

Cybersecurity Skills Development Strategy

MAY 2021



Table of Contents

ABOUT THIS REPORT	04	SECTION 6: QUALITATIVE RESEARCH	60
FOREWARD	05	The Talent Group	62
SECTION 1: EXECUTIVE SUMMARY	07	The CISO Group	63
SECTION 2: KEY FINDINGS	12	The Vendor Group	64
SECTION 3: RESEARCH METHODOLOGY	19	Overview of Opinions	65
SECTION 4: DESKTOP RESEARCH	22	Conclusions from the Interviews	69
Reports of Cyber Skills in Ireland	23	SECTION 7: QUANTITATIVE RESEARCH (TRAINING NEEDS SURVEY)	71
Dynamics in Cybersecurity Employment	25	Part 1 - About Respondents	72
Cybersecurity Capability Maturity	28	Part 2 - Training Practices	73
Scale and Cost of Cyber Crime	28	Part 3 - Training Requirements	74
Issues and Trends in Cyber Crime	30	Part 4 – Future Challenges	77
Government and Cybersecurity	33	Part 5 – Resourcing Intentions	78
Other Cybersecurity Trends	35	Part 6 – Cybersecurity Functional Maturity	79
Development	37	SECTION 8: FINAL CONCLUSIONS	82
Conclusions from Desk Research	39	SECTION 9: RECOMMENDATIONS	84
SECTION 5: MARKET REVIEW OF CYBERSECURITY TRAINING PROVIDERS	42	SECTION 10: APPENDIXES	87
Review of Online Training Providers	43	Appendix 1 – UK Report Recommendations	87
Specialist Training Providers	45	Appendix 2 – Leading Training Provider	
Cyber Training Initiatives in Ireland	47	Review Grid	88
University Cybersecurity Programmes	48	Appendix 3 – Cybok Cybersecurity Body of Knowledge Overview	89
Knowledge and Skill Frameworks	50	Appendix 4a – Job Postings (on LinkedIn for Cybersecurity)	90
Quality and Capability Frameworks	52	Appendix 4b – Hiring Companies (for Cybersecurity Job Postings)	91
Cybersecurity Jobs	53	Appendix 5 - Survey Design Process and Rationale	93
Career Entry Points	54	Appendix 6 – Detailed Survey Findings	96
Cybersecurity Career Paths	54	BIBLIOGRAPHY	107
Conclusions from Market Review	57		

About this Report

The purpose of this Future Skills research project was to identify the future skill requirements within Cybersecurity in Ireland, with a particular focus on the objectives and needs of the Skillnet Ireland target audience.

The underlying objectives were to:

- Detail the key factors influencing the demand for cyber skills.
- Detail the qualitative and quantitative needs of the target audience.
- Critique existing Cybersecurity programmes and training providers.

The outputs from this research report will be used to define the strategic priorities for the it@cork Skillnet's future offerings for Cybersecurity.

Who this report is aimed at?

The desired target audience for this report is as follows;

- Government and support agency strategy and policy makers.
- Education and training providers.
- Cybersecurity vendors and providers.
- Managers involved in the recruitment and training of Cybersecurity skills.
- Senior Executives within organisations seeking a better understanding of Cybersecurity.
- Managers with responsibility for Strategy, Risk Assessment and operating of Cybersecurity Teams.

This report also brings together a list of initiatives, education programmes and Cybersecurity training platforms that help indicate the progress achieved whilst also identifying emerging trends.

This report will also help policy makers shape incentives and supports that can make Ireland more attractive to further Foreign Direct Investment whilst also supporting the expansion and growth within the indigenous sectors.

The ambition of this report is to contribute to the on-going development of a body of knowledge that is context specific to Ireland.

By continuously building data insights through this type of research about Cybersecurity we will be helping Multinational Companies (MNCs) & Small and Medium Enterprises (SMEs) with the on-going maturity of Cybersecurity skills development.

Foreward



“ **Mark Jordan**
Chief Technologist, Skillnet Ireland

The cyber landscape is constantly evolving. At Skillnet Ireland we believe that a long-term focus on research and talent is critical to cementing Ireland’s enviable position as a leader in cybersecurity. We welcome the launch of the Cybersecurity Skills Development Strategy Report which underpins the importance of our continued investment in knowledge and skills to ensure businesses are ready to face the challenges of tomorrow.



“ **Gillian Bergin**
Director, it@cork European Tech Cluster

As the Director responsible for promoting it@cork Skillnet I see a particular relevance to focusing on Cybersecurity. Simply because it intertwines with business change and digital transformation and touches all aspects of IT management. In this project we worked hard to take an objective and non-biased approach to the research, and I think the report is better because of that.




“ **Annette Coburn**
Network Manager, it@cork Skillnet

I would like to thank the Steering Committee at it@cork Skillnet for their guidance and support. We are very well represented by the Cybersecurity sector on this team and this have been invaluable in defining the high level needs. This research is already helping shape our service delivery of skills programmes and has amplified our attention on Cybersecurity skill needs for the next 2-3 years. I look forward to reporting back on progress on each of the reports recommendations.



“ **Anthony O’Callaghan**
Chairperson it@cork

it@cork has a proud tradition of innovating through pioneering research. This research project is an important milestone, and we will use the deep insights from this report in driving our organisation to ensure we continue to help shape our region and community. As Chairperson I am delighted that we can deliver such high-quality research.

A hand is shown holding a glowing lightbulb. The lightbulb's glass part is filled with a blue and green network diagram of interconnected nodes and lines. The base of the lightbulb is a white outline of a screw-in base, also glowing. The background is dark, and the hand is in focus.

SECTION ONE

Executive Summary

Executive Summary

In August 2020 it@cork Skillnet commissioned a review into the Future Skills requirements for Cybersecurity in Ireland. This research was funded by Skillnet Ireland. The aim of this review and research is to help guide it@cork Skillnet and other stakeholders in its development of a strategic plan specifically for how it services the development of Cybersecurity related skills.

There are a wide range of factors currently influencing the demand for Cybersecurity skills

The Cybersecurity sector has been designated by the Irish government as a high potential growth area. Initiatives, such as Cyber Ireland, have been funded to help drive growth in this sector. Research into this complex sector within Ireland has been limited. This research and report aim to produce data insights specific to this sector that helps guide both public and private future investment.

This research was undertaken between September and December 2020. The research methodology included a literature review, interviews with subject matter experts and a detailed online survey.

The research revealed that there are a wide range of factors that are currently influencing the demand for cyber skills:

- The nature, scale and attack surface of cyber intrusions is in a state of constant change. This means that the importance of Cybersecurity is increasing whilst the skills required to manage and deliver safe cyber environments is evolving continuously.
- There is a low take-up on the implementation of standards and global best practices for Cybersecurity and this means that the sector remains at a relatively low level of capability maturity. The level of investment in training for cyber skills is relatively low in comparison to other ICT disciplines.
- There is a perception that people outside the cyber functions have a relatively weak understanding of the value of cyber investments and this creates a challenge in quantifying the value of Cybersecurity.
- Organisations are deploying vastly different management operating models, and this is one clear indication that the management science for Cybersecurity is still at a relatively low level of maturity. Examples of low competence levels include resource and workforce planning and training needs analysis specific to cyber.

- There is a prevalent perception that there is a skills gap and a shortage of resources and one of the consequences of this is that it is shaping job design, training needs analysis and recruitment practice decisions.
- The value chain ecosystem for the Cybersecurity sector is complex with a diverse set of enterprise, Government, and vendor stakeholders. Addressing solutions for cyber skilling requires an integrated and joined-up approach from all stakeholders.

The Research

The research shows that Enterprises have a demand for support with up and cross-skilling cyber resources:

- Availability of skilled resources and in particular job-ready resources.
- Support with the design and delivery of cyber skill training programmes.
- Improvements in ease of using internships and apprenticeships.
- Assistance with identifying and deploying best practices for training in Cybersecurity.

The researchers looked at a wide range of cyber training providers. There is a clear mix of very established (and standards based) training organisations and a newer generation of cyber training providers that focus more on the emerging learning science of blended, immersive, and remote training.

The literature review clearly indicated that there is limited context-specific labour and skill data on the Cybersecurity sector in Ireland. This means that many report analysts are using international data to describe and forecast needs in Ireland. This is important because international trends may be slower to adopt to the Irish contextual landscape or in fact may not materialise at the scale and scope predicted for other regions. Data from the UK and the USA, for example, must come with a health warning because Ireland presents with a different context compared to those markets due to its geography, scale and economic composition.

There is high demand for support with up and cross-skilling

The research highlighted that the Cybersecurity sector is still emerging and is a relatively immature sector. The sector, however, faces many challenges to keep organisations safe and secure. The general pace of change within the sector is significant and the increasing skill and competency demands this is placing on cyber leaders and teams is large.

Cyber leaders and teams are likely to need significant training and development yet are likely to struggle to find the time, funding, and resources to deliver this requirement. Training solutions that are very targeted, agile, and comprehensive at tackling the challenges faced by cyber teams are likely to be the ones that get attention.

The sector is well served by online training providers globally although local providers are somewhat limited. The survey indicates a strong demand for advanced training in Cybersecurity. With some exceptions most Cybersecurity teams in Ireland are small albeit often part of a global operation. Our research found that most cyber jobs in Ireland are mid-tier, and that there is a need for concentrated support to build more entry level positions and talent pools.

The research suggests that one of the primary reasons for relatively fewer entry level roles is because entry level roles are seen to be more economical if placed in offshore, lower cost economies. This is a systemic challenge for the sector and one that needs further and urgent attention. If there is a lack of entry level roles, then the ability of the sector to have a correctly skilled and well supplied talent pool will have inherent challenges.

Many Irish cyber teams face competition from lower labour cost countries with multinationals being able to choose from several options when planning an expansion. If entry level roles continue to be staffed in overseas locations, then the sector and businesses in general will always have a challenge to grow the scale and scope of the overall talent pool as every talent group needs a youth policy structure.

There is a perception that automation will ease this challenge by using AI to undertake lower skilled tasks. The level of investment in automation and robotics is clearly growing rapidly, however, automation does not remove the need to have a career path that includes entry level positions.

Off-shoring is a real risk to expanding the sector

Many organisations in this research have stated an intention to grow their cyber teams typically at the mid-tier and above. The scope of training topics is constantly growing in line with how technology is changing. This growth is being driven by, as mentioned above, the changing nature of attacks, but also by, for example, digitalisation, changes in the practice of software development (e.g., containerised development), infrastructure (e.g., remote access and working) and AI/Automation.

Ongoing research and dialogue with cyber leaders reveal that off-shoring is a real risk to expanding the sector and more needs to be done to make Ireland a more attractive destination. Given the pace of change within the sector, competitive pressures, and the relatively small scale of cyber operations within Ireland, it is likely that a joined-up national approach to supporting this sector is required to ensure that the right level of supports are in place. Much work is needed to develop practical and real-life career paths and development to make Cybersecurity an attractive profession with a future here in Ireland.

A photograph of two men in a meeting. The man in the foreground is wearing a black and white striped sweater and is writing on a whiteboard with a marker. The man in the background is wearing a light blue sweater and has his arms crossed. The scene is dimly lit with a blue tint.

SECTION TWO

Key Findings

Key Findings

The following findings synthesise the research and summarise those most significant to the aims and objectives of this research.

Based on the research and data gathering, Ireland Inc. appears to be in a good position to continue to take competitive advantage of the opportunities that are evolving and growing around Cybersecurity. Universities are investing in specific programmes for Cybersecurity; there is an existing cluster of world-leading Cybersecurity companies operating in Ireland; there is a base of indigenous Irish Cybersecurity companies, and the Irish Government has placed a focus on Cybersecurity.

This research found that there are relatively low numbers of new entrant vacancies for roles in Cybersecurity

- According to some participants in the research significant further development and evolution are required, however, to deal with existing systemic and organisational gaps that exist mainly due to the relative low level of maturity of Cybersecurity in Ireland. The industry has been slow, for example, to adopt global standards and best practices. Although there are industry representative groupings, these too are still at an early stage of development. Funding for academic research is another indicator of maturity and we are now starting to see that investment materialise.
- The research found that there is a low level of training and skills development investment today in Cybersecurity. The survey results indicate, however, that there is a general awareness that there is a need for further investment. The research also indicates that Cybersecurity is a complex field and presents a challenge for many companies to both undertake the right skills and training needs analysis (TNA) whilst also resourcing and designing effective Cybersecurity skills improvement programmes. Part of the reasons behind why TNA is hard in Cybersecurity is because the industry is still at an early development phase. This is further complicated by the rapidly changing nature and sophistication of Cybersecurity technology and cyber-attacks.
- This research found that there are relatively low numbers of new entrant vacancies for roles in Cybersecurity. This may present an opportunity for attracting new Foreign Direct Investment as well as fostering new entrants among existing companies in Ireland.

Only half of the surveyed companies used competency skill frameworks to identify training needs for Cybersecurity

42%
of companies provide 2 days of Cybersecurity training or less per annum

- There is a perception that AI/Automation will reduce the demand for some of the current entry level roles, so to move forward the sector will need to better define the cyber career path(s) including how new talent at an entry level is catered for. This is backed up by the qualitative research that shows that there is a gap in resource and career progression planning for Cybersecurity. This presents an opportunity to evolve how Cybersecurity skills development science and best practices are designed and deployed across Ireland.
- The research results, particularly from existing industry reports, indicate a clear need for advancing how Cybersecurity skills are developed at all organisational levels, for example, from new entrants right through to the CISO and the Board etc.. There is significant commentary that suggests that the Board do not feel well informed or educated on Cybersecurity. This has implications for cyber training as it directly impacts budgets, operational models, and training budgets.
- Certification remains important to a large majority of the survey respondents (77%). There are mixed views on the importance of certification and there are a small but growing group of experts who recommend a higher importance on gamification, purposeful and simulated learning, and recognition mechanisms like Digital Badges. Over two thirds of respondents expressed an interest in some form of cyber training initiative with the graduate placements being the most popular.
- The survey found that 42% of companies provide 2 days training or less per annum. Most companies in the survey had cyber awareness training programmes in place for their leaders and employees.
- Only half of the surveyed companies used competency/skill frameworks to identify training needs for Cybersecurity.
- The research identified a wide range of opportunities for improvement that have implications for all elements and stakeholders involved in the Cybersecurity value chain from job design, recruitment, qualifications, certification, learning interventions and skills improvement methods. For Cybersecurity training to be effective improvements are required across the full value chain and this is evidenced by the fact that there are so many factors influencing the demand and needs for Cybersecurity skills development.

It's difficult to determine future demand

Some university level programmes may not provide job ready resources in Cybersecurity

- Third Level Institutions, private training companies, and Skillnet Ireland's cyber programmes are examples of positive investments that are being made in growing the science and effectiveness of Cybersecurity skills development. An integrated, aligned and joined-up co-ordination of funding and investments at a national level will accelerate the maturity of the Cybersecurity capability.
- Some of the indicators that suggest significant weaknesses in cyber related skills development manifest themselves, for example, in perceptions around the availability of resources, ease of new entrants securing roles in cyber and the importing of resources from EU countries and Asia to fill gaps in the domestic supply of cyber skills.
- There was qualitative feedback that suggests that some university level programmes may not provide job-ready resources in Cybersecurity and that there was an over emphasis on computer science theory at the expense of practical skill development. This has implications for many aspects of Cybersecurity skills development including the Cybersecurity design of next generation internships, apprenticeships including short and agile interventions for up and cross skilling.
- One of the key challenges for the research group was to determine the current and future demand for Cybersecurity resources and skills. One of the early findings in the research was the fact that labour market statistical data specific to Cybersecurity in Ireland is limited and lacks sufficient precision.
- Many commentators on Cybersecurity are using global trends and international statistics to extrapolate future predictions for Ireland. It will be useful to continue to monitor these trends, however, there are some challenges with how accurate and reliable this extrapolation method could be. One of the key findings, therefore, is that there is no reliable definitive source of accurate statistics on the labour market pertinent to Cybersecurity in Ireland.

Open Vacancies

85%

of survey respondents plan to expand Cybersecurity roles in the coming few years

One indicator that the research group investigated was the volume of open vacancies. Although this is only one element of measuring current and future demand, it is a useful base metric. The research showed that the volume of open vacancies was significantly lower than other areas of ICT for the period under investigation. Cybersecurity is seen as a growth area for ICT by many practitioners and commentators, however, the current volume of vacancies is low.

- The research suggests that there are indirect and intuitive indicators that the demand for Cybersecurity skills and resources will grow in Ireland (e.g. 85% of survey respondents had a plan to introduce or expand one or more Cybersecurity roles in the coming few years). The precise scale and scope of this growing demand is difficult to forecast and this will pose a challenge in terms of the setting of the relative level of priority. Cybersecurity is a critical skill set and the research clearly shows why that is the case, however, given the relative level of maturity of Cybersecurity, some caution is required specific to resource and skill planning relative to the scale, speed, and scope of future demand.
- The research suggested that an agile and flexible approach to Cybersecurity skills development is required, especially as some practitioners suggest that Cybersecurity skills are not standalone functional skills but will in fact become more deeply integrated into other ICT disciplines. The pace of change in Cybersecurity also indicates the need for this form of approach.
- There is sufficient complexity to Cybersecurity that warrants a focused training priority. This is backed up by the fact that the number of 3rd level programmes has rapidly increased over the last 5 years that are specific to Cybersecurity. It does appear from the research and from early findings from the CyberTalent employment activation programmes, however, that a key priority for skills development in Cybersecurity is the need for purposeful skills practice in a safe, flexible and agile environment. The absence of these training interventions, resources and methods means that employers will continue to see most resources as not being job ready.

Some companies will be able to deal with Cybersecurity training through in-house programmes, but there will be many companies that will not have that level of funding or resource experience.

- The research also shows that there is a significant requirement to re-evaluate the role of internships and apprenticeships and there is a need to make it easier for companies to engage with such programmes whilst also deploying current best practices around training interventions.
- Cybersecurity jobs in Ireland tend to be primarily mid-tier ones, with limited entry level roles for new career starters to aim for; this points to barriers in terms of attracting new talent to the sector and expanding the overall number of jobs within this sector.

The survey results show that there are a mix of companies that use in-house cyber teams and others that use outsourced managed services. This is important because many managed services companies use offshore resources.

From the research there were many comments that suggested that the entry level roles; specific examples were Security Operations Centre (SOC) Level 1 and junior pen testing, are not economically viable to deliver from a cost base such as Ireland and tend to be serviced through outsourced providers with offshore teams.

There is no effective change or digital transformation without good Cybersecurity

- The skills development priorities will be shaped by the demands of businesses and Governments and our research shows some noticeably clear examples of this:
 - Most organisations are engaged in some level of digital transformation and there is no effective change without appropriate Cybersecurity.
 - The Cybersecurity threat landscape is continuing to shift through the current Covid-19 pandemic and as criminal/ state actors seek out new vulnerabilities this trend will continue.
 - The Cybersecurity ecosystem is expanding with requirements permeating out to supply chains, manufacturing operations and infrastructure (OT) as threat actors seek new areas of attack; this widening of the attack surface brings about a host of new challenges for cyber teams and with it comes a need for new skills and competencies.
 - Cybersecurity legislation and regulation is set to continue to evolve and expand.
- Technological advancements (e.g., cloud, containerisation, AI) are also placing new competence expectations upon cyber teams and targeted training and development support is needed to enable teams to remain effective in the battle against cyber crime.
- The research highlights that the technical skill and competency demands within the cyber sector are growing and changing as the performance expectations and responsibilities of cyber leaders and teams increase; in turn a clear commitment by organisations to invest in their cyber teams is required. This points to a general perception that business leaders do not fully understand the relevance and importance of making investments in Cybersecurity and there is a perception that this may result in inadequate funding.
- The survey research indicates that the strongest demand for the short-term Cybersecurity training was particularly for advanced training across a wide range of cyber topics including:
 - Cloud native security.
 - Network Security.
 - CyberSecurity architecture.

A person wearing a white lab coat and a blue lanyard is focused on working on a transparent, rectangular electronic device. The device is illuminated from within, showing internal components like a green circuit board and various connectors. The person's hands are visible, one holding a small component. The background is dark with a blue tint, suggesting a laboratory or workshop environment. A computer monitor is partially visible on the left side of the frame.

SECTION THREE

Research Methodology

Research Methodology

As part of the research design a list of 50 companies were identified to represent the best target audience for cyber training needs. In total, the online training needs analysis (TNA) survey was distributed to 173 companies.



44%
of those target companies responded comprehensively to the online survey

The research methodology consisted of four main parts.

Part 1: Desk Research - A review of published and publicly available reports on Cybersecurity.

- Between August and October over 40 industry reports were reviewed covering national, regional (EU, US) and global analyses of the Cybersecurity sector.

Part 2: Desktop review of cyber training providers and platforms:

- Between September and October 35 Cybersecurity training providers and their market offerings were reviewed.
- LinkedIn job posting data for Cybersecurity for the month of September (2020) was analysed.

