jobs/
[4] See: https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx
[5] See https://www.esg-global.com/blog/the-cybersecurity-skills-shortage-is-getting-worse
[6] See https://resources.stottandmay.com/cyber-security-in-focus-2020
[7] See: https://www.esg-global.com/esg-issa-research-report-2020

on previous figures ((ISC, 2019) [8], however, the percentage of women in cyber security roles is believed to be a smaller.

Presently, there is limited skills data specific to cyber security for Ireland and this provides a challenge in understanding the current skills landscape, the needs of industry and where there are challenges. In 2018 and 2020, the UK Government carried out quantitative and qualitative research to better understand the current state of the UK cyber security skills labour market. The work forms part of the UK Government's National Cyber Security Strategy (2016 – 2021), which is investing £1.9 billion under the strategy, to ensure the UK has a sustainable supply of home-grown cyber professionals. If Ireland aims to be a leading location for cyber security talent, innovation and solutions in Europe, similar research is required to understand the Irish cyber security skills labour market and investment in developing a sustainable supply of cyber security talent.

Initiatives Addressing Skills Shortages in Ireland

Although we do not have up to date cyber security skills data, there are a number of initiatives that are already addressing industry skills needs in Ireland. These include higher level education courses to entry level and conversion courses, and initiatives supporting students and women:

- There are a range of courses from entry level to post-graduate level in education and training boards and higher education institutes nationwide; Cyber Ireland has **mapped over 150 courses** that can lead to a cyber security career[9], including 16 Masters level courses in cyber security.
- In 2020, fourteen new cyber security courses in Higher Education Institutes (HEIs) were funded by government under the Human Capital Initiative (HCI) Pillar 1 and Springboard to address industry skill needs.
- Furthermore, under the HCI Pillar 3, an innovative and collaborative project, CYBER-SKILLS, received €8.1 million in funding to address the skills shortages in the cybersecurity sector. The project is led by Munster Technological University and will

[8] See: https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx
[9] See: https://www.cyberireland.ie/course-finder/

be coordinated nationally across University of Limerick, Technological University Dublin and University College Dublin, with Cyber Ireland the industry partner.

- In October 2018, the Cybersecurity Skills Initiative (CSI) was launched by Skillnet Ireland to develop awareness, bridge the skills gap and to set standards for skills and competencies for Cyber Security roles. The three-year plan will deliver cyber security training to over 5,000 people including training and accreditation to address skills gaps, attracting more young people, and in particular women into the sector and promoting Continuous Professional Development.
- A 2-year Cyber Security Apprenticeship (QQI level 6) was launched in February 2019 in Cork and Dublin, delivered by Fastrack to Information Technology (FIT).
- Cyber security conversion courses supporting job-seekers are available such as CyberQuest, launched in 2021, and ITAG Skillnet's Online Cyber Security Conversion, launched in 2020.
- Lost Summer Bootcamp is a 4-week structured programme for those third-level students missing out on cyber security internships in 2020.
- Cyber Women Ireland (CWI) was launched in 2019 to encourage the advancement and capacity of women involved in all aspects of the Irish cyber security sector and community, through the exchange of information and the cultivation of productive relationships. CWI runs regular meetings and has piloted a mentoring programme in 2020.

RESEARCH OVERVIEW

About this Research

Cyber Ireland's mission is to enhance the Innovation, Growth and Competitiveness of the companies and organisations which are part of the cluster to support Ireland in becoming a global cyber security leader. To ensure Ireland's cyber security sector can grow, compete internationally and companies can protect their business and customers, we need a better understanding of the cyber security labour market, the types of roles, certifications and qualifications required, skills shortages and skills gaps. If Ireland is to be a leader for cyber security talent, we need to be a leader in ensuring career opportunities and progression for women and people from all backgrounds.

Research Objectives

This is the first Cyber Ireland skills survey, which aims to understand:

1. **Where** the current skills, skills gaps (people lacking appropriate skills) and skills shortages (a lack of people available to work in cyber security job roles) are across Cyber Ireland members;
2. **The effects** of the cyber security skills shortages and skills gaps;
3. **The skill needs** organisations are challenged to meet through training and recruitment;
4. **Gender diversity** and inclusion programs in the cyber security industry; and
5. What are the necessary **recommendations for Government, Academia and Industry** to address skills gaps and shortages.

