CYBER | IRELAND
IRELAND'S CYBER SECURITY CLUSTER

Position Paper:
Achieving Our Cyber Potential 2030

Recommendations Summary

1. Government as a Driver: Coordinator, Accelerator, Catalyst

1.1 Government as a coordinator of relevant agencies in Ireland's cyber security ecosystem and further development of public-private partnerships.

1.2 Government as an incubator and accelerator, to set challenges that are mission-critical to society and our economy and collaborate with companies to develop their solutions and adapt their current technology to a new cyber challenge and pilot solutions.

1.3 Government as a business catalyst, prioritising the growth of Ireland's cyber security sector and setting ambitious targets to be a leader internationally. The Office of Government Procurement to engage with cyber security companies to help co-create inclusive and impactful tender opportunities to support the development of the domestic cyber security sector.

2. Scaling the Domestic Cyber Security Industry

2.1 A dedicated programme to support Irish cyber security start-ups and scale-ups, learning from the UK's Cyber Runway

2.2 Increase investment opportunities for Irish cyber security start-ups & scale-ups to scale rapidly

2.3 Continued export missions and initiatives from Enterprise Ireland targeting key growth markets in Europe.

3. Developing a Pipeline of Homegrown Cyber Security Talent

3.1 A bi-annual Cyber Security Labour Market Report to analyse industry demand (Skills Shortages and Skills Gaps) and supply in the market.

3.2 Industry to increase the number of entry-level career positions to meet the supply of students and attract people into cyber security roles

3.3 Supports for SMEs to attract, train and retain cyber security talent to build capacity in the domestic sector.

4. Developing a Cyber Security R&D Ecosystem

4.1 Establish a National Cybersecurity Research Advisory Forum with key government stakeholders, funders and representatives from all HEIs with expertise in cyber security

4.2 Mapping & tracking of cyber security research expertise, projects and investment across research groups and industry.

4.3 A dedicated cyber security research call to stimulate research, coordinate partners and engage industry. Explore the potential for a national cyber security R&D infrastructure.

4.4 Investment in a nationally available Cyber Range for advanced R&I and testing for both public and private sector organisations.

Introduction

Cyber security is critical for all sectors of our economy and is inextricably linked with our national security and the smooth functioning of society. This was brought home to the Irish public in May 2021, when the Health Service Executive (HSE) suffered a major ransomware cyberattack causing its core IT systems nationwide to be shut down, leading to widespread disruption to patient services. It was the most significant cyber-attack in the history of the Irish State; the cost of the response and recovery has reached almost €43 million, which could rise to €100 million.[1] Furthermore, the cost of cybercrime to the Irish economy has greatly increased over the past seven years[2] and the incidence of cybercrime in Ireland is higher than global average.[3]

Internationally, there has been a significant increase in cybercrime with the global costs to the world economy estimated at more than $1 Trillion in 2020.[4] That's roughly one percent of global GDP. This is further impacted by a worldwide shortage of cyber security professionals across organisations of all sizes and sectors. Due to the increase of cyber-attacks, such as ransomware, cybersecurity is a rapidly growing industry internationally and the global cyber security market is growing at an annual compound growth rate of 12%.[5,6]

Cyber Ireland's Policy Paper reviews the findings and recommendations of the first "State of the Cyber Security Sector in Ireland 2022" Report, in the wider context of the Irish and international cyber security ecosystem. The focus of the Report and Policy Paper is on the cyber security sector, however, our national cyber security underpins the economic growth potential and in turn, a strong industry will support the State's cyber resilience. The strengths of the sector are outlined, followed by context of the European Union's (EU's) strategy and ambitions in cyber security. It then highlights the key market opportunities for the growth of the Domestic and Foreign Direct Investment (FDI) sectors.