Part 3: Qualitative telephone interviews with a cross selection of opinion leaders and cyber industry practitioners.

- Between August and November 2020 over 50 telephone interviews were conducted concerning a strategic review of the skill requirements for Cybersecurity.

Part 4: Online survey.

As part of the research design a list of 50 companies were identified to represent the best target audience for cyber training needs. 44% of those target companies responded comprehensively to the online survey. In total, the online training needs analysis (TNA) survey was distributed to 173 companies. There was an overall 20% response rate (35 organisations).

The survey consisted of 27 questions covering: demographics, training need requirements, resourcing intentions, strategic issues, and maturity.

The online survey was open to potential respondents from November 11th to December 15th 2020 including it@cork members and non-members from across Ireland.



SECTION FOUR

Desktop Research

Desktop Research

To inform the strategy review and specifically the development process for the TNA, a critique was undertaken of the published and publicly available reports on Cybersecurity.



The aim of the desk research was to review information on:

- Reports of Cyber Skills in Ireland.
- Dynamics in Cybersecurity Employment.
- Cybersecurity Capability Maturity
- Scale and Cost of Cyber Crime
- Issues and Trends in Cyber Crime.
- Government and Cybersecurity.
- Other Cyber security Trends.
- Priorities in Cybersecurity Skills Development.
- Conclusions from Desk Research.

The purpose of critiquing these reports was two-fold:

a) To inform the development of a training needs analysis (TNA) survey.

b) Ultimately to aid the decision-making process on strategic priorities.

The following are the categories of reports that were reviewed and critiqued:

- Traditional research companies (IDC, Gartner, Forrester, McKinsey etc..).
- Governmental sponsored research and news publications (IDA, Enterprise Ireland, ENISA, UK Government, US Government).
- Vendor and Industry surveys (e.g., IBM, Trend Micro, Accenture, NTT, Deloitte, KPMG, EY, Grant Thornton etc.).
- Webinars and industry events (e.g. it@cork TechFest).

The results of this desk research are described in detail in the following pages.

1. Reports of Cyber Skills in Ireland

Our research revealed that Irish reports covering essential and in-demand Cybersecurity skills within Ireland are scarce, in fact, only one government report covered this in part.

Expert Group on Future Skills Needs (EGFSN)

EGFSN advises the Irish Government on the current and future skills needs of the economy. The Expert Group published (March 2019) a key report: 'Forecasting the Future Demand for High-Level ICT Skills in Ireland, 2017- 2022^[1]'. This report endeavours to scope the demand for skills across all key ICT domains. The Expert Group identified a set of global megatrends as drivers of local ICT skill demands and within 'IT Security' specifically called out Next Gen Security and IoT as essential component parts of the significant growth in digital transformation as well as a potential growth in demand for security managed services.

They used statistics from the market research firm IDC to extrapolate global trends for the context of the Irish market, combined with collating the views of a range of organisations and stakeholders. Their report also identified the following in demand Cybersecurity skills (technical and non-technical) in the diagram below.

Diagram 1: The Expert Group's in Demand Cybersecurity Skills

Business Skills to Assess the Impact of Security Stance.

Source: IDC 2018

Secure SW Development

Machine Learning

GDPR

Cloud Security

Security Technology Skills
(STAP, DDOS, ENDPOINT, SIAM, IAS etc..)



Data Analytics

Intrusion Detection

Collaborative Skills

Communication Skills

Critical Thinking

Psychology Skills

In summary the report highlighted the following general issues for Cybersecurity:

- Supply of graduates with ICT skills is still not sufficient.
- Improvements are needed to promote ICT as a career at all levels of education.
- Females are under-represented in Cybersecurity.
- Apprenticeship programmes and internships are critical success factors.
- Ireland will continue to depend heavily on immigrant workers.

There is an open question about the reliability in taking global statistics and extrapolating them to an Irish context. Looking at US trends (e.g., published statistics on ICT skill shortages) and assuming that the same trend will arrive in Ireland needs to be carefully reviewed on a context by context basis. This is because there is a common rhetoric in the cyber sector about skills and resource shortages. The ambition of this project is to endeavour to size and scope the market employment dynamics. Section 5 of this report provides a current view of market demand for cyber jobs in Ireland and this analysis is not (at least yet) following a global trend.

However, the EGFSN is a useful reference point because it puts Cybersecurity in the context of the range of ICT skills. It also highlights that there is a significant lack of critical data on Cybersecurity skills.

Other Irish Reports

The FIT ICT Skills Audit third bi-annual report (2018) ^[10], based on interviews with 118 Irish based ICT companies, found Cybersecurity & Digital skills (a combined focus) the fourth most in demand skill set. They also report a trend over the three audits that companies require employees with deeper, broader skill sets along with a range of transversal skills. It argues for more effort to create career paths to support this along with greater up-skilling opportunities for employees.

A new industry report by Cyber Ireland has recently been published concerning cyber security recruitment, pay and training practices.

2. Dynamics in Cybersecurity Employment

58%
of Organisations
have unfilled
Cybersecurity
vacancies

There are many reports on Cybersecurity employment market dynamics but unfortunately, there are no such reports publicly available, with a sufficient level of detail, for the Irish marketplace. We have focused on the top three most often quoted reports from cyber opinion leaders in summary below:

- ISC² Strategies for Building and Growing Strong Cybersecurity Teams Cybersecurity Workforce Study, 2019.^[iii]
- UK's Department for Digital, Culture, Media and Sport's (DCMS) Cybersecurity Skills in the UK Labour Market, March 2020.^[iv]
- ENISA's Cybersecurity Skills Development in the EU, December 2019.^[v]

These relatively recent reports have a consistent view of employment dynamics and they highlight the finding that there is a significant global shortage in cyber skills and cyber resources.

According to ISC²:

- The Cybersecurity workforce gap has increased on the previous year's survey, in the U.S., they estimate a Cybersecurity workforce shortage of nearly 500,000.
- They estimate that the Cybersecurity workforce needs to grow by 62% to meet the demands of U.S. businesses and the global workforce needs to grow by 145%.
- 51% of Cybersecurity professionals surveyed stated that their organisation is at moderate or extreme risk due to Cybersecurity staff shortage.
- They estimate the size of the Cybersecurity workforce of the UK to be 289,000.

According to the European Union Agency for Cybersecurity (ENISA):

- 74% of organisations are impacted by skill and resource shortages in Cybersecurity.
- Cybersecurity vacancies also took 20% longer to fill than those in other IT occupations.
- 58% of organisations have unfilled Cybersecurity vacancies and 60% of them take a minimum of 3 months to fill a position.
- 29% of organisations report that fewer than 25% of candidates are well qualified for the job.

64%

of Cyber firms have faced problems with technical Cybersecurity skills gaps

Two factors perhaps driving all these statistics concerning high skill gaps/skill shortages within Cybersecurity across a several economies is best expressed in the ENISA report:

- “The first one is the high expectations that employers have about the skill level of candidates that the current labour market can offer...
- ... while the second one is the lack of sufficient and suitable training provided to employees”.

According to the UK’s Digital, culture, Media and Sport (DCMS) report:

- 64% of cyber firms have faced problems with technical Cybersecurity skills gaps, either among existing staff or among job applicants.
- 25% say that such skills gaps have prevented them to a great extent from achieving business goals.
- 29% of cyber firms say job applicants lacking non-technical skills such as communication, leadership or management skills has prevented them to some extent from meeting their business goals, and a similar proportion (28%) say this about their existing employees.
- Relatively few joined as career starters (21%). Moreover, when excluding the large businesses from the sample, the proportion joining as career starters drops to 12%. This highlights that, outside the small number of larger businesses, very few appear to offer graduate schemes or other entry level positions.
- 24% of respondents report having staff in cyber roles undertake training.

Whilst not necessarily Ireland specific, some emerging themes from this research are:

- Cybersecurity workforces need to grow in all countries.
- Growth rates of 50% + are being projected.
- Risks appear to suggest that organisations do not understand Cybersecurity issues.
- General perception that there are difficulties in filling posts with the right skills quickly.

However, it is hard to extrapolate accurately from these UK figures given the differences in the two economies.

A recent report from the World Economic Forum (Future of Jobs Survey, 2020)^[vii], using data from 2020 economies, ranks ‘Information Security Analysts’ as 8th in the top 20 “increasing demand” roles, which lends support to the general premise that this sector is growing (see diagram below).

Increasing Demand



1	Data Analysts and Scientists
2	AI and Machine Learning Specialists
3	Big Data Specialists
4	Digital Marketing and Strategy Specialists
5	Process Automation Specialists
6	Business Development Professionals
7	Digital Transformation Specialists
8	Information Security Analysts
9	Software and Application Developers
10	Internet of Things Specialists
11	Project Managers
12	Business Service and Administration Managers
13	Database and Network Professionals
14	Robotics Engineers
15	Strategic Advisers
16	Management and Organisation Analysts
17	Fintech Engineers
18	Mechanics and Machinery Repairers
19	Organisational Development Specialists
20	Risk Management Specialists

Table 2: World Economic Forum’s Increasing Demand Jobs

Source: IDC 2018

It is likely the Cybersecurity market in Ireland is facing similar challenges as the UK. Important to note, during this research stage, there was a period of high uncertainty with employment and new jobs posting decreasing rapidly over the summer (e.g., Indeed’s Job Posting Index reveals a 33% decrease in September 2020 postings compared to the same period in 2019).

3. Cybersecurity Capability Maturity

The research for this report sought to identify where Irish organisations sit in terms of their Cybersecurity maturity. No research has been published on this that has sufficient depth of data so this appears to be another gap in understanding the Cybersecurity sector in Ireland. While there are many organisations offering maturity framework tools and processes to help organisations evaluate this, none offer maturity research reports or fully established maturity benchmarks to help organisations compare themselves. It is perhaps indicative of the lack of maturity within this sector generally.

4. Scale and Cost of Cyber Crime

Ireland's Department of Justice^[vii] report defines what cyber crime is, how the law needs to improve and the most common types of attacks that organisations can encounter, namely:

- Ransomware (Malware used to prevent user access to systems and files in order to gain a ransom payment for regained access).
- Other Malware (software used to attack computers, servers, and networks) threats.
- Data breaches and network attacks.
- Spear-phishing (email or electronic communication scams targeting individuals or organisations to install Malware and or steal confidential security/personal identity information).
- Attacks against critical infrastructure.

Like previous years, there have been several high-profile Cybersecurity breaches this year (2020) that have made front page headlines. The World Health Organization, Garmin, Cognizant, SolarWinds along with a host of universities and hospitals are well publicised breaches. Actual figures in relation to cyber-attacks are always difficult to establish with multiple reports from different organisations covering different metrics. We examine some of these reports below.

The PWC's Annual Report on Security^[viii] highlighted in April 2020 that 41% of decision makers reported that their firms had experienced at least one business-impacting cyber attack related to Covid-19. Neustar^[ix] reported a 151% increase in the number of attacks from January 2020 to June 2020 versus the same period in 2019. Working with Cambridge University's Crime Reporting Group they compare annual data on Attack Intensity, Volume and Duration as well as the origins of attacks.

The World Health Organisation (WHO) saw a dramatic increase in the number of cyber-attacks directed at staff and email scams targeting the public at large.^[x]

In terms of Covid-19, the NTT's Global Guide to Threat Intelligence suggests that many countries have not provided cyber awareness education for remote workers. Viewing this from the cyber criminals' perspective, it is a great incentive to continue their criminal campaigns at individual, organisational and state levels.

The latest report from the Department of Justice in Ireland suggests that criminals quickly respond to their changing landscape. "This type of activity has grown over the last six months, with criminals increasingly exploiting the online space during the Covid-19 pandemic. Our traditional methods of policy development and legislative responses do not easily lend themselves to the dynamic and rapid evolution of online crime while balancing individual rights."^[xii]

Reports from Accenture and Trend Micro are more cautious at concluding that there has been an overall significant increase in breaches and incidents. Although TrendMicro can see from their data an increase in ransomware, it is not categorical that the overall volume of incidents/breaches has increased.^[xiii] Accenture's Third Annual State of Cyber Resilience reports a drop in direct attacks and breaches, but their analysis suggests a jump has happened in breaches if indirect attacks are included in this.^[xiv]

There seems to be a likely consensus that Covid-19 related attacks have increased and that the nature of remote working has meant that the attack surface has changed. However, there is still potentially under reporting due to poor definition. For example, vendor companies may not want to tell how their software has failed and organisations will want to remain silent on ransom payments. Until a standardised means of measurement is developed and adopted globally it may be difficult to accurately estimate the scale of cyber-crime.

When trying to calculate how much cyber-crime costs, RiskIQ in their 'Evil Internet Minute Report' suggest a figure of \$2.9 million lost per minute, equalling \$1.5 trillion per annum.^[xv] This figure pre-dates Covid-19. Criminals are keeping ahead of public and private organisations, their police, intelligence, and defence forces. Money is not an issue for them, nor is compliance to regulations and standards.

Ransomware attacks, such as Garmin are being widely reported. Wired Magazine suggest that Garmin paid out \$10 million (US) to regain their systems. This payment happened against the advice not to pay. Such large amounts of money create a greater incentive for the criminals and provide another example of the lack of trust there is in preventative systems, whether with software or agencies.

The cost of cyber-crime is set to hit \$6 trillion in 2021 according to the World Economic Forum. Criminal gangs, state actors^[1], hacktivist groups and lone actors are continuing to operate at will. US thinktank Third Way estimate the chance of a criminal being prosecuted for a cyber-crime in the US is less than 1% (based on a ratio of arrests to the number of incidents reported).^[xvi] All the reports suggest the momentum behind cyber criminality will be maintained well into the future.

^[1] State actors (or nation state actors) are hacking groups acting directly or indirectly under the direction of a state's apparatus and are typically involved in espionage and sabotage.

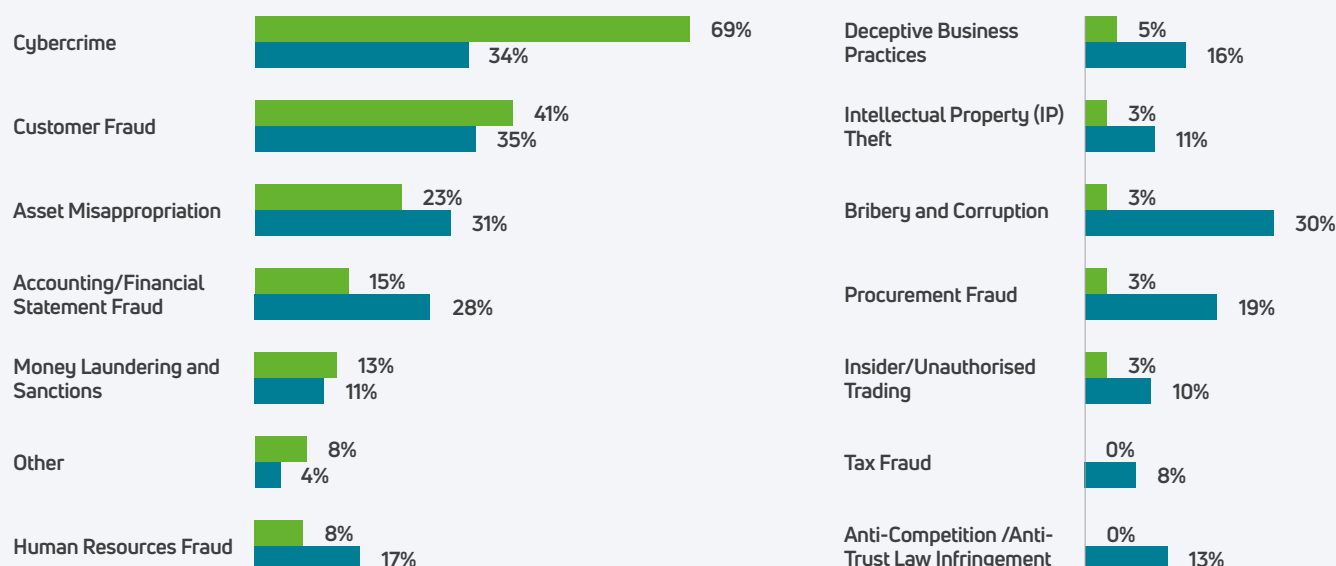
5. Issues and Trends in Cyber Crime

Deloitte Ireland’s Irish Economic Crime Survey 2020 report found that cyber-crime is the ‘most prevalent’ of all the economic crimes within Ireland. ^[xviii] The chart below shows it is double the global average, so far from being under the radar, Ireland is plainly a key target area for cyber criminals.

Diagram 2: Deloitte - Most Common Economic Crime by Type (Ireland versus Global)

What types of fraud, corruption or other economic crime has your organisation experienced within the last 24 months

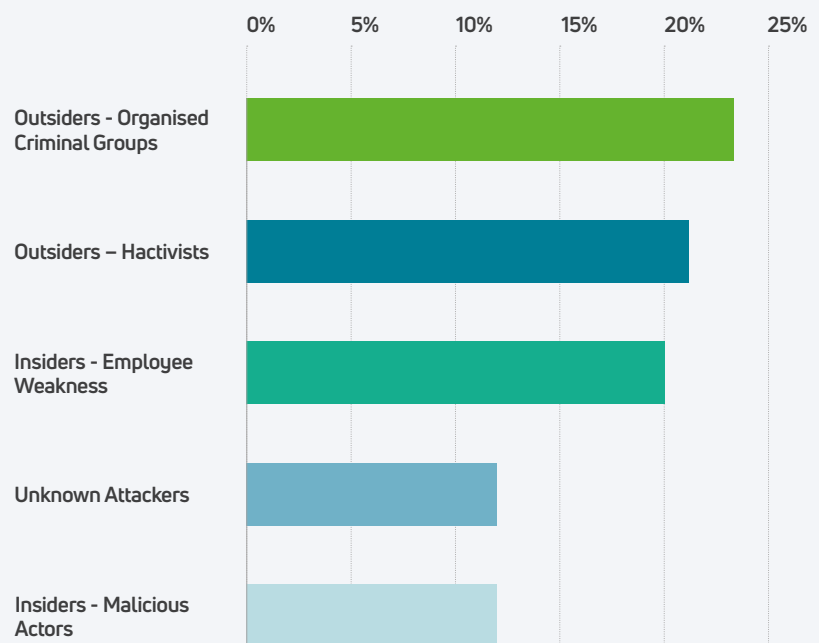
Ireland
Global



In the same Deloitte report, it shows that Irish management are generally aware of this situation with 65% of respondents stating they have a dedicated programme to address this risk (with the global average being 40%). The EY Global Information Security Survey 2020 report looks at different types of 'threat actors' ^[2] and found hackers are currently a growing source of threat, second only to criminal groups. ^[xviii] So, theft and ransomware are not the only motivations that cyber managers need to consider; the actions and investments of the organisation can be a motivator for an attack.

Diagram 3: Deloitte – Most Common Type of Threat Actors

Threat Actors Behind Confirmed Breaches



The EY report makes clear that innovations in technology are making it harder to maintain security: "What strikes you about business today is that technology is no longer controlled by IT because every new product and service is tech enabled in some way," says Vinod Jayaprakash, EY Cybersecurity Leader. "Unless you're working with those business partners, there will be all sorts of technologies being implemented across your business that are not even being considered from a security perspective." This doubles down on individual responsibility as well as education challenges. Thus innovations in technology can and do increasingly expose organisations to greater cyber risk.

^[2] Cyber threat actors is a broad category covering any individual or group undertaking malicious hacking activity.

Cyber-attacks are also happening in the Operational Technology (OT) side of business. The increased interest in IoT brings additional problems to OT as there is a greater exposure and an increased opportunity to attack manufacturing plants, utilities, oil platforms and even cement furnaces. In addition many expensive plants are still running on old software that is very vulnerable and very hard to patch.

A recent report from Centre for Secure Information Technologies (CSIT) confirms that attacks on Industrial Control Systems (ICS) and similar Operational Technology (OT) assets have increased by over 2,000 percent since 2018.^[xxx] In fact, the number of attacks targeting OT assets in 2019 was greater than the attack volume observed in the previous three years. Most of the observed attacks were centred around a combination of known vulnerabilities within Supervisory Control and Data Acquisition (SCADA) systems and ICS hardware components. There is a significant difference between the interest and attitude in OT versus IT security problems.

Gartner's analysis of Equifax CEO at the US congressional testimony following the Equifax hack in 2017 demonstrated a disconnect between executive understanding and levels of Cybersecurity capabilities in the organization. The final, subcommittee report issued in December 2018 indicated that "Equifax's CEO did not prioritize Cybersecurity".^[xx]

NTT's Global Threat Intelligence Report details the main threats to society from cyber crime. These include:

- Websites posing as 'official' information sources; created at an incredible rate, sometimes exceeding 2,000 new sites per day.
- Campaigns which distribute Malware variants.
- Attacks which spoof DNS via weak or default admin passwords.
- The use of an open redirect which pushes information-stealing, Malware to the affected system.