This survey will provide better quality data, representative of the Irish labour market, which is not available presently, in the following areas:

- Cyber Security Roles & Certifications
- Hiring & Retaining Security Staff
- Skills & Training
- Gender Diversity Programmes

Results will be published on Cyber Ireland's Website: https://www.cyberireland.ie

Methodology & Evidence Review

Existing literature and reports on cyber security skills gaps and shortages internationally were reviewed. Key reports consulted were:

- Ipsos MORI (2018), 'Cyber security skills in the UK labour market 2020: findings report,' Research report for the Department for Digital, Culture, Media and Sport.[10]
- ISACA (2019), 'State of Cybersecurity 2019: Current Trends in Workforce Development.'[11]
- ISC^2 (2019), 'Cybersecurity Workforce Study[12].
- The EY Global Information Security Survey 2018-19

Industry Survey

The survey was distributed during the summer of 2020 to Cyber Ireland members. The companies included in the study are part of the Cyber Security Cluster. These companies are deemed to provide cyber security products and/or services, or are companies with a need for cyber security expertise. In particular, companies with cyber security operations (Cyber Security Companies and SOCs) and organisations managing or running their own cyber security activities. The survey was targeted at the most senior person responsible for cyber security in the organisation.

The survey comprised of **forty-one questions** covering five main areas:

1. General questions designed to capture the demographics of the survey respondents.
2. Questions aimed at understanding the most prevalent cyber security roles, qualifications and skills in the industry.
3. Challenges with cyber security recruitment.
4. Investments in training and development.
5. Questions related to gender diversity in the sector.

[10] See https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020
[11] See https://cybersecurity.isaca.org/state-of-cybersecurity
[12] See https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study

The questionnaire consisted of closed questions, including predefined answers offering respondents the possibility to choose and rank among several options or the possibility to grade on a five point "very low" to "very high" Likert scale. Open-ended questions were used to improve the interpretation of the survey's overall results and provides additional valuable insights.

The survey was conducted over a six-week period, having been issued on 15th July, 2020 and closed 28th August, 2020. All Cyber Ireland member companies were notified and provided with a link to the survey requesting their participation. In addition, the survey was advertised nationally through a number of channels.

Recommendations Workshop:

A workshop was conducted in December 2020 with the participants of the survey to present the survey results and gather industry feedback to input into the recommendations. This allowed for further investigation of results and for industry to highlight challenges relating to cyber security skills, recruitment, retention and training. The workshop feedback was recorded and incorporated into the conclusions and recommendations of this report.

Research Gaps:

This primary research is specific to Cyber Ireland members and focused on the cyber security cluster. A larger study is required to assess cyber security skills across all sectors of the economy. Furthermore, due to the relatively small sample size, we can't break down the findings by organisation size and sector to perform a statistical analysis. The results are not sampled or weighted to be representative. The research does not assess specific skills gaps for the respondents, which requires a larger, more in-depth survey.

Acknowledgements:

The authors would like to thank all the organisations and individual research participants who took part in the survey and recommendations workshop. Thanks to those who inputted into the development of the survey and the survey recommendations, in particular the support of the Cyber Ireland Talent and Skills Working Group.

SURVEY FINDINGS

Section 1: Respondent Demographics

We asked that organisations choose the person most senior person responsible for their cyber security operations to complete the survey. The size of organisations was split into micro (1 to 9 employees), small (10 to 49 employees), medium (50 to 249 employees) and large organisations (250 employees or more). The survey was completed by 81 respondents representing the following organisation types (Figure 1):

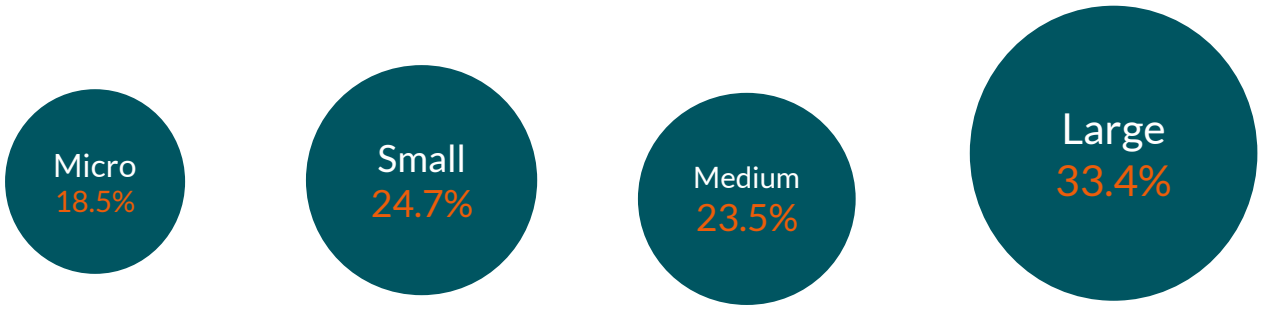

Figure 1: Respondent Organisations Size

Of the 81 respondents 52% are from Irish-owned organisations and 48% are from foreign-owned organisations.