To realise these opportunities and growth targets, we consider the barriers to growth for the sector at present. Finally, it sets out a range of recommendations to achieve our cyber potential, calling for a collaborative approach from stakeholders across industry, academia and government. The opportunity now exists for Ireland to capitalise on its strengths and competitive advantages to develop a strong cyber security sector, providing resilience domestically and competing internationally, if the right business environment and supports are in place.

1 https://www.rte.ie/news/ireland/2022/0223/1282617-cyber-attack-cost/
2 https://www.grantthornton.ie/insights/publications/cost-of-cyber/
3 https://www.pwc.ie/reports/irish-economic-crime-survey-2020.html
4 https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf
5 https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem
6 h-102500547.html ttps://finance.yahoo.com/news/global-cyber-security-market-2021

Securing Europe's Digital Future

Cyber security has become one of the main concerns for Europe's governments, organisations and citizens and the future development, opportunities and barriers to growth for Ireland's cyber security sector must be taken in the context of the EU's strategy and ambitions in cyber security. The European Commission (EC) published a new EU Cybersecurity Strategy at the end of 2020, covering the protection of essential services, industries and new technologies. A revised Directive on Security of Network and Information Systems (NIS 2 Directive) is in process which will expand the scope of NIS, strengthen security requirements and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU.

The EU Cybersecurity Act strengthens the EU Agency for cybersecurity (ENISA) and establishes a cybersecurity certification framework for products and services. There is increased research into digital security under the Horizon Europe (2021-2027) work programme 'Civil Security for Society' cluster with €1.6 billion funding available. The Commission aims to support cyber capacities and deployment through the Digital Europe Programme's investment of €1.9 billion (2021-2027) into infrastructures and tools across the EU for public administrations, businesses and individuals.

The European Cybersecurity Competence Centre (ECCC), based in Bucharest, together with the Network of National Coordination Centres (NCCs), is Europe's new framework to support innovation and industrial policy in cyber security. The Centre and the Network will make strategic investment decisions and pool resources from the EU, its Member States and, indirectly, the industry to improve and strengthen technology and industrial cybersecurity capacities, enhancing the EU's strategic autonomy.

There is no doubt that the EU is strengthening its cyber security capabilities and capacities in response to the increasing importance of cyber security for the EU's Digital Market and an over reliance on non-EU companies' technologies. This provides a major opportunity to grow the domestic sector by building up the capacity of Irish SMEs with goal of serving the EU Single Market. The National Coordination Centre will coordinate with industry, academia and research community, citizens, and the public sector and authorities under NIS. EU businesses will have access to direct grants and financial support.

The goal of enhancing the EU's strategic autonomy is a concerted effort in Brussels to limit dependence on non-EU controlled and headquartered enterprises and reducing their access to the EU Single Market. This also has the potential to greatly impact Ireland's attraction as a location for US, UK and other third country MNCs, in some of the following ways:

- Measures to restrict provision of services in the Single Market through the EU Cyber Security Act and the proposed NIS2 Directive.

- Regulating managed service providers and managed security service providers in digital infrastructure.

- Non-EU MNCs providing cloud services in the EU may be restricted on the basis of so-called 'sovereignty' requirements for cybersecurity certification under the EU Cyber Security Act.

- Exclusion from participation in EU co-funded investment programmes such as Connected Europe Facility, Digital Europe and Horizon Europe.

- EU co-funding of cross border projects on the island of Ireland under the Digital Europe Cybersecurity Programme cannot take place because Northern Ireland is part of a third country and is outside the Union.

- And as far as foreign direct investment screening into the EU.

This growing protectionism, notwithstanding the efforts of Ireland with some like-minded Member States to push for an open global approach encompassing trans-Atlantic cooperation, is also reflected in other digital files, such as the proposed Digital Governance Act, the Digital Markets Act and the Data Act.

Given the size and contribution of FDI to Ireland's economy, these risks need to be considered and mitigations put in place, such as diversification, attracting EU MNCs to Ireland, and building the capacity of the domestic sector.