- Exploit attempts against a previously known, remote code execution vulnerability in Citrix Application Delivery Controller and Citrix Gateway devices.
- Cyber-attacks on healthcare and support organisations, like WHO responsible for helping people through this health emergency.

Organisations are increasingly relying more on their web presence through customer portals and web applications, thus increasing reliance on the systems which attackers have already been frequently targeting.

KPMG's All Hands-on Deck 2020^[xxxi] report makes clear that "Cybersecurity professionals need to demonstrate they can protect the heart of the transformed business with an agility of thought and action that recognises the pace and speed at which cyber-criminals operate."

Secretary General of INTERPOL, Jürgen Stock suggests that "Cyber-criminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19."^[xxii] An INTERPOL assessment of the impact of COVID-19 on cyber crime has shown a significant target shift from individuals and small businesses to major corporations, governments and critical infrastructure. Criminals are taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption.

Many of the organisations that monitor threats have come up with risk lists that all demonstrate that the criminals have intimate knowledge of the Cloud, networks, and systems. The array of attacks shows competence in innovation, agility, automation, and software engineering. All reports indicate that the risk of cyber crime will continue and could potentially increase with the maturing of AI. The Cybersecurity threat landscape is set to evolve and expand at an increasing rate; and with it the knowledge, skills and experience required within a Cybersecurity team.

6. Government and Cybersecurity

75%
of survey respondents identified key measures their organisations lack

Governments around the globe are increasing their investment in national Cybersecurity infrastructure and regulation, however the risks are not always fully considered at all levels. Juhan Lepassaar from ENISA, has suggested recently that the EU is naive when it comes to cyber threats and the use of 5G Networks (his role as a Director is to further prepare EU States from attack by building greater capacity). Legislation has now been created at national and EU level to deal with criminals through the courts system.

At the EU level, ENISA has produced a Good Practices Gap Analysis Report in May 2020, which made a series of recommendations to be considered by CSIRT Teams and Member States.^[xiii]

The gap analysis identified fields for additional work which included data harmonization, automated Malware analysis, cloud monitoring, sector-specific measures and information sources, routing monitoring and automated collection of spam. It found measures such as cyber honey-pots, network telescopes and monitoring of DNS requests are not universally deployed.

75% of the survey's respondents identified key measures which their organisations lacked, and it found the main obstacles to implementing these measures included insufficient financial and human resources, lack of management support, insufficient law authority, trust issues with implementation, lack of expertise, lack of cooperation of the network owners, high network load and data privacy regulations.

ENISA believes the top four proactive measures that most CSIRT teams should consider implementing are as follows:

- Endpoint monitoring with SIEM for teams with authority to directly monitor the IT infrastructure in their constituency.
- Network monitoring as a basic measure that should be implemented in all monitored networks.
- DNS network-oriented collection and analysis.
- Media monitoring of publicly available information: social media, especially Twitter to maintain a basic level of situational awareness.

Ireland has had to contend with three EU regulations over four years: the NIS Directive (2016), GDPR (2018) and the EU Cybersecurity Act (2019). The latter seeks to create certification standards and compliance processes for ICT products and services by 2022. Ireland has established some effective national infrastructure for cyber work, namely, the National Centre for Cybersecurity (national CSIRT), the Department of Justice and Equality Cyber crime division, and the Cyber Teams in the Defence Forces and An Garda Síochána. Northern Ireland has the NI Cyber Centre and CSIT at Queens University.

Over recent years there have been a number of industry focused initiatives undertaken in Ireland to address the issue of Cybersecurity.

The Cybersecurity Skills Initiative (CSI) was led by Technology Ireland, as part of Skillnet Ireland. It aimed to provide IT professionals with the skills they need to become Cybersecurity officers, ostensibly raising security standards across the country. Their view was to provide the workplace skills development needed to provide adequate protections, as threats evolve and grow. The initiative included a comprehensive plan to train 5,000 people in cyber-security skills across 4,000 companies. There were five key objectives in the plan, which is called 'The Road to Excellence':

- The creation of a Cybersecurity skills pathway.
- Organic skills growth.
- Cybersecurity as a business issue.
- Attracting young people.
- Continuous professional development.

Over recent months, much of this work has been taken over by the Blanchardstown Campus of the Technological University Dublin (TUD).

Cyber Ireland, is located in the Munster Technological University. Their purpose is to bring together Industry, Academia and Government to represent the needs of the Cybersecurity Ecosystem in Ireland. The aim is to enhance the Innovation, Growth and Competitiveness of the companies and organisations which are part of the cluster. This cluster approach should drive engagement and participation. Cyber Ireland has plans to set up local clusters outside of Cork and have conducted a recruitment, retention, and training survey to gather insight into the sector at the national level.

Through the Government-funded Human Capital Initiative (HCI), Munster Technological University (MTU) and collaborating higher education institutions, have secured in the region of €30 million to address priority skills needs in cybersecurity, work-based and lifelong learning, new models of engineering education, the health and life science industry sector, and investment fund management. HCI is an initiative targeted towards increasing capacity in higher education in skills-focused programmes designed to meet specific industry requirements. This funding will help to ensure that the new university's engagement interactions, informed by best international practice, continue to make an impactful contribution to sustainable development in the region and beyond.

We are making progress with some very important Cybersecurity initiatives and programmes.

While work is being done at a European level in terms of the need for policy and direction it can often be hampered by Member States ability to apply this at a local level. If staff or skill shortages also exist in the Government bodies involved in National Security, then this is likely to hinder implementation and operationalisation of new regulatory requirements. However, it can be expected that new regulatory requirements will continue to develop in both the EU and US and that these will affect many Cybersecurity teams in Ireland. The EU Cybersecurity Act, for example, is likely to require organisations to ensure certification of their ICT products and services.

7. Other Cybersecurity Trends

The research company Gartner, amongst others, states that the Board are now pushing back and asking for improved data and understanding of what they have achieved after years of heavy investment. They suggest investment in Cybersecurity will slow into 2023 with pressure on CIOs to focus on cost optimisation and quantifying the risk to value decision making.

Similarly, the Accenture report highlights a growing fatigue with Cybersecurity at board level while arguing that organisations need to step up security, moving beyond enterprise protection to ecosystem protection (e.g., supply chains) in order to maintain their defences.

A recent Forrester study, conducted in the US in April 2020, revealed similar concerns:

- Cybersecurity threats thrive amid a climate of uncertainty, making it a topic worthy of board-level visibility.
- Business leaders want a clear picture of their organisations' Cybersecurity posture, but their security counterparts struggle to provide one.
- There is a disconnect in how businesses understand and manage cyber risk and the reality that Cybersecurity needs to evolve as a business strategy.

This may result in some tension at board level to maintain the focus on Cybersecurity at a point when many want to reduce it. Pressure on cyber leaders to put forward reassuring strategies and quantifiable cases for future investments to the board will be a key skill area for the future.

There is a clear need to better educate executives at Board Level

Looking at technology, NTT, one of the leaders in Cybersecurity, suggest that one of the biggest trends in cyber is security orchestration, automation, and response (SOAR). 75% of threats now detected in their SOC are done by supervised machine learning and threat intelligence. The Winning the Game (2018) survey and report by McAfee also explain how automation is a growing trend in Cybersecurity and conclude that “62% of those who currently aren’t, say they plan automation in the next three years.”^[xxiv] This may lead to a decline in lower-level Cybersecurity jobs (e.g., SOC level 1) while increasing skill requirements at the next level up.

NTT foresees the need for AI and machine learning to “recognize patterns across applications and infrastructure, identify anomalies in those patterns that point to potential attacks, and orchestrate security controls automatically – and instantaneously...” Other important trends noted by NTT are the ‘threat shift’ from infrastructure to applications, hyper-scale pattern recognition and, of course, cloud security. Future programmes may need to focus on enhancing the skills of experienced Cybersecurity professionals in areas like AI, cloud, analytics, and automation.

McKinsey Consulting Group proposes that cyber leaders need to help the Board: make trade-off’s, treat Cybersecurity like a permanent capital investment, and recognise that a “tiered security approach” may be more effective than a “blanket approach”.^[xxv] They also argue that Cybersecurity teams must move from a passive to active defence approach imitating military style operations that integrate operations and intelligence into singular teams. This speaks to a training requirement in terms of cyber education at Board level.

It is important to note that there is important legislation that organisations need to be aware of and compliant with (e.g. the EU’s GDPR and the NIS Directive). The latest EU Cybersecurity Act will introduce an EU-wide Cybersecurity certification framework for ICT products, services, and processes. Furthermore, many organisations who are Cybersecurity service providers may be required to complete US based SOC 2 (Type 1 or 2) audit reports, these audits are increasingly being used to ensure service providers are securely managing client data. We believe that legal and audit requirements are likely to continue to drive requests for future training and consulting support.

8. Priorities in Cybersecurity Skills Development

The UK labour market report (March 2020) provides some detail on the current Cybersecurity skill gaps reported by respondents as well as priority skill areas for Cybersecurity in the future. Current skill gap areas are outlined in diagram below.

Diagram 4: Cybersecurity Skills in the UK Labour Market – Skills Gaps for Cyber Firms.

Figure 4.7: Percentage of cyber firms that have skills gaps in the following technical areas, among those that have identified any skills gaps.



Base: 169 cybersector of business identifying any skills gaps.

Information gathered from the interviews by the UK researchers found five key future skill areas for Cybersecurity to develop:

- Cloud computing.
- AI and machine learning.
- Threat intelligence.
- Internet of Things.
- Incident response.

The UK Report is a must read for anyone in Cybersecurity.

7%
of organisations see cybersecurity as enabling innovation

The UK Report provides several insights into structural gaps and priorities that are likely to be relevant to Ireland as well. These covered the need for a more joined up government approach, greater support for students/new entrants, greater university-training, and industry alignment, etc. (with a full list of recommendations in Appendix 1 of report). The UK report’s findings and recommendations could be easily compared to the earlier work done in the US, Australia, France, ENISA’s Gap Analysis and the EU’s Cyber Skills Shortage report.

In the EY Global Information Security Survey 2020, the starting point is that all organisations should be aiming for ‘security by design’. They believe Cybersecurity should not just be contributing to the latest app. design but inputting into all business processes (digital or otherwise) at the start. A culture of collaboration will be needed between Cybersecurity and the other business functions to do this. Their findings reveal that Cybersecurity is involved in only 36% of new business initiatives and that only 7% of organisation see Cybersecurity as enabling innovation (and are more likely to view it as compliance driven).

KPMG’s All Hands On Deck 2020 report explains that cyber teams are typically “a collection of technical, operational compliance professionals” who need to become a “more strategic, forward-looking resource” that “listen to different perspectives and communicate more with business heads about what the organization really needs to worry about in this evolving ecosystem.” They suggest a greater need for collaboration, communication and business acumen is needed by cyber professionals to become trusted partners. The language is remarkably like that used for HR. professionals as they transitioned to business partners.

ENISA’s Cybersecurity Skills Development in the EU report (2019) found many issues with Cybersecurity education: “lack of educators, poor interaction with industry, little understanding of the labour market, outdated or unrealistic platforms in education environments and difficulty keeping pace with outside world”.

A key quote in the report (Conklin, Cline, & Roosa, 2014) was: “One of the biggest concerns in Cybersecurity education is students’ lack of hands-on experience, resulting in a skills mismatch between what the industry would like to see in a candidate and the skills that they actually possess.” This is consistent with this research and points to the need for ‘hands on’ skill development programmes for students/early entrants in Cybersecurity and may increase the importance of short form training interventions. One example quoted by practitioners was the idea of a bridging course between university and employment to give graduates more practical skills that make them more job ready.

9. Conclusions from Desk Research

The desk research summarised in this chapter informed the design of the Training Needs Analysis survey. The results of that survey will be used, in conjunction with all the research inputs, into the development of the it@cork Skillnet strategy for Cybersecurity up-skilling.

Cybersecurity is a dynamic industry that is still in its infancy. It is clear that competent people with pertinent capability are required as both society and industry struggle to protect themselves from the growing sophistication of criminal attacks.

Cyber teams require appropriate skills, time, tools, and resources to do this job properly. While it is the responsibility of each organisation to provide sufficient funding for Cybersecurity, there are multiple actions on a Government and European Union level that can help these teams to improve their capabilities.

Cybersecurity risks are creating the same challenges for public and private sector employers. While demand for Cybersecurity employees may have slowed somewhat in 2020, all the reports indicate that there will be continued growth in cyber threats and therefore continuing pressure on Cybersecurity teams to perform.

The evidence suggests recruitment, management and training expectations around Cybersecurity are not properly aligned with the labour market(s) nor with the pace of change within the industry. There is a likely need to re-frame the people processes of engagement, attraction, recruitment, training, career development within many organisations to ensure teams are fully equipped to handle the many future challenges coming their way. The Infosec 2020 IT & Security Talent Pipeline Study (US) found that companies who put in place best practice talent processes are 11% less likely to encounter hiring challenges.

Technology advancements will also create demand for new skills within Cybersecurity teams, AI/machine learning, cloud, containerisation, the list goes on. This is likely to create pressure for Cybersecurity employees for a deeper and broader skill set, requiring a range of specialised training for teams.

The threat landscape and ecosystem that needs defending is growing now requiring many cyber teams to cover supply chains, operational technology (OT), containers, cloud, etc.. With this comes new skills, systems and processes that need to be managed from a Cybersecurity perspective.

Regulations and auditing requirements are likely to be a growing requirement for many Cybersecurity teams. The new EU legislation addressing cyber certification will likely become a key skill / education need in the near future. Other teams operating or seeking to operate in the US may need to conduct SOC 1 or 2 audits.

The American Institute of Certified Public Accountants created the System and Organization Controls (SOC) security audits in 2011. Type 1 looks at security design and Type 2 at security operations over a period of time.

Many proponents are seeking to bring about changes in how Cybersecurity teams and leaders operate; active defence, security by design, trusted partners, cyber resilience, cyber risk appetite, etc.. This, on top of the legislative, technological and threat landscape changes all point to significant skill gaps (and shortages in some areas) remaining well into the future.

In summary, the literature review suggests that:

- Organisations are going to need support for the development of new skills for Cybersecurity in relation to a range of emerging technologies.
- Organisations will likely need to ramp up the investment in Training and Development (T&D) with support to undertake this in a structured and strategic way.
- New entrants will need hands-on experience to gain a foothold in the labour market, experienced employees will need continued support to up-skill.
- Expert panels will be needed to help formulate and keep training paths updated given the rapid pace of change in the industry.
- Transversal (soft) skills will be increasingly important to foster greater collaboration and learning agility within Cybersecurity functions.
- Cyber leaders will need help to deal with the increasing challenge of delivering a robust Cybersecurity system across a broadening ecosystem and will require support in managing the expectations of the Board.

There are many implications from the above for the development of the it@cork Skillnet Cybersecurity training strategy.

SECTION FIVE

Market Review



Market Review of Cybersecurity Training Providers

This section of the report concentrates on up-skilling solutions in the enterprise space, focusing on agile, online training options that could be utilised by it@cork Skillnet in future training programme delivery.

This section also takes a wider look at Cybersecurity frameworks, career paths and other learning initiatives and trends that could be pertinent to future it@cork Skillnet programmes.



In the review we discovered first that there are two main types of provider for online Cybersecurity training:

- Online training providers with either a specialisation in Cybersecurity or a broader ICT.
- Niche training providers with particular focus on one area of Cybersecurity (e.g. penetration testing, secure coding, etc.) or with a narrow training delivery focus (e.g., simulation training).

However, the main purpose of this review is to examine the leading online Cybersecurity training providers to identify those that might provide a good solution to common training requirements that it@cork Skillnet might be called upon to address in the future.

The leading online training providers were reviewed against a range of criteria such as their speciality focus in relation to Cybersecurity, breadth of courses, learning methodologies employed, etc..

One notable challenge in this review was assessing the quality of course providers as the leading providers generally have extensive course lists in the hundreds with each likely to vary in quality.

This indicates that when developing future Skillnet programmes, a side-by-side quality review of specific courses from a short list of providers would be required.

Online Training Providers

Overall, we found the market offers some compelling online, training options to either support or replace classroom-based training.

Table 3 provides the summary of the leading online Cybersecurity training providers. See Appendix 2 for further information on these providers.

The first step in this review was to identify those online providers who have a significant and broad focus on Cybersecurity training. At this point Massive Open Online Courses (MOOCs) providers were left out of the review as they tend to cover a broad spectrum of topics and quality can often be a concern (e.g. some operate as 'open' platforms for any instructor to add courses). Also left out were providers offering primarily Cybersecurity vendor/product training and related certification. Finally, cyber awareness training providers are not covered in any depth in line with the project's focus on skills.

The online training providers reviewed in depth were those that provided the broadest range of training across the Cybersecurity domain. Our review looked at the Cybersecurity training providers to identify their relative strengths against different types of common training needs. We found that they did have different strengths and specialties with the leading providers utilising a broader range of learning methodologies and modularised content to suit a wide range of needs.

Table 3: Online Cybersecurity Training Provider Comparison.

Provider Need/Fix Matrix	Infosec	Pluralsight	Immersive Labs	Sans Institute	Cybrary	Ciracadence	Secure Ninja	IRange-Force	ISC2	EC Council	O; Reilly
Instructor Training				√			√		√	√	√
Entry/Basic Skills Training	√	√	√	√	√	√	√		√		√
Certification Based Training	√	√		√	√		√		√	√	√
Team Simulation Training	√		√	√		√		√			
Advanced Courses/Labs	√	√	√	√			√	√	√	√	√
Online Tutor Support	√	√		√			√		√		√
Cyber Manager Training				√							√
Executive Development				√							
Cyber Awareness	√			√					√		√

The review found that many of the Cybersecurity training providers were advanced in their offering to the market with some leaders in terms of using gamification/ simulations for learning (i.e., early capture the flag events); a few now make this a central part of their learning methodology. Similarly, many others provided practical online labs with access to relevant software tools to deliver hands-on learning experiences.

Also, some of the online providers (e.g., Pluralsight and Infosec) have advanced learning management systems which may appeal to organisations undertaking extensive Cybersecurity training programmes. Of note, most of the leading online providers were based in the US and to a lesser extent the UK. One interesting gap noted when conducting the reviewing was the limited number of courses targeting the development of Cybersecurity managers and senior executives.

The review found that costs vary widely across the training providers depending on the delivery option selected. Below are some examples for some different Penetration Testing training options:

- Infosec – Penetration Testing 10 Day Online Bootcamp – 10 days online bootcamp instruction plus 3-month access to the learning platform for support modules: \$7,415 (USD).
- Sans Institute On-Demand - SEC560 - Network Penetration Testing and Ethical Hacking (4-month online access to six online video modules and 30 labs): \$7,020 (USD).
- Offensive Security – Offensive Security with Kali Linux - online video modules, course manual, 70 labs plus OSCP exam certification fee – 90-day access: \$1,349 (USD).
- Pluralsight – CompTIA PenTest+ programme – includes 10 courses with 22 hours of online learning plus a practice exam (with further access to 30+ other short penetration testing courses and the wider library): €410 for annual membership.

In summary, there is a good range of online Cybersecurity training options, with each provider offering something a bit different from the others. While online training is efficient and cost effective for skill development it is not always the best or sole solution, particularly as Cybersecurity is a complex technical domain in which learners can often benefit from direct instructor support, especially for new entrant training (as recent experience from an it@cork Skillnet programme confirms). However, for foundation or intermediate training delivered in an agile fashion, then the market offering for online training solutions looks quite compelling.

Specialist Training Providers

When considering more advanced Cybersecurity training requirements there are a range of specialist providers who may offer in-depth solutions. Our review found many providers who have specialised in niche areas within Cybersecurity (listed below).

Specialist Training Providers

CyberPrism	Cybersecurity Risk Management
Fairy Institute	Cybersecurity Risk Management
Secure Code Warrior	DevSecOps
Offensive Security	Pen Testing/Hacking
Evolve Academy	Students/Advanced Penetration Testing
Treehouse	Secure Programming
MIS Training Institute	Cybersecurity Auditing
Threat Sim	Anti-Phishing
Infosecure	Awareness and Cyber Culture Assessment
Pop Corn Training	Security Frameworks
Vigitrust	Data Protection
Cyber Bit	OC simulation and security tool training
Security Innovation	Platform, Languages and Frameworks, Simulations
CompTIA	Full range of Cyber Certification Training paths
Try Hack Me	Pen Testing/Hacking Gamified Simulations and Bite Sized Lessons
ISACA	Cybersecurity Training/Labs with in-house Credentials
Phish Labs	Cyber Intelligence

Finally, there is a range of training providers who specialise in cyber awareness training and many of these companies offer supporting behavioural change programmes, for example:

- Inspired E-Learning.
- Media Pro.
- Proofpoint.
- KnowB4.
- Cofense.
- Terra Nova.

Training Trends

The industry needs a common standard and framework for the development and delivery of micro credentials

This section provides a short summary of some of the recent training trends that are of relevance. One of the key trends of late is micro-learning where training is delivered in small, bite sized chunks (on average 15 minutes in duration).