Industry Sector

The majority of organisations are from the Cyber Security (49%) sector, with the remaining respondents coming from a diverse range including ICT (10%), Financial Services (7%) and Professional Services (7%), and other sectors.

Security Resources

Over 56% of respondents have their cyber security team staffed by employees of the organisation, for example MNCs may have their international cyber security operations centres based in Ireland. Almost one third (30%) of the surveyed organisations have a mix of outsourced and internal employees making up their cyber team and 10% are cyber security providers (Table 1).

SECURITY RESOURCES ARE SOURCED AS FOLLOWS:	
Cyber Security Provider	10%
Security resources are outsourced (managed service provider)	4%
Security resources are employees	56%
Mix of outsourced / employees	30%
Other (please specify)	1%
TOTAL	

Table 1: Where the Organisation sources its Security Resources

Cyber Security Team Size

Organisations were asked the size of their cyber security team, within the overall organisation. These ranged in size from small teams consisting of less than 5 cyber security professionals making up 33% of responses, teams with 6 to 20 people representing 26%, 20 to 100 people making up 24%, and 11% of organisations had over 100 cyber security professionals in their operations in Ireland.

Section 2: Roles and Certifications

Cyber Roles

The survey provided a list of seventeen cyber security roles and there is a significant spread of selection by the respondents across all of these roles, though the four most common are, cyber analyst, architect, engineer and consultant (Figure 2). In addition, respondents contributed twelve other cyber security roles in their organisations that were not listed.

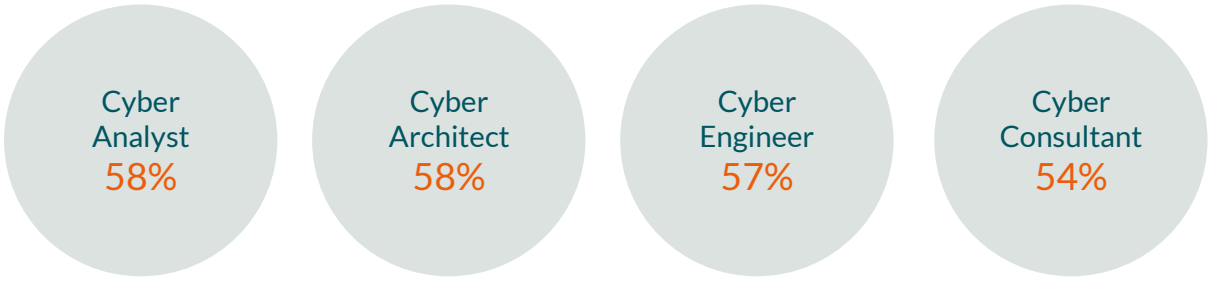

Figure 2: Most Common Cyber Security Roles

Qualifications & Certifications

The cyber security workforce in Ireland is highly qualified. Over four-fifths (81%) of organisations responded that their staff have a general technical degree (Computer Science, Engineering or Information Systems) with 41% having a specialist cyber security degree (41%). Fifty percent of organisations have employees with a cyber security master's degree and 11% have PhDs. Companies who had a staff member with a cyber security apprentice totalled 17% (Figure 3).