A Strong Robust Cyber Security Sector

With the "State of the Cyber Security Sector in Ireland 2022" Report, we have for the first time a directory of 489 firms offering cyber security products or services to the market or employing staff in internal cyber security operations in Ireland, who employ over 7,300 professionals in Ireland.

The numbers working in cyber security roles in the wider economy mean that the overall employment in the sector is actually much higher. 160 firms, approximately one third, offer dedicated (or pure-play) cyber security services and the remaining two thirds of firms offer diversified services (i.e., cyber security is part of a wider company offering).

There are four particularly notable locations for cyber security activity in Dublin, Cork, Galway, and Limerick. These are collectively home to 73% of all cyber security offices. Cork has more firms per capita than any other region and has the highest concentration of cyber security multinationals.

Dublin has the highest number of offices and employment, in particular across diversified companies with cyber operations. There has also been significant regional investments in Multinational Corporations (MNCs) cyber security operations in Sligo and Kilkenny, demonstrating the ability of the sector to provide employment and economic growth in all regions.

From the economic analysis of the sector, we see that Ireland has competitive advantages regarding a higher number of firms, employees, sector revenue (€2.1bn) and GVA (€1.1bn) per capita in comparison to leading Cyber Security regions like the UK, including Northern Ireland. However, average salaries are higher in Ireland than the UK, which makes it a more expensive location.

Skills Pipeline

With a worldwide shortage of cyber security skills, locations that can provide in demand skills and experience will gain investment. Ireland has a strong cyber security talent pool with approximately 30,000 professionals with relevant cyber security skills.

There are a range of courses and training programmes in place supporting a pipeline of homegrown cyber security talent. Starting with entry-level training for cross-skilling from the live register, or those looking for a career change, such as Future in Tech, CyberQuest, FIT Cyber Apprenticeship and Cyber Bootcamp.

Cyber Ireland has mapped over 50 courses through higher and further education institutes producing relevant graduates to the sector. The HEA-funded Cyber Skills Project aims to train up hundreds of professionals from industry into cyber roles within their organisations.

Ireland's Domestic Cyber Strength

Almost half of firms identified (240) are Irish, employing over 2,100 people, reflecting a base to support domestic firm growth and expansion of their cyber security teams. Of the Irish firms, 101 are dedicated cyber security firms employing 1,240 people.

Enterprise Ireland has over 60 client companies in their cyber security portfolio with 8 companies on their High Potential Start-up Programme. For the past 5 years, 20 Irish cyber security firms raised over €110m in external investment, with notable investments in Tines, 4Securitas, Vaultree, and Nova Leah. Ireland has a range of services available to support firms at the start-up and scale-up level through Enterprise Ireland, who invest in over 70 High Potential Start-Up companies each year and manage a portfolio of over 1,300 investments in client companies.

Ireland's FDI Cyber Strengths

Ireland has positioned itself as a leading global location for ICT and ICT-dependent industries through a strongly supportive regulatory, taxation regime and education system that supplies top quality talent. This successful FDI policy and international business environment has led to development of our cyber security MNC sector.

Foreign firms make up 51% (249) of the total yet support c.71% (5,250) of all employment in the sector. Cyber security firms headquartered in the United States have a particularly strong presence in Ireland, making up 28% of firms and supporting c.55% (4,000 FTEs).

Examining pure-play cyber security firms, 6 of the top 10 global software security companies are located in Ireland and we now know that there are almost 60 cyber security MNCs employing over 2,100 people. The second group are MNCs across diversified sectors (such as ICT, Telecoms, Financial services, Health, and Manufacturing) who have established their internal security operations or product security teams in Ireland.

Additionally, the cyber security operations of diversified MNCs are a major contributor to the sector with 190 firms employing over 3,100 people in their cyber security teams. MNCs' operations are larger than Irish firms, with 194 large MNCs in the sector, which is significantly higher than in other studies (UK & NI) and in comparison to the wider economy.