This approach to learning could be useful in terms of maintaining the knowledge and skill base of experienced Cybersecurity employees, given the limited training time available; it also lends itself to learning on mobile devices.

Similarly, accelerated training programmes focusing on a particular set of skills as part of a profession (e.g. network management) are becoming prominent; resulting in the use of micro-degrees, micro-credentials and digital badges. Aligned to this digital certification, badges are also becoming more common as learners use these to add to their social media profiles. While these micro credentials and badges can be appealing to some learners, a recent Skillnet Insight paper argues that there is not yet a common educational standard or ecosystem framework to define exactly what each of these really mean and their relationship to each other.^[xxvii]

Gamification and virtual simulations have advanced significantly over the past decade. There are a number of providers who now specialise in immersive simulations e.g., Immersive Labs, Cyber Bit, Range Force and Circadence. The benefits of this approach in terms of learning and retention are that it allows participants to see the impact of their decisions in a safe environment (particularly important for Cybersecurity) and furthermore a realistic simulated environment aids increased retention. It is also particularly useful in terms of facilitating team development.

Research by the eLearning Industry magazine forecasts a small decline in the self-paced e-learning segment in 2021, as evaluation evidence finds that learners are less likely to complete modules in this format. However, the overall e-learning industry is set to grow threefold by 2025 driven by growing acceptance for the need for lifelong learning and re-skilling, indicating the uptake of more blended approaches. This growth is also supported by research into the efficiency and effectiveness of e-learning. Brandon Hall's HCM Outlook Survey showed that e-learning reduces employee training time by as much as 40-60%.^[xxviii] This is important for many organisations and training managers where participants need to absorb significant amounts of information over a relative short period of time (particularly relevant in the ever-changing Cybersecurity sector).

Cyber Training Initiatives in Ireland

There is room for more traineeships similar to the ITAG conversion course to aid graduates into the workplace

See the following sections regarding this

As part of our Market Review, we conducted a search to ascertain the number of active, non-university, Cybersecurity initiatives in Ireland helping to train and transition people into Cybersecurity sector. At the time of this review there were:

- Skills Connect Initiative from Skillnet Ireland.
 - ICT Skillnet Future in Tech – remote blended programme for people seeking a career as a Cybersecurity specialist (comprising three certifications - CompTIA, Prince2 & Security Fundamentals). This is one of 7 ICT pathways.
 - it@cork Skillnet’s Cyber Employment Activation Programme (CEAP) and CyberQuest – remote blended programme for people seeking a career in a range of Cybersecurity roles. This programme was piloted in 2020 with a focus on migrant women and is now fully rolled out in 2021 as CyberQuest (www.cyberQuest.ie).
- Innovation Technology AlanTec Galway (ITAG) – Cybersecurity Online Conversion Course (10-week online programme – regional focus).
- ITAG – Certified Information Systems Security Professional (CISSP) programme (a 5-day bootcamp – regional focus).
- FIT ICT Associate Apprenticeship - Cybersecurity apprenticeship running over 2 years (in partnership with Solas/ETBs).
- Tech Learn (Software Skillnet) – access to Pluralsight/O’Reilly learning platforms for Small and Medium-Sized Enterprises (SMEs) with topics covering a wide range of professions including Cybersecurity.
- Technology Ireland ICT Skillnet offering includes:
 - Virtual Capturethe Flagevents.
 - ICTSkillnet CISCO Networking Academy (free).
 - Certified Cyber Risk Officer course (CCRO).
 - Master of Science in Cybersecurity.
- Cybersecurity Skills Initiative – a broad public/private sector initiative launched in 2018 focused on developing a national skill development programme. Several foundational and cyber management courses are provided via Skillnet Ireland on an ongoing basis.

University Cybersecurity Programmes

Our review also found that there are a wide number of Irish university programmes that either fully or partially cover Cybersecurity.

We did not find a centralised statistical source to measure the number of Irish Cybersecurity graduates, however, looking at these 16 programmes and estimating 10 graduates per year there is likely a supply of about 160 university-trained entrants into the Cybersecurity labour market each year.

Anecdotal and first-hand evidence suggests many graduates are struggling to find positions and our research into job postings showed that employers are primarily seeking experienced hires. The research group believes that this points to a mismatch in supply and demand that requires further investigation and will be key to it@cork Skillnet’s strategy for Cybersecurity.

Table 4: Irish (ROI) University Programmes for Cybersecurity

BACHELORS	
Institute of Technology Carlow	Bachelor of Science (Honours) in Cyber crime and IT Security
Waterford Institute of Technology	Bachelor of Science (Honours) Computer Forensics and Security
Technological University Dublin	Bachelor of Science in Computing in Digital Forensics and Cybersecurity
University of Limerick	Bachelor of Science (Honours) in Mobile Communications & Security
Limerick Institute of Technology	Bachelor of Science Data Analytics & Cybersecurity
Letterkenny Institute of Technology	Bachelor of Science in Computer Security and Digital Forensics

Table 4: Irish (ROI) University Programmes for Cybersecurity

MASTERS	
Munster Technological University	Master of Science in Cybersecurity
University College Cork	Master of Science Cyber Risk for Business
Athlone Institute of Technology	Software Design with Cybersecurity
University College Dublin	Master of Science in Digital Investigation & Forensic Computing
Dublin City University	Master of Science Security and Forensic Computing
National College of Ireland	Master of Science in Cybersecurity
Griffith College Dublin	Master of Science in Network and Information Security
Technological University Dublin	Master of Science in Computing (Applied Cybersecurity)
University of Limerick	Master of Engineering in Information & Network Security
Letterkenny Institute of Technology	Master of Science in Computing in Cybersecurity

Source: *Cyber Ireland and University websites*

Knowledge and Skill Frameworks

This section discusses some of the knowledge and skill frameworks that can provide support and direction for training and development programmes.

Our review found that there are several bodies that now provide technical, organisational and role-based standards to support the development of an organisation's Cybersecurity function. The leading standards and frameworks for knowledge and skills include:

- National Institute of Standards and Technology (NIST) – this leading framework (developed initially by the US Dept. of Commerce) defines Cybersecurity roles and task requirements along with associated learning guidance. It draws on a variety of IT standards to create a job framework. Although not marketed as a maturity model it provides tier progression like CMMC and other frameworks. Its education arm (the National Initiative for Cybersecurity Education - NICE) provides awareness training.
- Skills Framework for the Information Age (SFIA) – a non-profit organisation based in the UK offering job and competency / skills framework with a focus on software, cyber, big data, AI, digital and DevOps roles. This is a useful first port of call for more detailed job descriptions as it provides detailed information on knowledge, skills, etc. compared to other frameworks.
- The Att&ck (e.g. Adversarial Tactics, Techniques, and Common Knowledge) framework was developed by Mitre in 2013 as a body of knowledge focused on classifying cyber- attacks in terms of their routes and techniques to gain entry. This framework has been used then by organisations to help evaluate vulnerabilities, penetration tests, red hat exercises and skill development.
- European Union Agency for Cybersecurity (ENISA), launched in 2005, focuses on policy, research and education. It is currently developing a European Cybersecurity Skills Framework.



There are many other bodies that focus on standards and best practices in Cybersecurity, some with free access and others fee paying.

Below are a sample of some of the leaders:

- ISC² – an international body that manages a Cybersecurity body of knowledge used to guide and support their security training and certifications (e.g., CISSP) processes; they operate a fee-paying model.
- Cybok – the recently launched Cybersecurity Body of Knowledge's (BoK) codifying the Cybersecurity knowledge, developed by UK academia in conjunction with the UK's National Cybersecurity Centre. This framework offers a useful foundational knowledge tool for new entrants. Appendix 3 provides an overview of this BoK.
- First – is a leading global association for incident responders offering protocols, forums, best practices, and standards in the management of security incidents (e.g., NSCS is a member).

There are also numerous national bodies also developing job/skill frameworks for Cybersecurity including initiatives in Australia, Canada, Israel and Singapore. These offer alternative options or benchmarks for organisation's considering developing a framework.

Quality and Capability Frameworks

Capability frameworks help organisations evaluate their processes and practices across the different domains of a function to identify areas for improvement. Originally developed in the 1990s for software development they were then adopted by a number of large US government departments. Quality standards originated much earlier in the 1940s to agree measurement standards for industrial use and then grew to cover quality standards for IT, production, environment, etc..

- We found several standards and capability frameworks that can help organisations assess the capability of their Cybersecurity function. These include:
- ISO/IEC 27001 – Sets out a baseline for a range of information security practices and their dependencies with other security domains; provides organisations a well- recognised international quality standard.
- Centre for Internet Security – this US institute defines basic and advanced standards (controls and best practices), with their Top 20 as the baseline standard for defence against cyber threats.
- CM2M – Developed by Dept. of Energy in the US to improve cyber readiness of utility companies, covers 10 different cyber domains.
- CMMC – Cybersecurity Maturity Model Certification (newly issued in 2020) is used primarily by contractors working with the US’s Department of Defence.

All management consultancies have developed their own in-house maturity and ‘resilience’ models and job frameworks (e.g., IBM) as part of their offering to the Cybersecurity sector. In Ireland, the Innovation Value Institute (IVI) has started work on expanding their IT maturity model (IT-CMF) to encompass Cybersecurity. However, what seems to be missing now is a maturity model appropriately pitched for SMEs.

In summary both skill frameworks and maturity models can usefully underpin a large Cybersecurity development programme ensuring that the framework/model choice is well recognised, robust, and updated to ensure relevance in a rapidly changing sector. There are numerous management consultancy and training providers available to support organisations through this type of programme. Research for this project indicates that a potential lack of maturity in Cybersecurity is prevalent and therefore these types of solutions might be part of a future Skillnet offering.

What seems to be missing now is a maturity model appropriately pitched for SMEs

Cybersecurity Jobs

Table 5: Selection of Different Job Postings for September 2021 (job post count)

JOB GROUP	COUNT
Sales	4451
Software	4150
Project Management	3509
Operations Management	1752
Risk Management	1667
Accounting	1384
Law	1350
Auditing	1099
Tax	1005
Programming	965
Web Development	533
HR.	509
Cybersecurity	300
Management Consulting	257
Data Scientist	162
Cloud Architect	140
Network Administration	105
Hardware Engineer	42

Identifying the actual number of Cybersecurity jobs in Ireland for this part of the report turned out to be a difficult task as the Central Statistics Office (CSO) and other government agencies provide statistics covering only the wider field of ICT.

This prompted us to conduct a LinkedIn ‘job scrape’ exercise to provide an actual view of possible Cybersecurity job opportunities in Ireland. The initial search was for ‘Cybersecurity’ jobs posted in the month of September 2020 and we found 300 job postings. We then did a similar exercise for other job groups for comparison (see table), which showed that Cybersecurity jobs postings are 1/14 of those posted for Software.

We then reviewed the 300 jobs and reduced these down to 178 clear Cybersecurity job postings (i.e. we removed obvious duplicates or mis-postings). We found that the most common job titles were Cybersecurity Engineers (11%), Consultants (10%) and then Analysts (7%) with the remaining job titles spanning a broad range of different type of roles (see Appendix 4a). We noted that 70% of these postings were based in the Dublin region. We found that the vast majority of those posted were described as entry level positions however required around 5 years of experience.

From these 178 job postings we found that there were 105 different employers hiring across a broad spectrum of sectors (see Appendix 4b). This exercise revealed that there is still active demand for Cybersecurity employees in this current period of uncertainty, however, the overall demand is much smaller compared to many of the other common job groups. Our qualitative interviews with recruitment companies also identified that typically there are 200-300 Cybersecurity jobs posted at any one time and this exercise confirms this.

Note: In December 2020 this exercise was repeated and found a similar count (306 unfiltered job postings for Cybersecurity) however in May 2021 the same exercise indicated 665 jobs which equates to a doubling.

Career Entry Points

Our research found at this point in time a very limited number of graduate programmes providing an entry point specifically into Cybersecurity within the private sector in Ireland. These were:

- HPE Graduate programme (Graduate Information Security Analyst) and an employee trainee-ship programme.
- Accenture Cybersecurity Graduate Programme 2021.

We conclude that while Cybersecurity may be a growing profession it is relatively small compared to other more established professions. Additionally, there are very few entry level roles in this sector.

Cybersecurity Career Paths

Career paths come in many forms however, in the past few decades the emphasis has changed from the traditional hierarchical paths to more lateral paths. The decline in loyalty and commitment between employer and employee has led to shorter tenures with employees more inclined to switch employers to develop their careers. With the pace of change increasing across most industries, employees need to increasingly up-skill/re-skill to stay relevant in the labour market. Similarly, employers seem to have become less willing to train new employees or offer career paths to guide progression within their organisation. In our research into the Cybersecurity sector we have also encountered an increase in essential requirements for new entrants into cyber and across ICT in general (e.g. must be able to 'hit the ground running').

From the beginning Cybersecurity has often been a responsibility within more generalist IT roles, especially within smaller and medium sized organisations. Entry into the field of Cybersecurity has been attractive for technical professionals and the 2019 SEI survey found 58% of Cybersecurity professionals had previously worked in IT, Software Development, or Engineering.

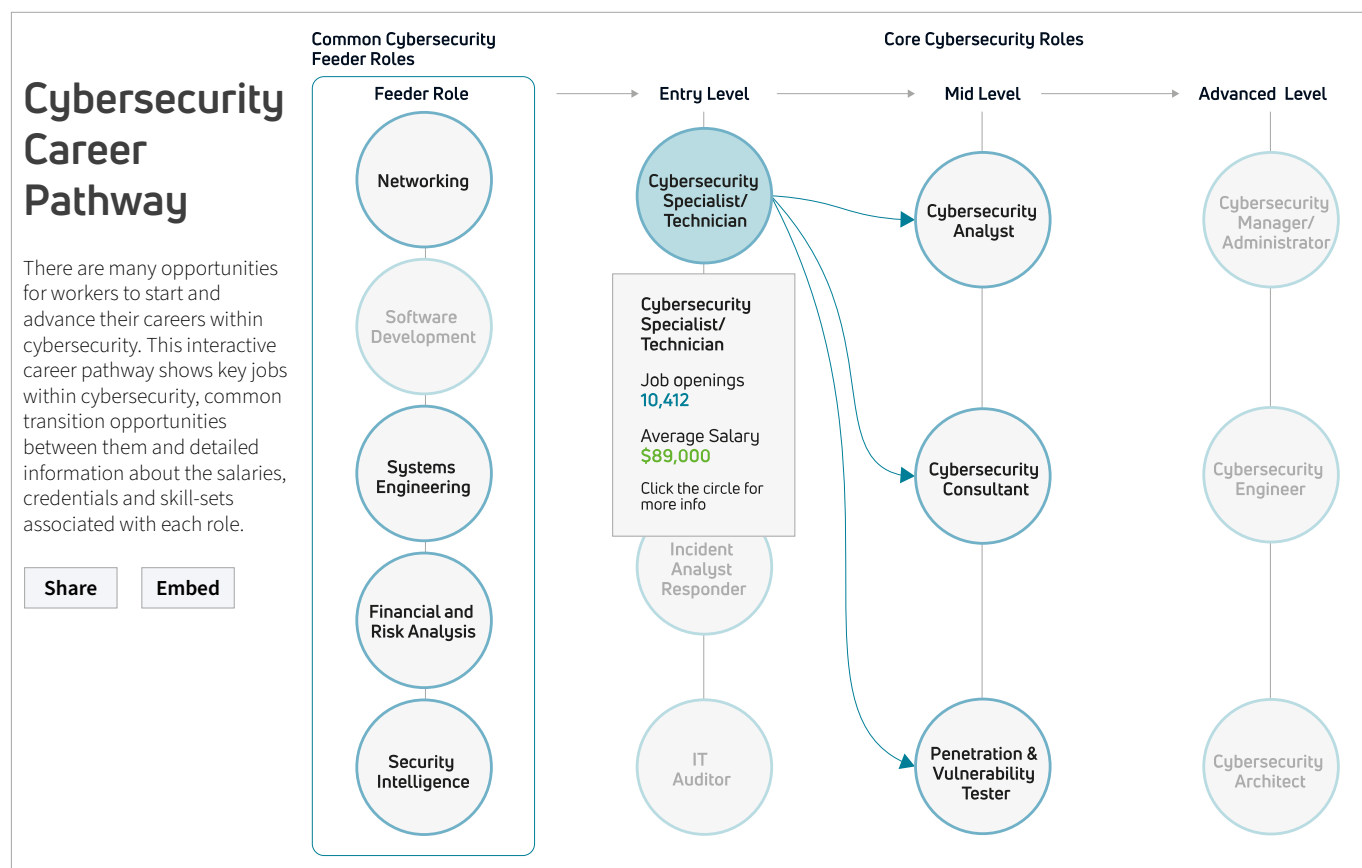
^[xxviii] Cybersecurity is a complicated profession to map as it can be centralised in places (e.g., SOCs) and diffused into others (Network Admin). It is not always a distinct job family as responsibilities can be found in different areas across an organisation (e.g. the development of the DevSecOps role in DevOps). However, it is important to define career routes within a sector if it intends to attract new entrants into the field.

Our review found there is less information publicly available on Cybersecurity career paths as there is on other jobs and skills. SFIA, for example, provides detailed information on jobs and skills but no information on different career routes into and around Cybersecurity. Some of the online training providers noted earlier set out Cybersecurity training streams linked to career paths (or starting points) but provide little information in terms of the routes and skills required to navigate these (unless perhaps implicitly through a series of aligned courses).

We found that there are some organisations taking steps to define career paths (mostly in the US) to address the skill shortage/gaps they are facing. Some US agencies have developed and published some interactive tools that set out different career paths with cyber.

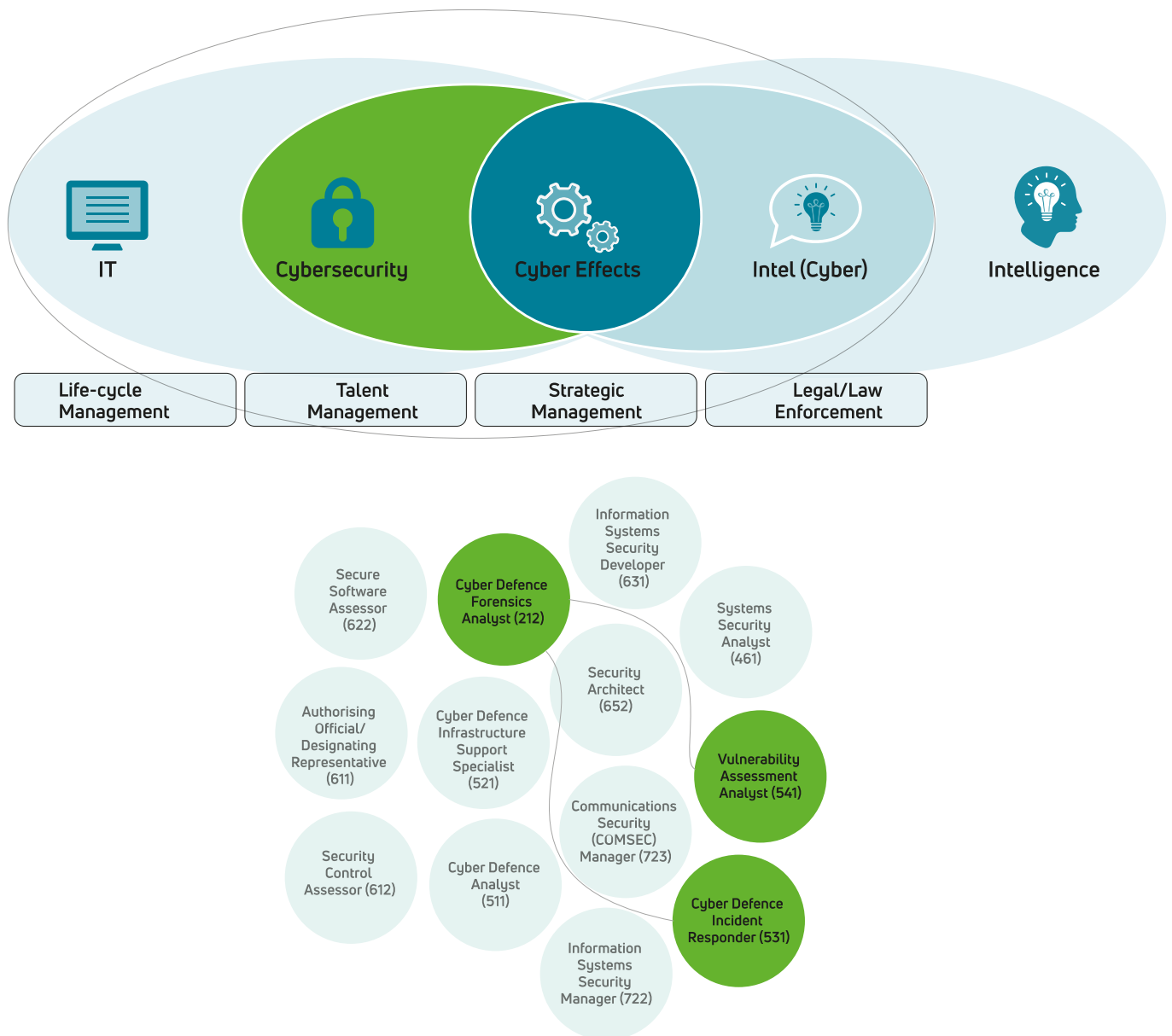
- CyberSeek – a consortium of partners in the US led by NICE that provides detailed information on the Cybersecurity labour market by State put together a simple but interactive career path tool. Each job in the tool is supported by labour demand and salary expectations information.^[xxix]

Diagram 5: CyberSeek’s Career Pathway tool (overview)



NICCS – the National Institute for Cyber Careers and Studies (US) offers a full range of jobs and detailed career paths across IT, Cybersecurity and Intelligence (along with a broad range of education information).^[xxviii] This tool allows for side-by-side job comparisons (covering tasks, knowledge, skills, abilities and capability indicators).