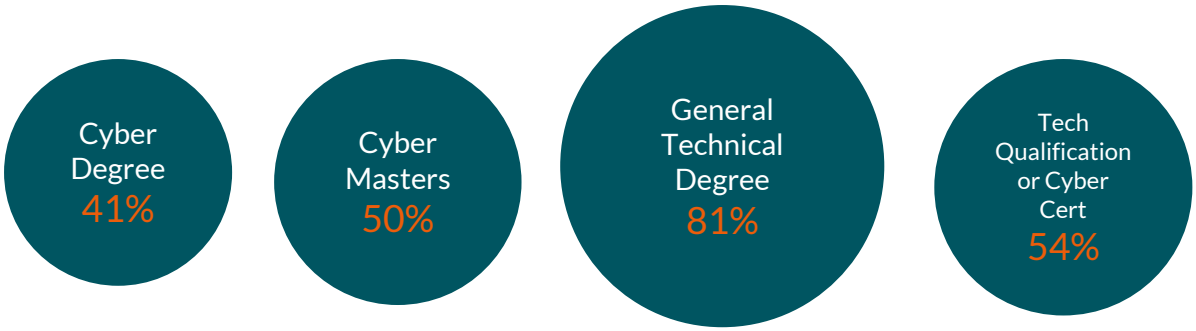

Figure 3: Most Common Qualifications of Cyber Security Staff

Looking at the most common cyber security certifications from respondent organisations, Table 2 displays the percentage of organisations with staff with the following certifications:

CISSP	**62%**
CompTIA	46%
CISM	42%
CEH	40%
CISA	34%
ISO2701	32%
Other Certification	40%

Table 2: Most Common Certifications

Twenty-four certification options and an "other" option was presented as part of the survey. Respondents noted an additional 19 certifications that staff had in their organisations. The result indicates a significant fragmentation in the market for cyber security certifications.

Respondents were also asked about the importance of additional skills not covered through qualifications or certifications, such as 'soft skills'. Over 90% of the following skills were judged to be important or very important:

- Oral and written communication skills
- Teamwork skills
- Critical thinking skills
- High-level technical skills such as incident response.

While over 80% considered an understanding of legal and compliance issues such as data protection to be important or very important. It is likely that there is a focus on legal and compliance issues in general, as a result of the General Data Protection Regulations (GDPR) which came into force in May 2018.

Section 3: Hiring & Retaining Staff

Hiring

The survey examined how organisations approach recruitment, retention and skills shortages. There are various routes for organisations to hire cyber security staff and likewise pathways for staff into cyber security roles. Table 3 shows that almost three-quarters of respondents recruit new cyber security staff from a previous role in cyber security, while 56% recruit from within the organisation and 53% hire entry level recruits which could be a graduate or an apprentice. There are opportunities for people coming from other roles as 41% hire from non-cyber security related roles.

WHERE DO YOU SOURCE YOUR CYBER SECURITY STAFF	
Recruited from a non-cyber security related role	41%
Recruited from a previous cyber security role	74%
Internal organisational move (staff redeployment / repurposing)	56%
Career Starter, graduate or apprentice	53%

Table 3: Where New Hires are Sourced From

Respondents were asked where they hire for cyber security roles. It was found that 57% are hired from Ireland, 28% from Europe and 15% internationally (outside Europe), indicating potential skills shortages or skills gaps in the Irish labour market

Fifty-five percent of respondents note that hiring for a cyber security role takes between two and three months, however, almost one-fifth (19%) of respondents highlighted that it takes six months or longer to hire a qualified cyber security recruit. This aligns with international research that also identified challenges around the time it takes to hire for cyber security roles.[13]

Based on respondent feedback, 39% have no specific cyber hire type and hiring is dependent on need at a given time. Twenty-six percent confirm the majority of hires have 1 – 3 years'

[13] ISACA (2020), State of Cybersecurity 2020. See https://www.isaca.org/go/state-of-cybersecurity-2020

experience, with over a quarter (27%) percent typically hire cyber security professionals with more than three years' experience. Only 8% of respondents state they are primarily hiring at graduate level.

Graduate Salaries

Graduate salaries in the main fall into two salary ranges: 31% of respondents hire graduates for cyber security roles between €25k - €35k, while a further 31% pay salaries between €35k - €45k. Fifteen of organisations pay graduate salaries over €45k. These attractive salaries should attract top students into the cyber security field. The difference in graduate starting salaries may be indicative of pay scales variation between micro, small and medium enterprises versus multinationals. Increased demand for top graduates and specific technical skills has led to increased salaries. Brightwater's[14] salary research noted cyber security analysts had pay increases of up to 20% in 2019 and expected this trend to continue in 2020.

Growth Sector

When asked if organisations will be hiring for cyber security roles next year, in 2021, sixty-two percent indicate they will, fifteen percent indicate they won't and twenty-three don't know what their hiring requirements will be (Figure 4). It is encouraging to see this growth given the survey was conducted amid the Covid-19 restrictions, which is impacting on jobs and the economy. With 62% of organisations planning to hire for cyber security roles in 2021, this will continue to put pressure on limited available resources.