Furthermore, the high-tech industry clusters and MNCs in Ireland are a key strength given their demand for cyber security, best practice, skills, innovation and external economics of scale. Accenture reports that Ireland is home to the highest proportion of cybersecurity leaders globally.[7]

"Leaders" are firms that achieve "significantly better results from their cyber security technology investments than other organisations", delivering and developing solutions at the highest standard within industry.

This showcases the current skill level of Ireland's cyber security workforce and the top factor for companies in locating their cyber business in Ireland is access to specialised skills.[8]

An Emerging R&D Ecosystem

Ireland's strong FDI sector, which has attracted high-value jobs, is supported through large scale research programmes. ICT is identified under Ireland's National Research Priority areas, which includes cyber security, providing opportunities for researchers and applications in this domain.

Cyber security research is carried out across a number of Science Foundation Ireland Research Centres, including LERO (Software), CONNECT (Future Networks and Communications), ADAPT (AI), INSIGHT (Data Analytics) and CONFIRM (Smart Manufacturing). This is also supported through several research groups across higher

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

8 https://www2.deloitte.com/ie/en/pages/risk/articles/cyber-opportunity-analysis-report.html

groups across higher education institutes (HEI), linking education, research, and industry regionally. New cyber security infrastructure is coming on stream, such as Munster Technological University's (MTU) mobile Cyber Range, funded through EI Equipment Call (€250k), and TU Dublin's Collaboratory and Security Operations Centre, funded under the Regional Enterprise Development Fund (€2.1m), which are both focused on developing industry projects.

As well as publicly funded research, Cyber Ireland's R&D survey in 2019 identified 25 companies undertaking cyber security R&D activities. These companies include both dedicated cyber security companies and diversified companies applying security research across diverse application areas and sectors.

Irish organisations have performed relatively well in attracting EU R&D and deployment funding for cyber security. Irish partners are participating in two of the four large scale (€15m each) European Cybersecurity Centre pilot projects, CyberSec4Europe (LERO) and ECHO (Maynooth University). University College Dublin's Centre for Cybersecurity and Cybercrime Investigation led a €7m EU H2020 project to develop a shared intelligent platform in the prediction, detection and management of crime.

What's the Role of the Cyber Security Cluster?

Today's, and tomorrow's, challenges demand new business models and ways of collaborating. No single company, university or government agency can solve these complex challenges alone. Only through cooperation and collaboration across organisational, political and cultural boundaries will they be addressed. Clusters provide a neutral cooperation platform and are the future way of collaborating.

Cyber Ireland, the national cyber security cluster organisation, was founded in 2019 to bring together industry, academia and government to represent the needs of the cyber security ecosystem in Ireland and support its growth. The cluster is industry-led, hosted at Munster Technological University and is supported by government through Enterprise Ireland, IDA Ireland and the National Cyber Security Centre.

Our cluster Mission is to strengthen productivity and competitiveness in companies through cooperation on innovation and the transfer of knowledge between companies, knowledge institutions and other support actors in the cluster.

Our Cluster Vision is to be a driving force to support world-class talent, innovation and solutions for Ireland's cyber security cluster.

Cooperation in our DNA

Industry clusters are a major part of the European industrial landscape, supporting increased jobs, wages, innovation and productivity. Cyber Ireland was established based on European best practice in cluster development. It has been developed with cooperation in its DNA to overcome the complex challenges facing business, government and society in cyber security.

In less than 3 years we have proven successful in facilitating connections, building trust, and supporting collaboration in our key activities. These initial wins have established the potential for further growth and success through the cluster model.

Coordination & Cooperation

The cluster has already over 130 members nationwide, with over 80 Irish start-ups and SMEs and almost 40 MNCs. We bring together eleven of the top higher education institutes (HEIs), who supply the skills and research required by industry. Additionally, we work with public and private training providers, education and training boards and relevant Skillnets.