Diagram 6: NICCS Cyber Career Pathways Tool (overview)



These tools highlight a broad range of Cybersecurity entry point roles: analysts, consultant, SOC operative, penetration tester/ vulnerability analysis, incident responder, security auditor, risk officer. Our research points to a clear gap in Ireland in terms of defining, measuring, and monitoring Cybersecurity career paths matched to actual labour demand in Ireland. An initiative covering this gap would encourage and direct potential new entrants and help employees/employers/educational institutions invest in the right skills.

Conclusions from Market Review

The main purpose of this review was to examine the Cybersecurity training providers and here we found that this space is well served with a broad range of providers in this field. Some of the providers offer advanced, online learning platforms, gamification and simulation exercises to support the learning process and offer cost effective options to help individuals up-skill/re-skill in this field. We also found a full range of specialist training providers as well as traditional providers offering classroom training.

There are a number of well-respected job/skill frameworks available to support skill programmes providing credibility and a quality check to any new initiative. In fact, many of the training providers that were reviewed state they do this mapping already, often using the NIST and/or the Att&ck frameworks for this purpose.

Research has found that purely online, self-paced training can result in higher drop off levels (of trainees) compared to instructor led programmes. To ensure high completion rates future programmes should consider cost effective ways to blend online training with instructor support. Some of the online training providers state this is part of their offering and the quality of this support should be explored when selecting future online training providers.

Perhaps of most significant finding is the need for further research into the supply and demand in the Cybersecurity labour market within Ireland. We established that there is a notable supply of graduates entering the market and a broad range of organisation's seeking employees however, very few offer entry level jobs. This suggests a need for support structures to help new entrants gain practical Cybersecurity experience and a foothold into this sector and for employers to become more accepting of the need to invest in new entrant training and development.

Future programs should consider cost-effective ways to blend online training with instructor support

A shared investment in job training and work experience could give new entrants the boost to start their careers in this sector. This investment, in turn, could widen the cyber talent pool in Ireland and improve its standing as a place to start or expand a Cybersecurity operation.

We believe that an important element of support should also include the development of realistic career path guidance within Ireland that accurately defines the demand from employers in terms of likely/in-demand Cybersecurity roles and skills. This will better enable universities and students to evaluate how likely a Cybersecurity programme will equip individuals to find roles in the Cybersecurity sector.

In summary, more needs to be done to ensure the right supply of new entrants are coming into the job market with the right skills. This is something that can be addressed through collaboration among the Skillnet groups as well as support from industry bodies like Cyber Ireland.

A group of business professionals are seated in a circle on a light-colored wooden floor, clapping their hands. A woman in a white dress stands on the right side of the frame, gesturing with her right hand towards the group. The background consists of large windows with a view of greenery outside. The overall scene is brightly lit, suggesting an indoor setting with natural light.

SECTION SIX

Qualitative Research

Qualitative Research (Interviews)

This section of the report covers the feedback from the qualitative interviews. The purpose of the telephone interviews was to collect as wide a set of views as possible from people involved in Cybersecurity. The aim of this was to help with the design of the TNA online survey and directly input into the need's identification itself.



Three key, distinct groups were identified for the telephone interviews:

- a. Talent Group – people involved in the recruitment for Cybersecurity roles. This was a combination of recruitment agencies and in-house talent acquisition specialists. This group also included views from universities and Government agencies (Enterprise Ireland and IDA).
- b. CISO Group – this group comprised of senior leaders that are managing Cybersecurity functions and teams in Ireland.

- c. Vendor Group – this group of people work in companies that provide Cybersecurity services and products to Irish industry.

A fourth small group, the New Entrant Group, was added later, although not part of the original design (included as a short addition to this section). This was a group of recent graduates that have been identified as wanting to start careers in Cybersecurity. This group of people were canvassed to ensure that as broad a set of views as possible was evaluated as an input to the TNA design.

There was a high level of willingness to participate in this interview process

92%
of priority contacts were interviewed as part of this research

Interview Design

These covered the following six broad topics using an 'open questioning' research technique:

1. Cyber strategy.
 - a. Level of importance to business performance.
 - b. Outlook for the future.
2. Cyber Risk Evaluation.
 - a. Maturity Levels.
 - b. Current Gaps.
 - c. Tools and approaches.
 - d. Critical risks.
3. Awareness Levels.
 - a. Levels of employee awareness.
 - b. Priorities for employee awareness.
 - c. Gaps and issue.
4. Basic and Advanced Cyber Skills Training.
 - a. What training is provided?
 - b. Gaps.
 - c. Priorities.
5. Emerging and Future Skills.
 - a. Key trends.
 - b. Critical Priorities.
6. Management of Cybersecurity Resources.
 - a. Resourcing and Recruitment.
 - b. Challenges.
 - c. Supports from it@cork Skillnet.

The interview followed a semi-structured format using the above questions as a standard template. Interviews typically lasted 45 to 60 minutes (on average). There was a high level of willingness to participate in this interview process. An initial target list of priority contacts was produced and 92% of this list were interviewed as part of this research.

A. The Talent Group

There is a short-term focus on resource acquisition with little structure around building and developing a long-term cyber talent pool

The Talent Group interviewed for this research was a mixture of cyber specialists in recruitment companies as well as in-house recruitment and training managers. This group of people play an obvious and central role as they are the conduit between the organisation, the hiring managers, and the marketplace.

This clearly means that they have a somewhat unique contextual perspective on the internal organisational drivers and capabilities, the recruitment behaviours and practices as well as the labour market conditions. Recruitment and training are therefore critical elements of the Cybersecurity value chain. The research gathered from this group is dominated by a set of specific perceptions around what needs to improve around the skill/labour market, for example:

- There is a mis-match of expectations between the levels of experience and capabilities required by companies against what is actually available in the domestic and international market supply. This is sometimes quoted as one of the reasons that recruitment lead times in Cybersecurity is sometimes a problem.
- Although some companies invest in internship programmes, overall the industry is falling short on having a strategic and sustainable approach to long term skill and capacity building for Cybersecurity.
- The short-term importing of Asian and eastern European resources to fill vacancies is an often quoted example of the opportunity and challenges that shape the current skills landscape for Cybersecurity.
- There was also a reflection from this group that identifies some of the internal organisational challenges. Many organisations do not have mature tools and frameworks to develop competency models and resource capacity plans that are specific to cyber risks. This in turn may limit efforts to define roles and subsequently training needs.

- Cyber is rapidly evolving and this means that the nature of the roles is also rapidly changing. This creates challenges on many fronts including balancing the relative priority of cyber against other ICT domain priorities as well as the ability of the organisation to define job roles. Developments, for example, in OT, DevSecOps, digital transformation, AI, makes it difficult for organisational designers to draw up job specifications and training plans for cyber.
- There is also a view that business risk associated with cyber threats is not well understood by senior management. This is one reason quoted for the slow maturing of the sector by talent specialists.

The examples quoted above are perceived as the barriers to having a sustainable and strategic labour market. One of the central themes for this group was the perceived 'barriers' to a healthier and more sustainable labour market for Cybersecurity resources.

B. The CISO Group

There is a view from this group that most organisations in Ireland do not have a dedicated Chief Information Security Officer (CISO). In larger organisations there is an impression that where CISO roles exist, they typically will not be in Ireland.

The CISO role is a fine balancing act between a set of potentially conflicting forces. The skill requirements at the CISO level can be summarised as follows:

- Managing the expectations of the board and gaining support for a roadmap of investment and funding.
- Keeping abreast of the security threat landscape.
- Constant review of security controls, governance and risk oversight.
- Balancing typically scarce and hard-fought ICT budget.
- Development of a strategy that can future proof the delivery of effective Cybersecurity in a constantly changing crime environment.
- Manpower planning and organisational design of cyber teams.

C. The Vendor Group

The Vendor Group tend to look at Cybersecurity through two specific lenses: can they identify companies who are willing to invest in Cybersecurity and secondly are the economic conditions right for releasing spend in Ireland on cyber related products?

From this viewpoint there is a strong belief from this group that the current economic conditions in Ireland do not support the deployment (at least at scale) of new entrant cyber roles. There is a perception that most new entrant level cyber roles are more economically delivered from eastern Europe or Asia (new entrant roles discussed were typically SOC L1 and junior pen testing roles).

Findings from the New Entrant Group

In July 2020 it@cork Skillnet launched a CyberTalent Employment Activation Programme (CEAP) for Women initiative. The programme comprised 11 women and was delivered over a six-month period. The participants fell into 3 categories:

- a. 3rd level graduates from IT related disciplines.
- b. 3rd level graduates from media and arts courses.
- c. Graduates with Master's in cyber and forensics studies.

The group used the Immersive Labs cyber training platform as a means of gaining practical hands on experience in Cybersecurity. Their feedback can be summarised as follows:

- There was very positive feedback about the cyber training platform as that was hugely beneficial in terms of their practical Cybersecurity skills. There was a general feeling that their college courses lacked this type of hands-on experience. This was crucial because experience was the number one requirement of employers even at the new entrant level.
- Although the individuals had identified with wanting a career in Cybersecurity, they were not fully aware of the range of jobs in Cybersecurity nor could they easily articulate their plan for finding a new entrant cyber role.

One of the key findings from the CEAP programme **Skills Connect** is that many graduates require more understanding of the roles within the cyber job family and require more prescriptive guidance as to how to prepare and train for particular roles. For example, some of the participants identified SOC L1 as a good starting point. However, until they had engaged with the Immersive Labs platform, they had no prior training in SIEM technologies or even in Active Directory.

There was very positive feedback about the cyber training platform

Overview of Options

Some of the quotes from participants have been grouped into the following tables. To illustrate the degree of differing views we have categorised the comments as generally 'positive' or 'negative'. In the table there are a wide-ranging and sometimes conflicting set of views on cyber skills and training in Ireland.

These are verbatim quotes from the interviews. Some perceptions and opinions can be common however there are also some striking views that are held by small minorities. The report writers identified a top 12 list of quotes that attempt to capture a very high-level summary. These are highlighted in blue in the table below.

Qualitative Feedback	Positive	Negative
The Job Market Demand	The opportunity in Cork should be big for cyber as it's perceived nationally as a cyber cluster.	There are only a small number of vacancies in Cork for junior roles in cyber SOC and none in pen testing.
	A reactive approach to Cybersecurity resources is no longer enough, we need to be better planned.	There is no high demand for cyber roles because there is no understanding of the risk at a management level.
	We need a balance of Irish and non-national and we need more women.	Maybe 200+ open job vacancies across Ireland right now but there are 1,000s in software engineering. The market is not big for cyber.
	We need to be careful not to force the job market.	Heavy emphasis on automation as companies can't afford Level 1 humans.
	We have to move beyond just looking at the graduate market.	The issue with selection is the qualifications first mentality. That is a deep-rooted mind set, which means they are looking at the wrong people.
	The labour market including Cybersecurity will change a lot over the next 12-18 months.	Cyber is not the biggest employment market in Cork right now.
		Internships are a fantastic idea, but companies are not motivated or well equipped.
		Catch 22 - because every hiring manager wants many years of previous experience.
		There is a big issue in making security attractive to IT and engineering people.
		Very hard to gain employee loyalty in this current market.
		My university course was good, but it has not given me hands on experience and that's what companies #1 requirement is.
		Capacity is very low and 8 out of every 10 candidates are non-Irish.
	It's a hiring behaviour issue not a skills or resource shortage.	

Qualitative Feedback	Positive	Negative
Awareness of it@cork Skillnet	The Skillnet model is totally fit for purpose and is agile, which is what is needed.	Awareness levels on Skillnet is low and perception is unclear.
	You are the first support organisation to ever contact me about my Cybersecurity training needs (and we are a key vendor in this region).	Not aware of skillnet programmes.
Quality of Cybersecurity Training	Placements are the key to unlocking growth in cyber skills.	The only way that cyber is going to improve in Ireland is when there is more funding for university-based research.
	Multinationals have bought into the Apprenticeship model and are willing to take them on board.	The biggest gap right now is that people are unwilling to spend money on cyber training.
	The training foundation has to be about setting standards, but this needs to be at a very sophisticated level.	People focus on the new entrant and unfilled jobs - the biggest issue is that the existing staff are not great quality when tested against capture the flag events (especially in SOCs).
	The only strategy is to train on the job but also to have this as team-based training not individuals supported by a mentorship programme.	The core issue is that companies don't have the training resources to undertake cyber skills programmes.
	Cyber people use a different language and terms to other IT functions, and we need to get better at communicating about Cybersecurity to the rest of the business.	We are not equipped to teach them the role, they need to come in job ready.
	More intensive and structured work experience needs to be part of the 3rd level courses.	I don't think companies have proper training on cyber awareness that is specific to remote working.
		The big issue with the cyber training platforms is that they don't give enough hands-on experience.
	Cyber is way too complicated and we need to find better ways of training and explaining.	
Organisational Design for Cyber Teams	We need to benchmark ourselves against the US and their maturity in cyber.	There is a fairly fundamental level of naivety in most companies and it is scary because of the sophisticated levels of threat.
	Our SOC is currently in India but as an industry we need more of this capability in the EU and ideally in Ireland.	Companies don't know what they are doing when it comes to cyber and confuse cyber skills into other IT roles.
		We don't have the hiring or training capability in-house.
		Cyber should be important but companies have too many products and too little time.
Career Paths and Development	Cyber is not a standalone job family. It is embedded in all technology roles and this is the core issue.	CISO's and SOC Managers are not fussed by certification.
	At the C-level there is no-where to obviously progress at the upper level.	Wage inflation and staff tenure are huge problems.
	The outlook is positive, not seeing any layoffs in cyber teams or pay cuts for people working in cyber.	

Qualitative Feedback	Positive	Negative
Future Training Needs	The big money shot is Microsoft Azure and Azure DevOps that is where the greatest skill shortage is.	Big lack of OT Knowledge.
	There is however a gap in the region for the more advanced and specialist courses. These would include the likes of ISACA and ISC2 courses, OSCP, CISSP, CRISC, CISA, CISM and also the courses offered by SANS. Bringing those calibre of courses to the region (even annually) would certainly provide higher paying roles and allow horizontal movement from accounting, management roles in other industry verticals etc.. That in turn would be a more attractive target to large incoming companies and the cycle would continue.	The current SOC doesn't work because the decision making of staff is not correct and they are not agile enough.
		There are too many cyber products and too little time to train.
		The issue is that the business doesn't always understand the risk.
	Our next battleground is IOT.	
	OT/Scada is wide open and a huge gap that does not have enough focus.	
	5G and other technologies will force a total rethinking of the Cybersecurity ecosystem.	
	Machine learning and automation is the primary strategy for the skills shortage.	
Impact of Covid	Not seeing the overall volume of incidents growing due to Covid, just a shifting in emphasis.	Now is the time to detonate ransomware attacks and the majority of companies are nowhere near prepared for this.
	Hiring for cyber roles is increasing and has not reduced as a result of Covid.	Some clear marketing scaremongering by vendors probably mis-using the statistics.

Qualitative Feedback	Positive	Negative
Level of Capability Maturity		<p>20 years later we are still talking about effective password procedures.</p> <p>Organisations simply don't understand the level of risk and the value of protecting against that risk.</p> <p>The old approaches to Cybersecurity aren't working. In 2019, despite increasing Cybersecurity budgets 9% year-on-year, enterprises still saw a 26% increase in security incidents. Combined with an increasingly mobile workforce with a unique set of risks, this has created a brand new landscape that calls for a completely new strategy.</p> <p>The Cyber Industry needs a wake-up call and although there are many initiatives, they are not falling under a cohesive joined-up overarching strategy.</p> <p>The people trying to fix the cyber problem are not doing it against any standard and without a standard it's likely to be wasted effort with no long-term value.</p> <p>Not enough awareness of SOC 2 Type 2.</p> <p>Off-shoring is a potentially big issue, it's like sending our national school kids to another country for basic education.</p> <p>Cyber starts with basic pen testing and we don't do enough of that - nobody knows what a pen test is. There is no easy answer.</p>
Growth Opportunities	<p>There is a huge opportunity to build on the cyber cluster that already exists in Cork.</p> <p>Big question for the IDA - in the current climate how do they keep jobs here as well as how do they grow the sector.</p> <p>What's the economic value to Ireland Inc of SOC L1? We need to look at this question again and maybe we need a different type of investment incentive.</p> <p>We need more global players (and new ones) to help create the conveyor belt for Cybersecurity career paths.</p>	<p>There is a strategic drive of pulling resources and functions back into the US.</p> <p>Many of the new entry jobs like SOC and Pen Testing are simply not economic to deliver in Ireland.</p> <p>There are significant gaps in support at all levels, not just at new entrant levels. The driver is the lack of leadership understanding and the expectation that cyber has an ROI. It's a cost of doing business. Don't waste precious time.</p> <p>The scale of the Irish market is just too small.</p> <p>One of the big drivers for whether cyber skills is a growth area is whether companies in Ireland follow an in-house or an outsourced model.</p> <p>Very little Foreign Direct Investment (FDI) activity from cyber companies in recent times in our region.</p>

The outputs of these interviews have been used as one input into the design of the TNA questionnaire and helped shape some of the priorities. An online survey has length restrictions, so some judgements were applied to create the final set of questions. The design approach and prioritisation of questions is described in the TNA Design section.

Conclusions from the Interviews

The following table summarises the key findings of the interviews (all groups) by theme.

Question Groups	High Level Observations
1. Cyber Strategy	In general, Cybersecurity is important to business performance and may even be growing in criticality, but there are challenges in securing budget, executive management support, resourcing, and delivery of effective training.
2. Cyber Risk Evaluation	<p>Cyber Risk is not well understood by managers outside the cyber function and there are a majority who hold the view that organisations are being very naïve about the risks from Cybersecurity attacks.</p> <p>There is a strong perception that COVID-19 is having a game changing impact on Cybersecurity and this is partly fuelled by a belief that digital transformation is being accelerated because of the pandemic.</p>
3. Awareness Levels	It appears from the interviewees that awareness levels at both a senior management level and among the wider employee group is low.
4. Basic and Advanced Skills Training	<p>There is not a common view of the quality of training and it appears that cyber training may be at a low level of maturity.</p> <p>There were only few examples of where companies have in-house cyber training specialists and also only a very small number of examples where companies are using cyber specific training platforms. It appears that most training is either vendor-led or on-the-job.</p>
5. Emerging and Future Skills	<p>People found it hard to scope and size future skills needs. It is possible that companies are still struggling with capacity and resource planning to start so have not done much work on future skills. However, areas that were commonly quoted for future skills were:</p> <ul style="list-style-type: none"> - OT/ICS/SCADA. - IOT. - Cloud and Infrastructure. - DevSecOps. - Containerised development. - Device and domain-based security. - Identity and access. - Data loss prevention.
6. Management of Cybersecurity resources	<p>Different groups have different perceptions:</p> <p>The Talent Group are pre-occupied with the challenges of job/organisational design and talent acquisition. This often focuses on issues concerning whether the organisation has a mature understanding of operating models for cyber. There is a perception that the job specification outlined by companies (e.g., qualifications and experience) is simply not available in the market. The talent group also find that hiring managers are sometimes unwilling to look at creative or new approaches to resource planning.</p> <p>As a comparison, the Vendor Group tend to focus on budget availability and the economics of cyber delivery in Ireland. A common view is that entry level roles like SOC L1 and junior pen testing are not economically viable for Ireland Inc.</p> <p>The CISO Group have a pre-occupation at times with managing the expectations of the senior management team.</p> <p>Amongst all the groups, very few people believe that they have a robust way of measuring Cybersecurity capability maturity. Most people also believe that employment growth in Cybersecurity is and will continue to grow based on global trends and most people believe that there is a resource and skills shortage when it comes to cyber talent.</p>

The background is a chalkboard filled with various hand-drawn mathematical diagrams and formulas. At the top left, there's a bar chart with four bars of varying heights. To its right is a flowchart with a box containing the number '2' and arrows pointing down and right. Further right is a network diagram with nodes and connecting lines. Below these are several mathematical expressions: $\frac{75+12}{81} = 51\%$, $\frac{79\% - 12\%}{00,12}$, $\frac{1621500 + 47300}{1668800}$, $\frac{(11^2 + 82)}{77}$, and $\frac{58^2}{17^2}$. There are also pie charts, one with a 31% slice highlighted, and another with a 2% slice. A hand holding a pen is visible on the right side, appearing to be in the process of drawing or writing on the board. The overall theme is quantitative research and data analysis.