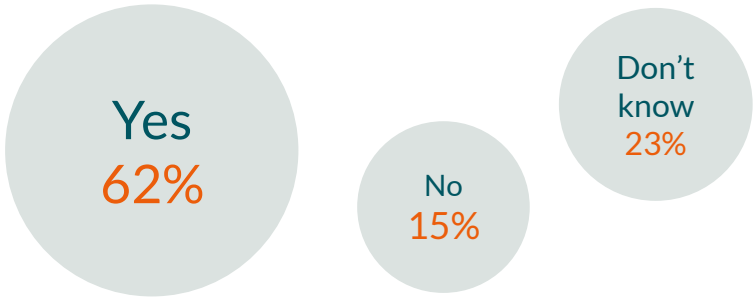

Figure 4: Organisations planning to grow their cyber security team in 2021

[14] Brightwater Salary Survey, 201
9 https://www.brightwater.ie/docs/default-source/surveys/salary-survey/2019/brightwater-survey-salary-2019.pdf?sfvrsn=bd528376_0

Of the organisations planning to hire in 2021 the majority of respondents (82%) will hire for technical cyber security roles, 50% will hire for graduate level cyber security roles and 22% will seek to hire Cyber Security Managers (Table 4).

CYBER SECURITY ROLES TO BE HIRED IN 2021:	
Graduate	50%
Technical cyber security	82%
Non-technical cyber security	12%
Cyber security manager	22%
Senior manager / Director of cyber security	20%
Executive or C-suite cyber security (e.g. CISO)	2%
TOTAL	

Table 4: Cyber Security Roles to be Hired in 2021

Suitability of New Hires

In reviewing how well qualified cyber security applicants are for the cyber security positions they apply for, in general candidates are qualified for their role (Table 5.) For more experienced roles, the candidates available match the expectations for the employer. However, for graduate roles, 25% are less qualified and 5% are poorly qualified for roles in cyber security. This is broadly in line with sentiment in the industry globally that graduates lack good communication skills, proper understanding of security architecture, awareness of risk as a discipline, project management knowledge, and critical thinking skills. On the other hand, it should be assessed whether industry is adequately determining the kind of experience, education and capabilities needed for a given security role and the renumeration for the role to attract the right quality of candidates.

QUALIFIED FOR THEIR ROLE?	Poor Qualified	Less Qualified	Neutral	Qualified	Well Qualified
Cyber Graduate	5%	26%	36%	29%	3%
Cyber Specialist (over 3 years' experience)	0%	10%	39%	46%	5%
Senior Cyber Specialist (over 10 years' experience)	0%	5%	22%	48.%	24%
Cyber Security manager	0%	7%	40%	37%	16%
Senior manager / Director of cyber security	0%	7%	36%	35%	22%
Executive / CISO	2%	2%	40%	31%	25%

Table 5: How Qualified are Various Cyber Roles

Staffing Levels & Shortages

Worryingly, over 42% of respondents asses that their cyber security team is somewhat understaffed and 5% are significantly understaffed, with 43% of organisations appropriately staffed. That is, the cyber security function in that business does not have sufficient staff to carry out those day to day tasks required for the organisation to be cyber protected.

Cyber security teams may be understaffed due to open vacancies, an inability to recruit the right candidates, competition for skills, or salaries may not match the expertise required. When asked whether the organisation has unfilled, or open, cyber security positions, 49% of respondents had open roles at the time. These indicate serious skills shortages and skills gaps in cyber security in Ireland. Table 6 presents the roles that are most difficult to hire for by percentage of organisations' responses.

Security Engineer	28%
Security Analyst	24%
Security Architect	24%
Security Consultant	24%
Security Specialist	19%

Table 6: Most difficult roles to fill

This aligns with cyber security roles data from the CyberSeek.org project backed by the NICE (National Initiative for Cybersecurity Education) Cybersecurity Workforce Framework[15], which identifies the top five cyber security positions organisations in the USA are hiring for are:

1 Cybersecurity Engineer is the most in-demand security position for 2020, this is an intermediate to advanced-level position in most organisations
2 Cybersecurity Analyst role is the second most in-demand security position in 2019 and again in 2020
3 Network Engineer/Architect is an advanced-level position requiring 5-10 years professional experience
4 Cyber Security Consultant is a position which is typically not employed by in-house security teams but usually is a self-employed contractor or works for an external or third-party security consulting firm

Respondents note the primary reasons these open roles are difficult to fill is due to "Candidates lacking the desired attitude, skills, qualifications or experience" according to 49% of respondents, 42% note "too much competition from other employers", 39% note a lack of candidates generally (skills shortages), 37% consider that "candidates lack the required attitude, motivation or personality" and 34% highlight that candidates lack the desired technical skills (skills gaps). Of the open (unfilled) cyber security roles in the respondent's organisations, seventy-seven percent are technical cyber security positions.