Government plays a central role in the cluster, from economic development agencies, such as EI and IDA Ireland, to those protecting our country, such as the National Cyber Security Centre (NCSC), An Garda Siochana and Defence Forces. Cyber Ireland has become the collective voice for the cyber security cluster and coordinating body.

The following case studies profile the value of cooperation between organisations in the cluster:

Case Study: Supporting SME – MNC Connections

A low level of SME and MNC engagement was identified as a challenge for Irish cyber security companies, which has been worsened with the impact of Covid and the lack of events to facilitate networking. Given our strong FDI sector how might we increase engagement to grow Irish SMEs' business opportunities internationally through MNC operations in Ireland?

Cyber Ireland partnered with Enterprise Ireland and IDA Ireland to run a Virtual Cyber SME - MNC Networking Event in November 2021. 34 SMEs took part with the opportunity to meet with MNCs for new business. The event attracted directors and managers with responsibility for IT and IT Security from 17 MNCs. Over 60 targeted, one-to-one meetings were arranged with feedback from participants showing it was the most efficient platform to find and meet with new partners.

Case Study: Increasing Investment Opportunities for Irish Start-ups & Scale-ups

Global investment in cyber security firms reached record levels in 2021 surpassing $20bn.[9] However, Irish cyber security start-ups have longer lead times to secure investment in comparison to high-tech start-up hubs in Europe, such as London and Berlin. Additionally, there was a funding gap in European cyber security investment of over €4 billion in 2019 when compared with the USA. The lack of specialised growth capital, strategic buyers as well as international marketing and business skills is leading Europe to fall behind the US, Israel and China in this key strategic sector and European digital and cybersecurity champions are required to bridge the gap. Within this operating context, a new initiative was urgently needed to help address the funding deficit.

Cyber Ireland and Enterprise Ireland partnered with the European Cyber Security Organisation (ECSO) to host the Cyber Investor Days in Dublin, June 2022. Cyber Investor Days is a matchmaking initiative designed to provide access-to-finance and access-to-market opportunities for European cybersecurity start-ups and SMEs. Since its launch in 2017, the ECSO Cyber Investor Days have received more than 550 participants and hosted more than 600 B2B meetings.

VC's, with a cybersecurity focus from around Europe, travelled to Ireland to hear pitches from the 14 European cyber start-ups, including 8 Irish companies. This was followed by B2B meetings introducing the start-ups to investors, partners and buyers. The initiative has highlighted the innovative technologies in the Irish cyber security sector and brought VCs and investment opportunities for these start-ups, addressing a barrier to growth.

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

Case Study: A Collaborative Nationwide Skills Initiative – Cyber-Skills

In 2019, Cyber Ireland highlighted the severe shortage of cyber security professionals in Industry which could impact organisations of all sizes from SME's to MNCs and even public bodies. This concern and urgent need led four Irish universities, Munster Technological University (MTU), Technological University Dublin (TUD), University College of Dublin (UCD) and University of Limerick (UL), to collaborate and address this skills shortage. They created "Cyber Skills", a national programme that provides online, fully flexible, university accredited, micro-credentials and pathways that focus specifically on creating new skills, upskilling and reskilling for industry professionals in Ireland. Cyber Skills was awarded funding of €8.1 million by the Higher Education Authority (HEA), Human Capital Initiative (HCI), Pillar 3 highlighting the importance of such an initiative.

Dell and Mastercard became the first industry partners to work with the academic institutes to create three courses informed by their needs to cross-skill IT professionals. The project is now developing further courses with the input of industry partners across Manufacturing, financial services and SMEs. Cyber Skills also provides immersive learning with its Cyber Range which can simulate real-world scenarios and environments, including complex IT environments and attacks on IT infrastructure, networks, software platforms and applications in a secure, sandboxed virtual environment.