SECTION SEVEN

Quantitative Research

Quantitative Research

(Training Needs Survey)

The context of the Future Skills Programme and its Training Needs survey is that the it@cork Skillnet is seeking to gather data and information on the future skill requirements for Cybersecurity within its membership base and beyond.

Feedback from ongoing telephone interviews with subject matter experts was also fed into the survey design

This information is needed to inform future training programmes. It specifically targeted those people who have responsibility for Cybersecurity within their organisation.

It was anticipated that only some respondents will have conducted an internal Training Needs Analysis (TNA) to be able to clearly define their training needs. As such, the design must also facilitate those who have not completed a TNA and will provide likely topic areas of training for them to consider.

Additionally, the survey was designed to include emerging strategic issues within Cybersecurity so that the respondent may consider and evaluate whether these may be applicable to their organisation and then consider whether they will need to invest in training in these areas also. Given the lack of data available on the size of the Cybersecurity sector in Ireland, we included questions to gather information about the Cybersecurity employee resources within their organisations and whether they expect these to grow or not.

Research

Research was conducted as part of the design process with the starting point to look at recent comparable surveys (Cyber Ireland and the UK's DDMSC/Ipsos Mori surveys) as well as strategic issues and training trends from various industry reports. Some questions were adopted or adapted from these. Feedback from ongoing telephone interviews with subject matter experts was also encapsulated and fed into the survey design. The survey design was a very iterative process with new priorities emerging as the other research phases progressed. Appendix 5 explains the design process.

Considerations

There were several important factors that needed to be considered in the design process.

- Respondent – these are likely to come from a broad range of organisations with some having in-depth Cybersecurity resources and others having very few. Similarly, Cybersecurity maturity is likely to vary significantly.
- Population – while the survey is originally intended for Skillnet members, it was also issued much further to capture training and strategic issues and trends nationally.
- Length – the survey seeks to go beyond training requirements which significantly increases survey length and requires a careful balance in design to avoid survey fatigue. Not all the proposed questions could be included.
- Complexity – the survey needed to be as simple as possible to ensure reliable and informative responses and manage the overall cognitive load/fatigue.

The following section summarises the key findings from the survey. The full survey responses can be found in Appendix 6.

About Respondents

Conclusions

The profile of the respondents is informative, and the quality of responses was high (e.g., very few questions were skipped). Six respondents were Cybersecurity Vendors.

Findings

- We received 35 responses to the survey.
- The question completion rate was very high, indicating the length and complexity was correctly pitched.
- 23 of the respondents worked in Cybersecurity strategy and operations roles, 3 in Cybersecurity training role, the remaining in other cyber related roles.
- 15 respondents were at the C-suite level.
- 18 respondent's organisations were foreign owner and 17 indigenous Irish.
- The majority (74%) of respondents were from large organisations.
- 12 were in the ICT sector with the remainder spread across 9 others.
- 26 were from large organisations (250 plus employees).
- 10 were members of the Skillnet.

Training Practices

In this section we asked a small set of questions concerning training delivery preference, certification, and interest in future training initiatives.

Findings

- Certification remains important to a large majority of respondents (77%).
- Over two thirds of respondents expressed an interest in some form of cyber training initiative with the graduate placements the most popular.
- Most provided employees one to two days training per annum.
- Most had cyber awareness training programmes in place for their leaders and employees.
- Only half used competency/skill frameworks to identify training needs.

Conclusions

A positive finding is that many respondents had programmes in place for leaders and employees, but the data indicates that there may be an under-investment in training for resources working in cyber teams. This means there is a focus on security awareness but maybe not sufficient focus on cyber training for cyber professionals.

There also seems to be scope to utilise skill frameworks more to help organisations identify training needs, although any framework used would have to be regularly maintained to keep pace with the changes in the sector.

Training Requirements

In this section of the survey, we provided respondents with a detailed set of potential training needs (both technical and transversal) for the Cybersecurity teams and asked them to select which one was a priority need for them.

Findings

- The top foundation training need was in ‘Security standards’ with 16 positive responses.
- The top advance training need was in ‘Cloud cyber/native security’ with 23 positive responses.
- There was demand but uncertainty of the level training required for OT/ICT/SCADA, indicative of an area of growing concern and focus for many companies.
- 34 respondents provided answers to this question with ‘Communication skills’ the largest need followed closely by ‘Incident Response Planning & Simulations’
- 27 of respondents felt certification was important part of cyber training for their organisation.
- 17 were positive towards supporting graduate placements.

Technical Training Needs Ranked

We have collated and ranked the number of positive responses to the training topics below for both advanced and foundation training.

Technical Training Needs Ranked

We have collated and ranked the number of positive responses to the training topics below for both advanced and foundation training.

ADVANCED	COUNT	FOUNDATION	COUNT
Cloud cyber/native security	23	Security standards e.g., ISO 27001, CIS Top 20, Mitre Att&ck, etc.	16
Network security	22	Mobile security	15
Security architecture	21	Domain specific security e.g., devices	14
Security Operations Centre (SOC)	20	DevSecOps including application security	14
User behaviour and activity monitoring	20	IoT security	13
Incident response	20	Security assessments (e.g., SOC 2- Type 2)	13
Data Loss Prevention	19	AI automation	12
Vulnerability management	19	Penetration testing	11
Threat intelligence	18	Risk governance	11
Risk governance	17	Digital forensics	11
Cyber playbooks	16	Threat intelligence	10
Penetration testing	15	Interpreting malicious code	10
Data Protection/PII/SPI	15	Data Protection/PII/SPI	10
Regulatory compliance	14	Data Loss Prevention	10
Security standards e.g., ISO 27001, CIS Top 20, Mitre Att&ck, etc.	13	Vulnerability management	10
Security assessments (e.g., SOC 2- Type 2)	13	OT/ICT/SCADA	9
Interpreting malicious code	12	Security architecture	9
Digital forensics	12	Regulatory compliance	9
Domain specific security e.g. devices	11	Cloud cyber/native security	9
DevSecOps including application security	11	Security Operations Centre (SOC)	8
Mobile security	10	Cyber playbooks	8
IoT security	10	Network security	7
AI automation	8	Incident response	7
OT/ICT/SCADA	7	User behaviour and activity monitoring	6

Transversal Training Needs

The top five transversal skills identified as a training need were:

1. Communication skills.
2. Incident Response Planning & Simulations.
3. Leadership.
4. Risk and Governance Management.
5. Project Management.

Conclusions

From the training topics we provided there was a high level of real demand for a high level of training need across all the cyber topics, indicating a strong demand for training. On average most respondents are indicating a demand for advanced technical training over foundation training (i.e. on average there were 13 positive responses per topic for advanced training compared with just 8 for foundation training). This suggests the need to seek out leading training practitioners capable of providing advanced, up to date training for future programmes.

In terms of transversal training, there may be an underlying need to have a structure in place to better manage risks and the potential inevitable incidents organisations are likely to face. Perhaps a programme that covers leadership, risk, governance, and response planning may be required. Transversal skills, for example, are a critical element of educating and influencing the Board of Management.

We also found that certification was rated as important for organisations, which is a key consideration for future programme development. There was some level of interest for different T&D initiatives, with 25 indicating interest on some of the options offered. This is encouraging and suggests that there may be some demand for these types of initiatives going forward.

Future Challenges

In this section we presented respondents with future Cybersecurity challenges gathered in our earlier research. Respondents were asked to rate these as critical, important or not important. They were then asked about new skills required to respond to these challenges.

Findings

- Perhaps not surprisingly 'Remote working security', 'Preparing for a major incident response' and 'Cloud native security' were the top 3 critical challenges facing Cybersecurity.
- 'IoT security' and 'Cybersecurity agile testing capacity' were the least important challenges facing Cybersecurity (selected from a list of 15 challenges).
- 18 respondents felt the challenges required new skills, with cloud security the prevalent skill area cited.

Conclusions

The top three challenges above reflect our research elsewhere. While 'Remote working security' presents perhaps the most current concern for cyber leaders, followed then by incident preparation.

The final top challenge presents what seems to be a rapidly growing concern related to the move to cloud and digitization; perhaps the biggest challenge. We see incident response preparation as a priority also under the transversal skills section.

Resourcing Intentions

In this section we asked a series of questions about the current Cybersecurity service structure and about future growth intentions.

Findings

- 7% of respondents managed their cyber security service in-house, 40% used a mix of in-house and outsourced services and 8% outsourced their cyber security services.
- Most (69%) do not plan to change how Cybersecurity services are delivered.
- 6 respondents who currently have a mix of in-house/outsourced services plan to bring services in-house.
- 22 (63%) of the respondents had selected more than one role to grow in the future.
- Incident Response Specialist was the top growth role among respondents. followed equally by Security Administrators, DevSecOps, and Threat Hunting & Intelligence.
- 23 (65%) of the respondents report that skills shortage is having an impact on the business.
- About half of respondents' cyber function would consists of only a few individuals or a small team, while the other half have full size cyber teams or functions.

Conclusions

Most of the respondent group had some or all Cybersecurity services in house with some of these planning to expand in-house cyber services. These respondents also identified roles that they were planning to grow confirming this intention. However, it would be useful to identify why they are planning to do this and what it may mean in terms of wider trends.

Here again we see the underlying issue of incident response, with this role the top role for future growth. We also see here the emerging role of DevSecOps (ranked 2nd jointly) which may be the start of a growth trend.

Cybersecurity Functional Maturity

In this section we have a two-part question asking respondents to rate fifteen different Cybersecurity functions in terms of their maturity and the importance to improve in this area.

RESULTS TABLE	IMPORTANCE	MATURITY	GAP
Employees Cyber Awareness	3.74	3.47	-0.27
Identity and Access Management	3.69	3.85	0.17
Data Protection	3.66	3.76	0.11
Network Protection	3.59	3.91	0.33
Operational Security (OT/ICT/SCADA)	3.50	3.28	-0.22
IT Infrastructure/Architecture	3.49	3.83	0.34
Incident Management	3.49	3.91	0.43
Risk Management/Business Continuity	3.40	3.77	0.37
Threat Intelligence	3.35	3.74	0.38
Cybersecurity Strategy and Governance	3.31	3.74	0.43
Compliance and Auditing	3.23	3.79	0.57
Software/Application Security (DevSecOps)	3.18	3.58	0.39
Penetration Testing	3.18	3.71	0.52
Digital Transformation	3.03	3.59	0.56
Digital Forensics	2.91	3.45	0.54
Average rating	3.69	3.38	0.31

Key Findings

- Employee Cyber Awareness was rated the most important area to improve while Digital Forensics the least important.
- Incident Management was rated the most mature function while Operational Security the least, however both these were identified as training needs.
- The most notable negative gaps between the improvement scores and corresponding maturity scores for the different functions were for Employee Cyber Awareness and Operational Security.

Conclusions

Based on the rating scale provided the respondents felt they needed to improve in all cyber functions, with greater differences found in terms of their importance. Respondents, on average, felt the two main gaps (the difference between maturity and improvement required) were Employee Self Awareness and Operational Security (this an emerging area of concern).

Interestingly, Digital Transformation is given a lower importance rating, typically an area of collaboration for Cybersecurity. Our research highlights concern about how Digital Transformation can open new avenues for cyber-attacks, so perhaps this importance is underestimated.

Other Survey Initiatives

Cyber Ireland launched a new survey in July 2020 and the initial results have now been shared. This research survey is important as it will add more insight

specifically from a cyber industry perspective. That combined with the survey as part of this project will help inform whether a more comprehensive approach is required to measure and monitor employment levels and skills requirements for Cybersecurity within Ireland.

At it@cork Skillnet there is a more focused emphasis on cyber skills for all industries and levels. It is clear, however, that all Government agencies (Skillnet Ireland, IDA, Enterprise Ireland, Solas etc.) will need to have a capacity to audit ICT/cyber skills on a regular and accurate basis. Also, they are seeking to build regional clusters within Ireland that will need the ability to drill down specifically into all the professional groups under the ICT industry heading (e.g., ICT statistics broken down by programmers and IT technicians is not sufficient).

CAPABILITY MATURITY SCALE GUIDE
Level 1 – Unprepared. Ad-hoc processes and insufficient systems/resources.
Level 2 – Reactive. Resources and processes defined on a project basis.
Level 3 – Defined. Resources, policies and processes defined and centrally managed.
Level 4 – Measured. Fully resourced. Performance measured, monitored and controlled. Automation of basic tasks.
Level 5 – Progressive. Culture of continuous improvement. Advanced automation of tasks and controls.
Not applicable.
Don't know.

IMPORTANCE RATING SCALE
Level 1 – Less important now, reducing resources here.
Level 2 – Satisfied with current state.
Level 3 – Important to improve.
Level 4 – Very important to improve.
Level 5 – Critical to improve.
Not applicable.
Don't know.

01 01010101010101001011010101001010
010101011010100101010101010101010
01010101010101010101010101010100
01011011010101010101010

02 01010101010101001011010101001010
010101011010100101010101010101010
01010101010101010101010101010100
0101101101010

03 01010101010101001011010101001010
010101011010100101010101010101010
01010101010101010101010101010100
010110110101010101010101010101010

04 01010101010101001011010101001010
010101011010100101010101010101010
01010101010101010101010101010100
010110110101001010

SECTION EIGHT

Final Conclusions

213213 533455
7657568
56756756
7867876889
78678789789
87798797
7867886976
78979878978

2564	5464	6445	8787	6464	9
54534	464646	4544646	644	5464	4
45465	4432113	4313	43131	43131	4

Final Conclusions

The Cybersecurity industry (including academics, practitioners, training providers, product vendors as well as Government agencies) has potentially reached a major junction and inflection point in the evolving maturity journey of the sector.

As the sector moves from an early adoption phase to potentially the start of a new growth phase, changes on how cyber training and management practices are designed and managed will need to continuously evolve. This is required to make this capability maturity happen thus enabling better definition and wider implementation and industrialisation of Cybersecurity best practices.

There is some confusion about the quantum of resource and skill gaps in cyber in Ireland due to a lack of primary research and statistics. A more scientific and rigorous approach to this is required to enable appropriate decision making.

There are many positive examples of well-focused investments and skills development programmes, but the sum of these individual parts may not be sufficient to enable the level of systemic, organisational, and training intervention changes required:

- Ongoing, regular and industry wide research is required to improve our ability to reliably predict and forecast skill and training dynamics.
- For the sector to mature there is a need for a more precise definition of best practice based on comprehensive benchmarking aligned to international standards and accepted maturity frameworks.
- Appropriate business planning frameworks around business case investment and cyber strategic priorities need to be widely adopted.

- There is a need in the short term to bridge the gap between the level of resources available compared with the level of skill available in the labour market. This has implications for job design, recruitment practices, career planning, as well as training and skill development interventions. In its simplest terms a scientifically grounded training programme that up and cross skills resources in an agile, deep learning and practical way is required to cater for the different needs of MNCs and SME's.
- The insights from other studies, for example, the UK and the US, point to the need to have a healthy new entrant cohort of people finding employment in Cybersecurity. This is supported by the findings of this research which clearly shows there are an exceedingly small number of opportunities for new entrants. The question remains, however, as to how to best enable a long-term training support strategy for new entrants given the current labour market dynamics and economics in Ireland. Currently the research shows that the focus of employers is on higher skilled cyber roles.

A group of diverse people, including a woman in a blue striped shirt, a woman in a green shirt, and a woman in a red turtleneck, are smiling and holding up lightbulbs in a meeting room. The background shows a whiteboard with sticky notes and a blue wall. The scene is lit with a warm, golden light, creating a positive and collaborative atmosphere.

SECTION NINE

Recommendations

Recommendations

The table below summarises for each of the key players in the Cybersecurity eco-system recommendations that have been analysed because of this research programme. The scale of opportunity is in direct proportion to the level of co-operation needed by the stakeholders to tackle some of the challenges and issues facing the sector.

STAKEHOLDER GROUPING	RECOMMENDATIONS
Skillnet Ireland	<ol style="list-style-type: none"> 1. Continue promotion and investment in cyber specific training programmes aligned to digital transformation and enabling enterprise. 2. Enhance greater co-operation and collaboration between relevant Skillnets to both align and join up the cyber offerings whilst also developing the body of training science that is specific to cyber.
it@Cork/it@cork Skillnet	<ol style="list-style-type: none"> 3. Continued promotion and showcasing of our region and Ireland as a global centre of excellence for Cybersecurity through proactive strategic support of our Government agencies. 4. Promotion and support of Cybersecurity awareness and education programmes for specific groups such as Executive Board Members and the SME sector. 5. Alignment with other it@Cork initiatives to support and improve gender balance and diversity in Cybersecurity. 6. Support Enterprises with Cybersecurity standards and frameworks that improve skill and capability maturity specific to the Irish context. 7. On-going commitment to the delivery of subsidised upskilling programmes for companies and unemployed groups specific to Cybersecurity. 8. Development of training success case studies to enable the showcasing of best practices and agile training delivery. 9. Creation of a specific learning and know-how sharing group dedicated to Training, Recruitment & People Managers with responsibility for Cybersecurity skills development. 10. Continuous development and education to support companies to undertake effective TNA for Cybersecurity specific roles.
3rd Level Institutions and Training providers	<ol style="list-style-type: none"> 11. Funding of academic and scientific research into the science of skills development training will need to be constantly re-evaluated. There is a significant body of research and industry know-how on Cybersecurity management science already available, but it needs further investment to meet the speed and nature of change facing this dynamic sector. 12. A constant and regular macro review and evaluation of the effectiveness of training science on Cybersecurity (e.g. just-in-time training, purposeful simulation, blended learning, integrated apprenticeships and next generation internships etc..).

STAKEHOLDER GROUPING	RECOMMENDATIONS - continued
General Industry participants	<p>13. The industry (potentially through industry bodies like Cyber Ireland) need to improve the attractiveness of the industry for new employees and continuously work to de-mystify the sector so that there is enhanced understanding of the sector.</p> <p>14. Industry needs to have greater collaboration with 3rd level institutions and a wider and deeper implementation of a new generation of internship and apprenticeship models that accelerates the job-readiness and availability of resources to meet the growing demand.</p>
Government	<p>15. EI and IDA play a central role in both attracting new employment growth as well as underpinning existing cyber employment. There is a need to widen and deepen the number of cyber companies across the country. There needs to be an evaluation of more targeted FDI as there is a need for more entry level employment and this requires certain types of companies to set up in Ireland.</p> <p>16. Specific supports will be required for the SME sector and new thinking will be required to enable better cyber capability within these companies.</p>

Future Challenges

There is a significant willingness on behalf of people to get involved with the further development of this industry sector. If you want to get involved, here is how you can do that:

How to get involved and stay connected

Contact: Annette Coburn

Email: skillnet@itcork.ie

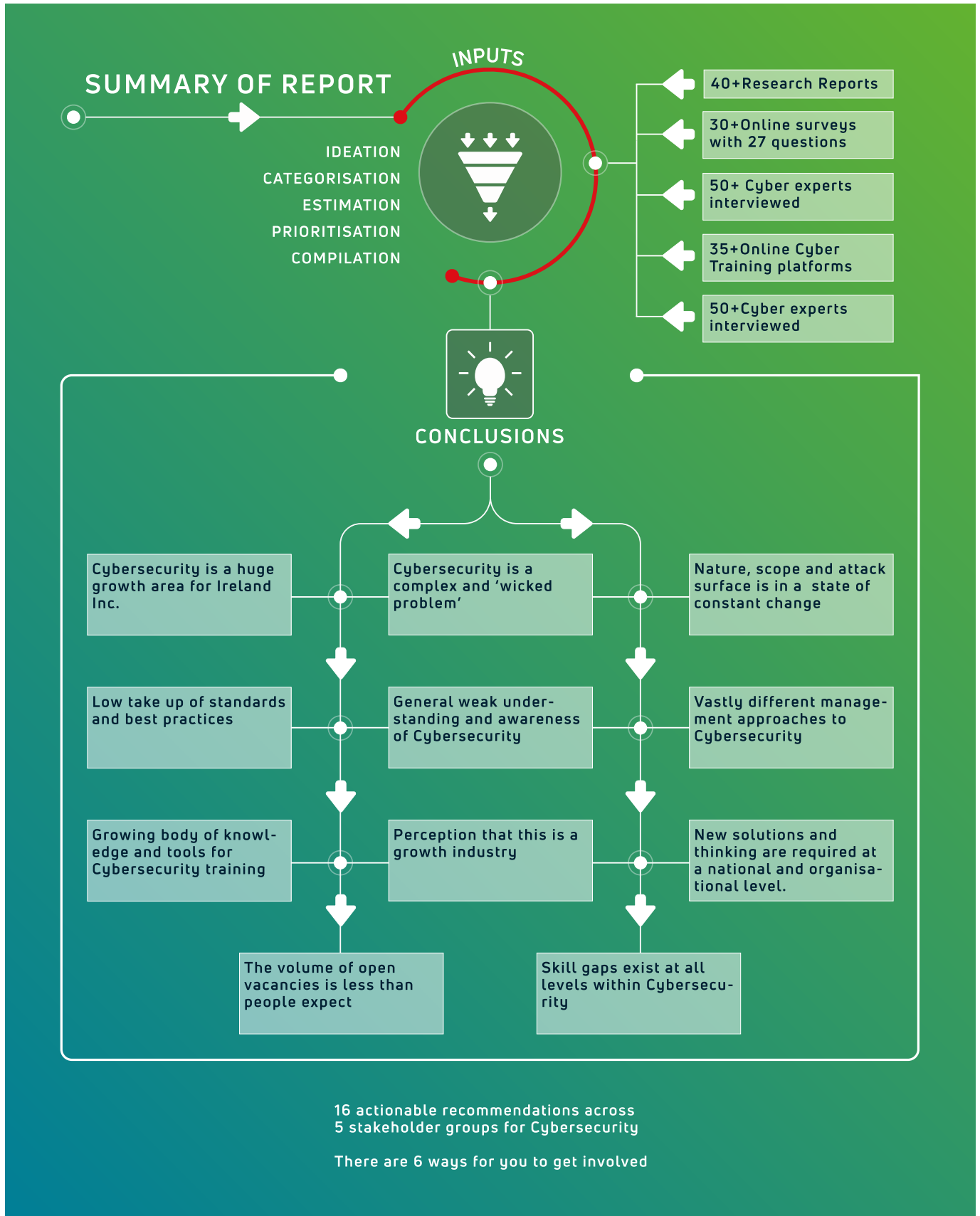
Call: +353 86 084 8704

Web: www.itcorkskillnet.ie

LinkedIn: <https://www.linkedin.com/company/it-cork-skillnet/>

CATEGORY	WHAT'S INVOLVED
Mentoring	There are a number of Cybersecurity training programmes and there is a significant demand for people who are available to mentor particularly new entrants into Cybersecurity.
Apprenticeships/Internships & Graduate Programmes	Companies who wish to run apprenticeships in their Cybersecurity teams should contact us for contact with potential candidates graduating from our programmes.
Employment Opportunities	Please make us aware of any open vacancies and these will be posted to our existing unemployed trainees.
Learning Communities	The plan is to create a community of training managers with specific responsibilities for Cybersecurity.
Event Speakers/Thought Leadership	Please contact us if you have thought leadership and know how on Cybersecurity.
MNC and SME Cybersecurity training programmes	If you have plans to train your in-house team on any aspect of Cybersecurity please contact us for how we can support.