[15] CyberSeek.org project backed by NICE https://www.cyberseek.org/

Staff Turnover & Retention

Turnover and retention of staff in cyber security roles is a challenge for industry, seen in Table 7. However, staff turnover rates did not increase significantly when 2019 rates are compared to 2018.

STAFF TURNOVER	No Turnover	Less than 25%	25% - 50%	51% - 75%	76% - 100%
2018 – Indictive %	40%	45%	13%	0%	2%
2019 – Indictive %	39%	43%	13%	4%	2%

Table 7: Staff Turnover in 2018 and 2019

Staff turnover has primarily occurred in the 1 to 3-year career timeframe with respondents acknowledging 50% turnover in this category. The next largest turnover is in the 4 to 10-year career timeframe with 39% turnover. Those in the 11 to 25-year career timeframe represents 18% of turnover across the organisations surveyed. In exploring the reasons for staff turnover, the key issues highlighted by organisations are:

1. 75% cite "better financial incentives (e.g. salaries, bonuses)"
2. 58% declare "promotion and development opportunities" are the key turnover factors
3. 30% highlight "family situation changes (e.g. children, marriage)" as the primary reason for staff turnover in the cyber security team.

A number of organisations have employed successful initiatives to increase staff retention, the most popular of which are:

1 Improved flexibility and remote working,
2 Internal training programmes, paid courses and education,
3 Developing career pathways and progression,
4 Supporting a strong culture, and
5 Financial incentives.

Section 4: Skills & Training

Training Needs

In the past twelve months, 72% of organisations have undertaken an analysis of their cyber security skills or training needs, however only 52% have a training plan in place. Of those with a training plan, 32% acknowledge that their training plan falls below being effective. The most in-demand areas of formal training identified are displayed in Table 8.

Cloud-enabled cybersecurity	63%
Incident Response	47%
Soft Skills (leadership, teamwork, communicating to persuade/educate)	45%
Regulatory Compliance	43%
Risk based Frameworks	40%

Table 8: Most In-Demand Training Areas

Training Supports

Of those organisations surveyed, 93% support their employees in gaining security training and certification, which supports the continued growth and development of the industry and helps reduce skills gaps. Seventy percent of organisations have an employee working towards, or planning to gain, formal qualifications or certified training in cyber security.

In an effort to reduce cyber skills gaps, 65% have increased staff training, almost 30% have increased their reliance on artificial intelligence or automation and 25% of respondents increased their reliance on certification to attest to tactual skill mastery. Only 10% of organisations had no initiatives to help decrease cyber security skills gaps.

Section 5: Gender Diversity

Cyber security teams in Ireland are made up of predominantly men. Over a quarter (27%) of organisations surveyed have an all-male cyber security team, 42% have significantly more men than women and 22% percent have somewhat more men than women.

In regard to challenges retaining women in cyber security roles, 47% haven't had difficulty, but for 27% it has been problematic. Forty percent of organisations have a broad diversity programme to support women, and a further 17% have a specific cyber security diversity programme. Yet, 27% don't have a diversity programme to support women and 17% weren't aware if their organisation had any such programme.

CONCLUSIONS & RECOMMENDATIONS

This research provides insight into the types of cyber security roles, the challenges that organisations face in recruiting and the current state of play in relation to training, development and gender diversity. The results have highlighted strengths and identified serious challenges of the Irish labour market, including cyber security skills gaps and skills shortages. These shortages are impacting organisations of all sizes (micro, small, medium and large), across a range of sectors including indigenous and foreign owned companies. To address these challenges, recommendations are made that will need to be jointly addressed by industry, academia and government.

A Growth Sector & Skilled Workforce

The cyber security cluster in Ireland will continue to grow, in line with international trends of a growing cyber security market and demand for talent. Of those organisations surveyed 62% plan to hire in 2021, 82% of these will hire technical cyber security staff and 50% will hire new graduates. At the time of the survey (August 2020), twenty organisations noted they have 70 open cyber security positions. This bodes well for the growth of the sector, but also asks questions of whether the Irish labour market has the skills available to meet this growth and take advantage of international opportunities.

We found that the cyber security workforce in Ireland is highly qualified with a high proportion of cyber security teams having general technical degrees (81%), a cyber security master's degree (50%) or a doctorate related to cyber security (11%).

Skill Shortages (a lack of people available to work in cyber security job roles)

The research has identified a number of indicators of cyber security skills shortage in the Irish labour market: organisations security teams are understaffed, the length of time it takes to fill cyber security roles, and the high percentage of hires from outside of Ireland. Organisations have difficulty in filling specific roles: Security- Engineer, Analyst, Architect, Consultant and Specialist.

There is an immediate need for organisations to increase recruitment and invest in their security teams, however, this under resourcing of cyber security teams is compounded by the skills shortage in the Irish labour market. Given the current implications of Covid-19, hiring from outside Ireland will prove increasingly challenging for those organisations who today depend on an international labour market. Specific cyber security roles are difficult to fill due the skills shortage, but we must also consider whether employers are offering suitable compensation for the roles on offer to attract candidates.

Retention is a particular problem for SMEs who cannot compete with large organisations' salaries. Access to new technologies is critical for SMEs to retain and upskill staff, as employees want to gain experience with the newest technology. In addition, it was noted that an often-overlooked area is whether candidates have the aptitude for cyber security roles. Industry is encountering candidates who are not suitable for roles though they may have the required educational qualifications.

1. Recommendations to Address Skills Shortages

With a worldwide shortage of cyber security professionals and a clear skills shortage in the Irish labour market, addressing these skills shortage will need to take a short, medium and long-term approach as there is no silver bullet.

- **Short-term:** Organisations are encouraged to adopt remote working practices to: a) increase staff retention and b) recruit internationally for technical skill shortages that can't be met locally. The most successful initiative found to increase staff retention was improved flexibility and remote working. Furthermore, COVID-19 has changed the perspective to managing remote teams and recruiting new hires internationally. Facilitating international remote working can improve retention rates of international staff and could provide cost benefits to the company.

- **Medium Term:** Increase the number of course places available in skill shortage areas. Feedback from workshop participants indicates the need for short term courses and to

facilitate new and flexible learning pathways for industry using micro credentials and online learning. This would allow professionals to upskill on the job and take modules / micro-credentials over a number of years. A skills and training needs analysis is required to understand the current, and future, cyber security skills needs of industry to ensure the appropriate modules and courses are available to meet industry needs.

- **Long-Term:** To grow the overall pool of cyber security professionals in Ireland, initiatives are required to attract children, students and adults to cyber security careers. For adults, creating clear career pathways for people from different backgrounds and expertise is required, and utilising aptitude tests or assessments to ensure candidates are suited to cyber security roles. Attracting children and students into a career in cyber security requires greater career promotion and role models, changing the mindset that it's for boys and those interested in programming, and growing the overall number of students choosing Science, Technology, Engineering and Maths (STEM) courses at third-level. Investing in a national Cyber Range to provide cyber security training and education to secondary school students, third-level students and citizens will improve the cyber security skills of the next generation and increase the number of fully prepared students entering the cybersecurity workforce.

Skill Gaps (people lacking appropriate skills) & Training Needs

Skills Gaps were identified as a serious challenge impacting industry. The lack of technical skills is a primary reason for open roles not being filled and the majority of open (unfilled) roles are technical cyber security positions. The most in-demand training areas are Cloud-enabled security, incident response, soft skills, regulatory compliance, and Risk based Frameworks. This survey did not conduct an in-depth skills and training needs analysis.

Companies are already addressing these skills gaps with initiatives to increase staff training, reliance on artificial intelligence or automation and reliance on certification to attest to tactual skill mastery.

2. Recommendation: A Cyber Security Skills Gaps Analysis of industry is required to identify current, and future, skill gaps and ensure the continued growth of the sector. The research should include a training needs analysis of industry to align current training, certifications and qualifications with industry skills needs.

Standardise Cyber Roles, Qualifications & Certifications

One notable challenge for job seekers and organisations alike is the large number of cyber security roles in the industry. This survey asked about twenty-seven of the most common cyber roles while respondents identified an additional twelve roles. With such a range of job titles, and criteria for these roles, this may be contributing to the delays in recruitment identified. Cyber security also has a large range of qualifications and accreditations; twenty-four certification options were presented and respondents added a further nineteen. There is significant fragmentation in the market for security certifications, which impacts ease of hiring and keeping skills up to date.