Report Summary



Appendix 1 - UK Report Recommendations

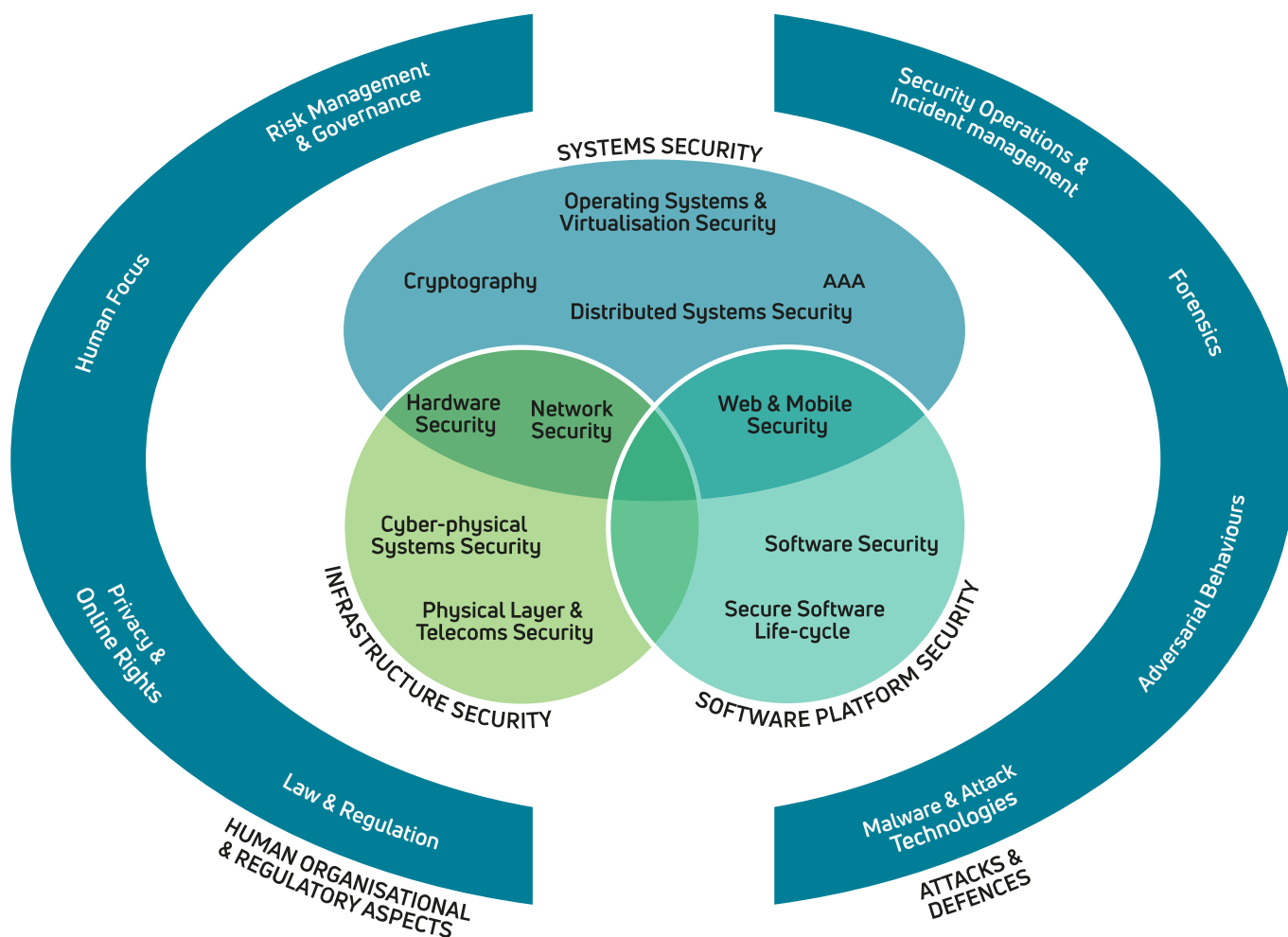
The following long list of recommendations in the UK Report are all based on the evidence generated from their study. It requires engagement from government, the cyber sector and other cyber employers, education institutions and recruitment agencies to take them forward.

RECOMMENDATIONS	
1	The entire programme of government activity on Cybersecurity skills should be joined up under a cohesive brand.
2	There should be further work to explore how schemes such as CyberFirst can be made more widely available to young people and attract as broad a pool as possible.
3	There should be further work with schools and universities to improve their understanding of the breadth of career opportunities in Cybersecurity, so they can promote these careers more.
4	Universities that offer courses in Cybersecurity should work with the cyber sector to ensure that these courses adapt to the evolving needs of the sector.
5	There should be case studies of cyber employers that have used on-the-job training and work shadowing effectively, to get new joiners, apprentices and those transitioning from non-cyber roles to be job ready.
6	There should be a consistent approach – one that can feasibly be scaled up for promoting and endorsing high-quality Cybersecurity training providers and courses to cyber employers and individuals.
7	There should be further guidance for recruitment agents, or partnerships between agents and cyber employers, to improve their understanding of the requirements for different cyber roles.
8	There should be more engagement with cyber employers to better understand the challenges they face when seeking apprentices in cyber roles and to encourage greater uptake. This could build on ongoing work to develop new apprenticeship standards for cyber roles.
9	There should be a review of the existing range of Cybersecurity training courses. This would assess the extent to which these courses provide employers and training recipients with the necessary technical, practical and soft skills to work in cyber roles.
10	There should be further promotion to raise awareness among wider (non-cyber) staff in SME's.
11	Cyber sector businesses should be encouraged to broaden their recruitment, to look beyond job applicants that have 3 to 5 years of experience. This includes apprenticeships and other work placements, starting graduate schemes or other opportunities for career starters, and recruiting from more diverse groups.
12	As part of the ongoing work to map Cybersecurity career pathways, there should be a focus on developing the pathways for those moving from non-cyber roles into cyber.
13	There should be further engagement with cyber employers based outside geographic hotspots to better understand the recruitment barriers and challenges they might face as a result of their locations.
14	There should be guidance and best practice examples provided to the heads of cyber teams on how to improve diversity in recruitment and how to make working environments more attractive for diverse groups.
15	Communications around diversity in Cybersecurity should be re-framed, to focus more on how a diverse workforce can address skills gaps. This could be through a communications campaign, sharing positive case studies.

Appendix 2 - Leading Training Provider Review Grid

Training Providers	Infosec	Plural-sight	Immersive Labs	Sans Institute	Cybrary	Cira-cadence	Secure Ninja	Range-Force	ISC2	EC Council
Focus	Cyberskills	Wider technology skills	Cyberskills	Cyberskills	Cyberskills	Cyberskills	Cyberskills	Cyber	Certification	Certification
Speciality	Online	Online	Labs	Premium training	Online	Gamification	Certificate training	Simulation training	Pool Certs + providers	Advanced qualification training
Based	US	US	UK/US	UK/US	No info.	US	US	US/Estonian	International	US
Number of cyber courses	683	137	700+	60+	335	No info.	US	200+	Hundreds	Hundreds
Bretts of cyber coverage	All Cyber roles	Cyber/Ops/Software	All Cyber roles	All Cyber roles	Cyber/IT/Data/Cloud/DevOps	Common SOC Cyber roles	All Cyber roles	SOC/DevOps/Engineer	All Cyber roles	All Cyber roles
Depth of topic coverage	Advanced	Foundation/inter.	Advanced	Advanced	Foundation/inter.	Foundation	Advanced	Advanced	Advanced	Advanced
Cost per annum	\$299	€400 individual \$800 enterprise	€600	-	\$400	\$900			Professional membership	\$250
Cost per course				EG \$7,000			\$500 per day		€80-€880	\$600-\$4,000
Learning methodologies										
Skill assessment	Adaptive	Adaptive								
E-learning modules										
In-person workshops										
In-house workshops									Cyberbix (local)	
Live streaming workshops										
Personalised (AI) content										
Online labs			Speciality							
End of module assessments					No info.			No info.		
Real cyber tools					No info.		No info.			
Boot camps					Community					No info.
Online facilitation support								Virtual	Online course	
Projects/assignments	No info.		Labs				No info.			
Books									App. versions	
Video modules		Mostly video	Very limited							
Real life simulations	No info.				Capture flag			Battle force		No info.
And of course evaluation					No info.			No info.		
User communities			No info.	No info.						
Intelligence/updates		No info.	Dedicated team	Research instit.			Conferences		No info.	No info.
Awareness/Comp. training		Not speciality	Not speciality		1 course					
Career/role/skills path's	70	Ltd. for cyber	NIST based		Limited	Limited				
Customising path's functionality										
Manager updating		No info.	No info.							
Dashboard										
Analytics										
Gamification	Basic	None	Advanced	Netwars	Tracking	Advanced				
Certification prep courses				GIAC						
Framework mapping	NIST	NIST	Mitre/NIST/Crest	NIST	NIST	NIST		NIST/Mitre/OSWASP	CBK	NIST
Multiple languages		English only	English only	English only	English only	English only				
Duration of courses										
Short courses (hours)										
Medium (e.g. boot camps)										
Long (e.g. qualifications)				Degree level						
Resource management tool		Flow								

Appendix 3 - Cybok Cybersecurity Body of Knowledge Overview



Appendix 4a - Job Postings (on LinkedIn for Cybersecurity)

We searched online for 'Cybersecurity' jobs on LinkedIn covering those posted in the 'past month' (September) for Ireland. There were 348 job post results with many easily identifiable as outside the Cybersecurity domain. A review brought the number down to 173 posts and with some basic recoding and consolidation we found 59 distinct job titles. (Note, we were unable to identify and remove duplicate job postings by different recruiters

at this point but estimate 30% are duplicates). We also found Information Security roles incorporating Cybersecurity responsibilities so have left these in the table. The top three roles include Cybersecurity Engineer, Cybersecurity Consultant and then Cybersecurity Analyst. This exercise showed the broad range of Cybersecurity jobs posted nationally during September.

ADVANCED			
Cybersecurity Engineer	19	Chief Technical Officer - Cybersecurity	1
Cybersecurity Consultant	18	CISO	1
Cybersecurity Analyst	12	Compliance/Audit Specialist	1
Information Security Analyst	10	Cyber Incident Response Specialist	1
Cybersecurity Manager	8	Cyber Risk Adviser	1
Security Architect	8	Cybersecurity Project Manager	1
Application Support Engineer	5	Cybersecurity Senior Analyst	1
Security Engineer	5	Data Privacy and Risk Consultant	1
Business Analyst (Cybersecurity)	4	Data Privacy Manager	1
Cybersecurity - Assistant Manager	4	Director of Cybersecurity	1
Cybersecurity Director	4	Information & Cybersecurity Specialist	1
Privileged Access Administrator	4	Information Security Consultant	1
Security Product Manager	4	Infrastructure Engineer	1
Application Security Engineer	3	IT Security Systems Engineer	1
OT Cybersecurity Specialist	3	IT Systems Security Auditor	1
Security Admin	3	Lead Security Design	1
Security Analyst	3	Lead Systems Engineer	1
Security Policy Analyst	3	Network Security Engineer	1
Threat Investigator	3	Security Development Architect	1
Business Systems Specialist	2	Security Incident Response Engineer	1
Domain Architect, OT Security Lead	2	Security Information Specialists	1
Graduate Security Operations Analyst	2	Security Metrics Lead	1
Information Security Delivery Manager	2	Security Operations Engineer	1
Product Security Technical Project Manager	2	Security Service Delivery Manager	1
Security and IT Compliance Assessor	2	Senior Penetration Tester	1
Security Researcher	2	SOC Manager	1
Senior Cloud Security Engineer	2	Threat Analysis Engineer	1
SOC Analyst	2	Threat Analyst L2	1
Threat Analyst	2	Trainee IT Security Engineer	1
Chief Information and Technology Officer	1		

Appendix 4b - Hiring Companies (for Cybersecurity Job Postings)

During September 2020 we found a total of 105 employers (excluding recruitment agency job posting).

LINKEDIN JOB POSTINGS HIRING COMPANIES – CYBERSECURITY (SEPTEMBER 2020)					
1	AbbVie	Pharma	54	McAfee	Cyber
2	Accenture	Consulting	55	Medtronic	Med Dev
3	ACI Payment Systems	Finance	56	Microsoft	ICT
4	ACI Worldwide	Finance	57	MILESTONE SOLUTIONS	ICT
5	Adaptive Mobile Security	ICT	58	MultiPlooy Limited	ICT
6	AIG	Insurance	59	N3	Sales
7	Amazon	Retail	60	Norton LifeLock	Cyber
8	Amazon Web Services (AWS)	ICT	61	Nova Leah Ltd	Cyber
9	Analog Devices	Medical Devices	62	Novartis	Pharma
10	Arkphire	ICT	63	One Identity	Cyber
11	Avanade	ICT	64	Oomnitza	ICT
12	AxiomSL	ICT	65	Oracle Corporation	ICT
13	BAE Systems	Defence	66	Palo Alto Networks	ICT
14	BlackBerry	Cyber	67	PartnerRe	Insurance
15	Brightwater	Cyber	68	Perrigo	Pharma
16	Canonical	ICT	69	Quest Software	ICT
17	Carraig Donn	Retail	70	Rapid7	Cyber
18	Click Dimensions	ICT	71	Red Hat	ICT
19	Cloudbeds	ICT	72	Regeneron	Pharma
20	CONTINENT 8 TECHNOLOGIES	ICT	73	Ryanair	Ryanair
21	Covalen	Utilities	74	Salesforce	ICT
22	CrowdStrike	Cyber	75	Security Risk Advisors	Cyber
23	Dell	ICT	76	Shutterstock	Media
24	Department of CCAE	Public	77	SKOUT CYBERSECURITY	Cyber
25	Eaton	ICT	78	Skyhigh Networks	Cyber
26	Ergo	ICT	79	Smartedges solution	ICT
27	eSentire	Cyber	80	Smarttech247	Cyber
28	Eurofins	Pharma	81	Solas Consulting Group	Consulting
29	Eurofins Ireland Clinical Diagnostics	Medical Devices	82	Sophos	ICT
30	Facebook	ICT	83	StorageCraft Technology	ICT
31	FBD Insurance	Insurance	84	SurveyMonkey	ICT
32	Fidelity Investments	Finance	85	Synchronoss Technologies	ICT
33	FireEye, Inc.	Cyber	86	Tenable	Cyber
34	First Data	Finance	87	TU Dublin	Education
35	Fiserv	ICT	88	Titan HQ	Cyber

LINKEDIN JOB POSTINGS HIRING COMPANIES – CYBERSECURITY (SEPTEMBER 2020) - continued

36	Forcepoint	Cyber	89	TQS Integration Ltd.	IT
37	Genesys	ICT	90	Trilateral Research	Legal
38	Global Shares	FinTech	91	Twilio Inc.	ICT
39	Google	ICT	92	Ulster Bank	Finance
40	Grant Thornton	Consulting	93	UnitedHealth Group	Insurance
41	HCL Technologies	ICT	94	Unity Technology Solutions	ICT
42	Hewlett Packard Enterprise	ICT	95	University College Cork	Education
43	Huawei Ireland Research Center	ICT	96	Vectra AI	ICT
44	IBM	ICT	97	VMware	ICT
45	Ignite Mental Health	Charity	98	Vodafone	ICT
46	Intuity Technologies	ICT	99	Western Union	Finance
47	J.P. Morgan	Finance	100	White Hat Security	Cyber
48	Johnson Controls	Facilities	101	WILLIAM FRY	Legal
49	Keeper Security	Cyber	102	Workday	ICT
50	KPMG Ireland	Man Con	103	Wu Xi Biologics	ICT
51	LRC Group	Finance	104	Zenith Technologies	ICT
52	Mastercard	Finance	105	Zscaler	ICT
53	Maynooth University	Education			



Appendix 5 - Survey Design Process and Rationale

Survey Question Order

Overall, there are 27 questions currently, some are straightforward multiple response questions which are cognitively easier to answer. Others are more complicated and time consuming, so some degree of survey fatigue can be expected. In anticipation of this we have prioritised the training needs first and then the resourcing and maturity questions second.

Input

- In terms of best practice survey design two experts were consulted for their input (Rob Browton of Feedback Works and Dr. James Cuffe of UCC).
- In terms of the technical content the survey was reviewed by subject matter experts in McKesson and Smarttech 247.

As a result of the feedback from the above collaborators a number of questions are amended and, in a few cases, dropped.

Link to the TNA Process

The survey will provide a vital input into the design of future skills programme for it@cork Skillnet. There will be specific data on the training topics required by respondents and also the strategic Cybersecurity priorities for the organisations. This data, once analysed, will enable the Skillnet to prioritise its training offering in terms of topics in most demand and can be reviewed in terms of those currently offered in the Cork region. The Skillnet will be able to go out directly to respondents with a proposed programme offering based on the survey to capture specific demand and initiate the commissioning stage with training providers.

Question Rationale

This section sets out the rationale for each section of the survey as well as the questions.

Part 1 – Respondent Profile

This section contains eight questions to gather the business demographic data of respondents to provide information about responding organisations. This will allow for a breakdown of the data by sector, organisation size etc.. The questions are listed below and are mostly standard and self-explanatory in nature, however a note is provided if required.

Q11. Respondents' responsibility for Cybersecurity – given the diffused nature of Cybersecurity within organisations we decided, rather than ask respondents for their roles (requiring a long list of response options), to use a simpler option of asking about responsibility for Cybersecurity (resourcing, training & strategy).

Q2. Level of respondent (i.e., C suite) – a simple measure of seniority which may provide an indication of importance for Cybersecurity.

Q3. Industry.

Q4. Size of organisation.

Q5. Origins of organisation.

Q6. Member of it@cork.

Q7. Name if member (required).

Q8. Name if not member (optional).

Part 2 – Current Training Practices

This section seeks to identify whether respondents are conducting the basics in terms of training and development practices as well as in the provision of employee Cybersecurity training generally.

Q9. Conducts a structured TNA – this will provide a picture of how 'evidence based' the responses are overall.

Q10. Provision of Awareness Training – to determine whether they provide basic cyber training to employees.

Q11. Formal training programme for Cybersecurity employees – a check on whether any planning and training investment is done currently.