Feedback from workshop participants highlights a mis-match between companies, the salaries they are offering and the skills they require. Organisations need to move away from job descriptions based on a long list of qualifications and certifications, which are not realistic.

3. Recommendation: Development of a Cyber Security Career Framework for Europe to describe roles, competencies, and skills for cyber security, which can be utilised by individuals, employers and training providers. The European Career Framework can build on existing work such as the NIST NICE Career Framework. Senior managers and recruitment managers should utilise standardised job roles and the associated skills and qualifications relevant to the role from existing cyber security career frameworks.

Upskilling and the Adequacy of Training Plans:

Organisations are making a significant investment in addressing skills gaps through upskilling and training with 93% of organisations support training and certification. However,

internal training plans exist in just over half (52%) of the organisations surveyed, and only 62% state the plan is effective.

Workshop participants noted a lack of understanding in Human Resource (HR) and Learning and Development (L&D) teams of the specific requirements of the cyber business. This is contributing to the disconnect between training plans and the training that is delivered.

4. Recommendation: Organisations to evaluate their internal training plans and the degree to which it is meeting the needs of the security team and the broader organisation. Education is needed to align HR and L&D teams and the cyber function in the business.

Cyber Apprenticeships

The apprenticeship scheme has been utilised by the UK to address technical skills shortages for a number of years and has proven a successful model, in particular for cyber security. There is broad agreement from industry that a place exists for apprenticeships, short-term or conversion courses. Graduates from these courses will need a strong base knowledge of networking, systems and an ability to reverse engineer code.

Seventeen percent of organisations had a staff member with a cyber security apprenticeship and there is an opportunity to grow the number of companies taking in employees with a cyber security apprenticeship. The FIT Cyber Security Apprenticeship was launched in 2019 in Cork and Dublin and was over-subscribed with applications but requires a similar number of industry placements for apprentices over the 2-year programme.

5. Recommendation: Increase adoption of the Cyber Security Apprenticeship programme to address skills shortages and assessment of the challenges for industry in taking on apprenticeships.

Graduates & Entry Level Roles

Graduates play a vital role in addressing skills shortages and skills gaps, if their skills meet the requirements of industry. A healthy labour market provides opportunities for graduates in entry level roles and more experienced roles to further career progression. Sixty-two percent of organisations are planning to grow their security team in 2020 with 50% expected to hire for graduate level cyber security roles.

Graduates' salaries are attractive for cyber security roles and should attract top students into the field. However, 26% of Graduates are less qualified than expected and 5% are poorly qualified. Workshop feedback noted that graduates were mostly from computer science degree programmes and most organisations don't require master's level students' as often there is no need for specialisation. In the main they have found undergraduates to be well educated and adaptable. The question exists whether graduates are exposed to industry skill needs or whether industry is inadequately determining the kind of experience, education and capabilities of graduate roles.

6. Recommendation: Further investigation is required to ascertain are enough entry level cyber security roles available for graduates and what are the skills that graduates are lacking for entry level roles.

Gender Diversity Programmes

The cyber security sector is male-dominated in Ireland, similar to ICT and trends internationally. Retaining women in cyber security roles was identified as a challenge with 30% of turnover due to "family situation changes (e.g. children, marriage)" and over a quarter of organisations (27%) have difficulty in retaining females.

Specific initiatives are required to support the attraction, retention and advancement of women in cyber security. While broad diversity programmes supporting women exist in many organisations there is room for improvement as 44% of organisations don't have a diversity programme or weren't aware if they had one.

7. Recommendation: Support the attraction, retention and advancement of women in cyber security with a Diversity Survey to assess equity, inclusion and diversity in the cyber security sector in Ireland. Further work is needed to identify specific challenges for women in cyber security in Ireland and to investigate the efficacy of Gender Diversity Programmes and share examples of best practices. A 'Diversity Toolkit' could provide concrete tools, tips and recommendations for companies and individuals to be able to apply to the recruitment, hiring and retaining of women in the cyber security sector.

This survey is a starting point to benchmark the cyber security skills landscape in Ireland with the cyber security cluster. Clearly further investigation is needed across a number of areas from skills and skills gaps, cyber roles and competencies, graduates and diversity in the sector. A larger bi-annual survey (every two years) is required, expanding to include companies outside of the cyber security cluster to give a full picture of the cyber security needs of organisations across all sectors of the economy. This survey should be conducted by a suitable national organisation and funded appropriately.