Q12. Training days per annum – a measure of how much investment is made in Cybersecurity training (however this may be a hard question for respondents to be accurate about).

Q13. Using a skill framework – to provide an indication as to how mature they are in managing employee development i.e., ad-hoc versus structured.

Part 3 – Training Requirements

A core section that seeks to establish training needs and other supports for training.

Q14. Technical training needs – to capture training requirements in a broad and complex field using a developed list of likely training topics (expands on a similar question in the CSI survey) with foundation and advanced response options.

Q15. Transversal training needs – a simplified version of Q14 with respondents only ticking those skills that apply.

Q16. Delivery of training – seeks to gather information as to training delivery preferences to help inform future programme design (a difficult question but may provide valuable information such as a strong preference for online training or classroom).

Q17. Importance of Certification – seeks to determine whether futures programmes should be tied to some certification process (or not).

Q18. Interest in T&D Initiatives – given the lack of entry level roles noted in other research, this question seeks to determine interest in initiatives aimed at tackling this.

Q19. Financial support for T&D initiatives – building on Q18, seeks to measure funding capacity to support T&D initiatives to inform possible funding arrangements for future Skillnet initiatives.

Part 4 – Future Challenges

A short section to prompt consideration of future Cybersecurity challenges and what this may mean for future skills.

Q20. Strategic issues/challenges – this matrix question prompts respondents to consider which strategic issue is critical/important/not important for their organisation. Subsequent analysis will help the Skillnet to also explore and prioritise programmes based on this.

Q21. New or Emerging Skills – linked to Q20 this open comment box allows respondents freedom to articulate their thoughts on these issues potentially capturing new skills requirement not yet identified in survey.

Part 5 – Cybersecurity Resources

This section seeks to identify whether their Cybersecurity resources are growing, shrinking or changing in some way.

Q22. Cybersecurity Delivery – seeks to capture data on the degree respondents in-house or outsource Cybersecurity services.

Q23. Changes to above – following Q22 it captures potential changes / trends to this position.

Q24. Cybersecurity Resources – aims to capture the total number of Cybersecurity employees.

Q25. Resourcing Planning – this matrix question seeks to gather the type and number of roles in Cybersecurity in the organisation and which are likely to be static, grow or shrink in the coming years. This will help inform any role specific programmes required.

Q26. Shortage in resources – this question seeks to discover whether this heavily reported issue is a reality for respondents.

Part 6 – Cybersecurity Maturity

Q27. Function Maturity and Area for Development - this matrix question sets out the core Cybersecurity capability areas and asks respondents to consider their maturity in each and whether any of these require improvement. Uses simplified maturity scales to fit with a survey format. Provides an alternative way to capture training needs as well as offering the potential for a gap analysis exercise.

Questions Removed in the Design Process

Feedback from some reviewers felt that the survey (earlier versions) was too long, which is a concern shared by the project team. Survey questions were reviewed in terms of importance to the main goals of the survey and whether the other research streams would also be able to provide useful information on those questions under review.

1. Do you think Cybersecurity is a standalone career path?
 - *While an important issue, it is a very debatable question given the relative lack of maturity, also many SME may not see it as a career path purely due to scale.*
2. Which certifications do you feel are important for members of Cybersecurity team/potential employees to have? (tick those most appropriate).
 - *A form of this question is found in the Cybersecurity Ireland survey. Also, reviewers felt this question was very long and would 'slow' the respondents.*
3. Does your organisation have in place a Cybersecurity strategy and risk governance process?
 - *We cover this in Survey Q27 Maturity, albeit in a different format.*
4. To what extent has Cybersecurity been integrated into your organisation's IT strategy and planning process?
 - *We suggest this can/is be best covered through the other research streams.*
5. Similarly, to what extent has Cybersecurity been integrated into your organisation's strategy and planning process?
 - *We suggest this can/is be best covered through the other research streams.*
6. How confident are you that the general Irish economy can deal with these issues and challenges?
 - *A macro-economic type question better suited to the other research streams.*

Appendix 6 - Detailed Survey Findings

Part 1 – Respondent Profile

Q1. What responsibilities do you have within your organisation’s Cybersecurity function? (select most appropriate).

Cybersecurity strategy and operations.	23
Cybersecurity training.	3
Other cyber responsibility (please specify):	9

Q2. Is your role at the C suite leadership Level?

Yes.	15
No.	20

Q3. What industry is your organisation in?

The breakdown of responses by sector are as follows:

Information and Communication Technology/Telecommunications.	12
Cybersecurity Vendor.	6
Financial/Insurance Services.	6
Heavy Engineering/Manufacturing.	3
Pharmaceutical.	2
Retail/Wholesale.	2
Food and Drink.	1
Cybersecurity Partner.	1
Professional Services.	1
Agriculture.	1

Q4. What is the size of your organisation?

Large (250 plus employees).	26
Medium (50 to 249 employees).	5
Micro (1 to 10 employees).	3
Small (11 to 49 employees).	1

Q5. What are the origins of your organisations?

Foreign owned.	18
Indigenous Irish.	17
Yes.	10
No.	25

Part 2 - Current Training Practices

We would like to understand more about your approach to providing Cybersecurity training to your employees.

Q7. Have you conducted a structured training needs analysis (TNA) for your Cybersecurity function in the past year?

- 20 (57%) state they have conducted a formal cyber training needs analysis in the past year.

Q8. Have you a formal training programme in place for your Cybersecurity employees?

- 24 (69%) state they have a formal training plan in place for the cyber teams.

Q9. Do you have a formal Cyber Awareness training programme for:
- The Leadership Team?

- 28 (80%) state they have a cyber training programme in place for their leadership team.

Q9. Do you have a formal Cyber Awareness training programme for:
- Employees?

- 29 (83%) state they have a cyber training programme for employees.

Q10. How many days formal training per annum per person would your Cybersecurity employees have on average (for both classroom and blended training)?

No response.	1
Don't know.	3
None.	4
One to two days.	11
Three to four days.	4
Five to six days.	3
Seven plus days.	9

Q11. Do you use a competency/skill framework to help identify the training needs for your Cybersecurity employees?

- 17 (49%) respondents use competency/skill frameworks to identify training needs.

Part 3 – Training Requirements

We would like to understand your likely Cybersecurity training requirements for the next 1 to 3 years.

Q12a. What Cybersecurity skill areas do you plan to train employees in over the next 1 to 3 years? (select the options that apply).

TYPE	ADVANCED TRAINING	FOUNDATION TRAINING	BOTH	NOT SURE OF THE LEVEL REQUIRED	COUNT
Penetration testing	13	9	2	6	31
Security Operations Centre (SOC)	18	6	2	5	26
Security architecture	19	7	2	4	27
Threat intelligence	16	8	2	5	27
Interpreting malicious code	10	8	2	6	29
User behaviour and activity monitoring	18	4	2	5	29
DevSecOps including application security	8	11	3	7	25
AI automation	6	10	2	7	30
Risk governance	15	9	2	5	31
Regulatory compliance	12	7	2	6	31
Network security	20	5	2	3	26
Cloud cyber/native security	19	5	4	3	28
Mobile security	8	13	2	3	26
Digital forensics	9	8	3	8	28
IoT security	9	12	1	5	32
Incident response	17	4	3	6	27
OT/ICT/SCADA	6	8	1	11	30
Data Protection/PII/SPI	13	8	2	5	30
Data Loss Prevention	16	7	3	4	31
Vulnerability management	16	7	3	4	28
Cyber playbooks	14	6	2	6	30
Domain specific security e.g. devices	9	12	2	4	31
Security assessments (e.g. SOC 2- Type 2)	11	11	2	5	29
Security standards e.g. ISO 27001, CIS Top 20, Mitre Att&ck, etc.	11	14	2	4	30
Average	13	8	2	5	29

Q12b. If you plan to train employees in a specific vendor system over the next 1 to 3 years, please specify which system below:

Azure Sentinel.
EnCase, Magnet Axiom.
Focalpoint Data Risk academy.
Microsoft Suite of Security Products - e.g. MDATP.
Mostly internal training plus a bit of SANS.
MS Azure Security Center.
Multiple; too many to list.
n/a.
No Plan.
Palo Alto, IBM Qradar.
QRadar, CyberArk.
Splunk, Linux Red Hat Servers.
Training to be provided for multiple vendor systems.
Training varies across tools.
We're a very large organisation. Staff will receive training in multiple systems, as required.

Q12c. "If you plan to train employees in a specific programming language over the next 1 to 3 years, please specify which language below:"

Go, Python.
n/a.
n/a.
No.
No.
No Plan.
No plans to train employees, however Bash and Python are important to our SOC.
Python.
Python.
Python.
Python.
We're a very large organisation. Programming staff will receive training as required.

- Six respondents planning to train employees in Python.

Q12d. "If you plan to train employees in any other technical area over the next 1 to 3 years, please specify which area below:"

AWS, Azure.
Cloud Security.
CSSP.
Data Science & ML.
ISO27001.
Linux and Mac Operating System.
n/a.
No.
No Plan.
We're a very large organisation. Staff will receive all necessary training.

Q13. What transversal (i.e. soft) skills or non-technical areas do you plan to train your Cybersecurity employees in over the next 1 to 3 years? (select those that best apply).

Communication skills.	24
Incident Response Planning & Simulations.	21
Leadership.	17
Risk and Governance Management.	17
Project Management.	15
Agile.	14
Systems Thinking/Design Thinking.	12
Interpersonal Skills.	11
Teamwork.	9
Creative Problem Solving.	8
Critical Thinking.	8
Lean/Six Sigma.	8
Customer Service.	6
Innovative Thinking.	5
Business Case Development for Cyber Investment.	3
No soft skill training planned/required.	2
Training Needs Analysis.	2
Other (please specify):	1

- One respondent had an 'Other' training need in IAPP (a privacy certification)

Q14. In the future, how would you like your Cybersecurity training to be delivered? (select those that best apply)

Training Delivery Options	Preferences
Online training supported by remote facilitation/ coaching sessions.	13
A mix of online training and short F2F workshops.	9
Bootcamps (e.g. intense training spanning a number of weeks typically linked to a certification).	8
Purely online training with self-directed learning.	5
Team events (potentially involving Cybersecurity simulations).	3
Longer programmes (e.g. spanning up to year leading a qualification/certification).	2
Short F2F workshops (e.g. one to three days in length).	2
Don't know.	2

Q15. How important is certification-linked Cybersecurity training for your organisation?

Very important.	7
Important.	20
Neutral.	6
Not important.	2

Q16. Which of the following training and development initiatives (targeting Cybersecurity) would your company be interested in?"

INITIATIVES	POSITIVE RESPONSES
Graduate placements.	17
Internships.	13
Not interested in any of the above.	10
Funding of education at bachelor or master level in Cybersecurity.	8
Apprenticeships.	7
Traineeships and work placements.	5
New entrant mentorships.	4

Part 4 – Future Challenges

Q17. We would like to get your views on the challenges you anticipate facing in the Cybersecurity sector and what they might mean for future Cybersecurity skill requirements. How important will it be for your Cybersecurity employees to focus on the following strategic issues and challenges in the next 1 to 3 years? (select most appropriate response).

CYBERSECURITY CHALLENGES	CRITICAL	IMPORTANT	NOT IMPORTANT	NO RESPONSE
Remote working security.	23	10	1	1
Preparing for a major incident response.	23	11	1	0
Cloud native security.	19	11	3	2
Improving employee's cyber awareness.	18	14	2	1
Building cyber audit/assurance processes.	17	14	3	1
IoT security.	15	9	8	2
OT security.	14	11	6	3
Increased regulatory compliance.	13	17	4	1
Supply chain security.	13	16	5	1
Improving cyber risk governance.	12	20	3	0
Managing open source vulnerabilities.	12	15	6	2
Cyber vetting of suppliers.	11	17	5	1
Mobile application security.	8	20	5	2
Cybersecurity Agile testing capacity.	8	17	8	2
Utilising AI for Cybersecurity.	6	21	5	3

Q18. Considering the previous question, what new or emerging skills requirements will be important for your Cybersecurity employees to acquire?"

EMERGING SKILLS REQUIRED
Cloud assurance.
Cloud computing knowledge is probably the most relevant at the moment.
Cloud protection.
Container security, Kubernetes, knowledge of Linux kernel and systems.
Cyber professionals need to understand risk and be able to communicate to a non-technical audience.
DevOps, AI, SOAR.
Endpoint Detection and Response (EDR) technologies including Microsoft suite of products. Cloud Security and Web Application Firewalls (WAF).
Gathering and interpreting Big Data.
Improving Security Management skills including technical skills.
Incident Response, Breach Detection, Offline/Remote Challenges.
IoT Security, Cloud Security.
Managing Cybersecurity in cloud environments.
Managing the ecosystem in the context of Cybersecurity.
Multifunctional, multi- or bilingual and attention to detail plus forward thinking to suggest improvements.
Red and blue teaming.
Remote working, Cloud Security, Mobile Security, 3rd party/vendor security, phishing/vishing and other means.
Security frameworks like CIS.
Threat assessments and vulnerability assessments.

Part 5 - Cybersecurity Resources

We would like to get a view of the size and structure of your Cybersecurity function and resources to understand potential growth areas by role.

Q19. How are Cybersecurity services delivered within your organisation?

DELIVERY OF CYBERSECURITY	
Cybersecurity is a mix of in-house and outsourced capabilities.	14
Cybersecurity is primarily managed in-house.	13
Cybersecurity is primarily outsourced.	2
We are a Cybersecurity provider to other organisations.	6

Q20. Do you plan to make changes to how your Cybersecurity services are delivered?"

CHANGES TO SERVICES	
Bring services in-house.	7
No change.	24
Outsource further.	4

"Q21. How many Cybersecurity employees do you currently employ in Ireland?"

None (outsourced).	1
One to two in part time roles.	9
1 to 5 (full time roles).	8
6 to 10.	3
11 to 20.	3
21 to 50.	2
51 or more.	6
Don't know/no response.	3

Q22. Resource Planning

We would like to get a view on which roles are likely to grow in the coming few years. Do you plan to create new roles or expanding existing roles in any of the following? (select those that best apply)”

Incident Response Specialist.	11
Security Administrators.	10
Software/Application Security (DevSecOps).	10
Threat Hunting and Intelligence.	10
Security Architects/Engineers.	9
SOC Analysts L2.	8
Cybersecurity Team Leader.	7
OT Security Engineer.	7
SOC Analysts L3.	7
Cybersecurity Manager (e.g. Head of SOC).	6
Risk and Compliance Officers.	6
Senior Penetration Tester.	6
SOC Analysts L1.	6
Junior Penetration Tester.	5
Security Consultants (any level).	5
Digital Forensic Specialists.	4
IoT Security Engineer.	4
Technical Support/Support Desk.	4
Vulnerability Analysts/Assessors.	4
Cyber Learning & Development Manager.	2
Head of Cybersecurity.	2
No response.	5

Q23. Are you experiencing or do you expect to experience a shortage in skilled Cybersecurity employees that will impact your business?”

Don't know.	2
No, no impact on business.	5
No, no skill shortage encountered.	5
Yes, minor impact on business.	18
Yes, a significant impact on business.	5

Part 6 - Cybersecurity Maturity

We would like your view on the level of maturity you feel your organisation has achieved in the following key Cybersecurity tasks and whether it will be important to improve the capability in any of these. The two questions were:

Q24. On a scale 1 to 5 how mature is your...

Q25. On a scale of 1 to 5 how important is it to improve...

RESULTS TABLE	IMPORTANCE	MATURITY	GAP
Employees Cyber Awareness.	3.74	3.47	-0.27
Identity and Access Management.	3.69	3.85	0.17
Data Protection.	3.66	3.76	0.11
Network Protection.	3.59	3.91	0.33
Operational Security (OT/ICT/SCADA).	3.50	3.28	-0.22
IT Infrastructure/Architecture.	3.49	3.83	0.34
Incident Management.	3.49	3.91	0.43
Risk Management/Business Continuity.	3.40	3.77	0.37
Threat Intelligence.	3.35	3.74	0.38
Cybersecurity Strategy and Governance.	3.31	3.74	0.43
Compliance and Auditing.	3.23	3.79	0.57
Software/Application Security (DevSecOps).	3.18	3.58	0.39
Penetration Testing.	3.18	3.71	0.52
Digital Transformation.	3.03	3.59	0.56
Digital Forensics.	2.91	3.45	0.54
Average rating.	3.69	3.38	0.31

Part 6 - Cybersecurity Maturity

CAPABILITY MATURITY SCALE GUIDE:

Level 1 – Unprepared. Ad-hoc processes and insufficient systems/ resources.

Level 2 – Reactive. Resources and processes defined on a project basis.

Level 3 – Defined. Resources, policies and processes defined and centrally managed.

Level 4 – Measured. Fully resourced. Performance measured, monitored and controlled. Automation of basic tasks.

Level 5 – Progressive. Culture of continuous improvement. Advanced automation of tasks and controls.

Not applicable.

Don't know.

IMPORTANCE RATING SCALE:

Level 1 – Less important now, reducing resources here.

Level 2 – Satisfied with current state.

Level 3 – Important to improve.

Level 4 – Very important to improve.

Level 5 – Critical to improve.

Not applicable.

Don't know.

Bibliography

- [i] Expert Group on Future Skills Needs. "Forecasting the Future Demand for High-Level ICT Skills in Ireland, 2017- 2022." March 2019.
- [ii] FIT. "ICT Skills Audit, Widening the ICT Talent Pipeline for Sustained and Inclusive Growth." 2018.
- [iii] ISC2. "Strategies for Building and Growing Strong Cybersecurity Teams Cybersecurity Workforce Study." 2019.
- [iv] Department for Digital, Culture, Media and Sport. "Cybersecurity Skills in the UK Labour Market." March 2020.
- [v] ENISA (EU Agency for Cybersecurity). "Cybersecurity Skills Development in the EU, The certification of Cybersecurity degrees and ENISA's Higher Education Database." December 2019.
- [vi] World Economic Forum. "The Future of Jobs Report 2020." October 2020.
- [vii] Department of Justice and Equality Report. "Cybercrime: Current Threats and Responses." Sheelagh Brady and Caitriona Heintz. September 2020.
- [viii] PWC. "The Global State of Information Security Surveys; 2017, 2018, 2019."
- [ix] Neustar. "Cyber Treats & Trends: Jan-June 2020".
- [x] WHO News Release April 2020.
- [xi] NTT. "Global Guide to Threat Intelligence." 2020.
- [xii] Department of Justice and Equality Report. "Cybercrime: Current Threats and Responses." Sheelagh Brady and Caitriona Heintz. September 2020.
- [xiii] Trend Micro. "Securing the Pandemic-Disrupted Workplace - Midyear Cybersecurity Report." 2020.
- [xiv] Accenture. "Innovate for Cyber Resilience Lessons from Leaders to Master Cybersecurity Execution - Third Annual State of Cyber Resilience." 2020.
- [xv] RiskIQ. "Evil Internet Minute Report." 2019.
- [xvi] Third Way Institute. "To Catch a Hacker." <https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors>. October 29, 2018.
- [xvii] Deloitte. "Irish Economic Crime Survey." 2020.
- [xviii] EY. "Global Information Security Survey." 2020.
- [xix] Centre for Secure Information Technologies (CSIT), Queen's University Belfast. "Report on OT Vulnerabilities". April 2020.
- [xx] Gartner Report. The Urgency to Treat Cybersecurity as a Business Decision, 2020.
- [xxi] KPMG Security. "All hands-on deck: Key Cybersecurity considerations for 2020." 2020.
- [xxii] Interpol Report. "Assessment of the impact of COVID-19 on cybercrime". Quarter 1 2020.
- [xxiii] ENISA. "Good practice guide on training methodologies." 2020.
- [xxiv] McAfee. "Winning the Game report." 2020.
- [xxv] McKinsey and Company. "Hit or myth? Understanding the true costs and impact of Cybersecurity programs." 2017. <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/hit-or-myth-understanding-the-true-costs-and-impact-of-cybersecurity-programs>.
- [xxvi] Micro-Credentials: An Evolving Ecosystem, Insights paper, AUGUST 2020, Skillnet Ireland.
- [xxvii] www.eLearningLearning.com. "eLearning Statistics and Trends, 2020" <https://www.edapp.com/blog/elearning-statistics-trends-2020>.
- [xxviii] SEI Survey.
- [xxix] CyberSeek. "Cybersecurity Career Pathways". www.cyberseek.org.
- [xxx] National Initiative for Cybersecurity Careers and Studies. "Cyber Career Pathways Tool". <https://niccs.cisa.gov/workforce-development/cyber-career-pathways>.



it@cork Skillnet

The Rubicon Centre, CIT Campus,
Bishopstown, Cork.

T 00 353 (0)86 0848704

E skillnet@itcork.ie

W www.itcorkskillnet.ie

IT@Cork Skillnet is co-funded by Skillnet Ireland and network companies. Skillnet Ireland is funded from the National Training Fund through the Department of Further and Higher Education, Research, Innovation and Science.



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