As our world becomes more digital and cyber security becomes of more importance to all ages, Cyber Skills created an Education and Public Engagement Programme with the aim of educating young people and secondary students about cyber security and the career opportunities. The Cyber Futures website (www.cyberfutures.ie) features information about the type of roles in cyber security, and career stories from people across the industry. The Cyber Academy provides technical training to young people to educate the cyber workforce of the future with a one week camp for 4th and 5th year students. Both Cyber Future and Cyber Academy are funded under Science Foundation Ireland Discover Programme.

Ireland's Cyber Opportunity

The Cyber Security Sector Report estimates that the sector is growing (with respect to the workforce) in Ireland by a similar magnitude to international growth, at a rate of 10%+ per annum. Based on the current baseline estimates, Ireland's cyber security cluster could support up to €2.5bn in annual GVA and the employment of over 17,000 cyber security professionals in the sector by 2030, if the right environment and supports are in place.

We breakdown the opportunity to grow Ireland's cyber security sector into the following:

1. Ireland's Domestic Cyber Opportunity - ***Growing Irish Cyber Security Start-ups, Scale-ups & SMEs to export internationally***

2. Ireland's FDI Cyber Opportunity – ***Growing pure-play Cybersecurity MNCs and diversified MNCs cyber operations, with higher value R&D investment.***

Ireland's Domestic Cyber Opportunity

Investment in cyber firms is likely to increase given the commercial opportunities that exist internationally.[10] Ireland can benefit from this increased international investment for Irish cyber security start-ups and SMEs to fund expansion and growth in operations.

Given the priority of, and investment in, cyber security for the EU, there is major opportunity for domestic companies to target the EU Digital Market and tap into the funding through EU programmes such as Horizon Europe, Digital Europe and the European Competency centre. However, a question persists over the capacity of Irish companies to scale and deliver high value services to the European market, and their ability to access the EU funding programmes.

Looking at the opportunity to grow the domestic cyber security firms, there is potential to grow Irish Cybersecurity firms' employment from 2,100 to over 3,000 (10% per annum) by 2030, to increase the number of medium and large size companies. We should support the growth of more cyber security start-ups coming through EI's HPSU programme, increase the number of companies receiving investment over a 5-year period from 20, and grow the overall investment in Irish companies from >€110m.

Additionally, cyber security is critical for all sectors of the economy, and SMEs in particular. Supporting strong indigenous sectors (such as manufacturing, agri-tech, construction, fin-tech) to increase their cyber security preparedness will protect them from cyber-related risks and can provide a value-add to their business when exporting.

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

Ireland's FDI Cyber Opportunity

There are two distinct opportunities relating to FDI growth:

a) Growing the Dedicated Cyber Security MNCs

Ireland has established itself as a leading location for cyber security MNC investment and talent. Ireland's next opportunity is to grow these existing cyber security MNCs and their operations to move up the value chain to highly skilled and productive jobs in engineering, development and research. To do so Ireland needs to build a science base that directly supports the enterprise sector to build their capacity for R&D.

Ireland can also benefit from the increased international investment through attracting scale-up cyber security companies to establish in Ireland as a first point of entry to the EU market and whereby existing cyber security MNCs can fund expansion and growth in their Irish divisions. However, this may become less attractive to non-EU MNCs due to the EU's digital sovereignty and protectionism. Thus, Ireland's FDI strategy should consider attracting EU-headquartered MNCs to Ireland also.

b) Growing the Cyber Security Operations in Diversified MNCs

Ireland can build on its existing strong FDI credentials across high-tech industry clusters and its cyber security skills pipeline to grow the cyber security teams of diversified MNCs here. Key sectors should be targeted to attract cyber operations based on Ireland's existing relationships and success with MNCs from the USA and UK, with the addition of EU MNCs.

Currently, there are c.50 UK-based firms with a cyber security team operating in Ireland, including firms that offer diversified services such as PwC, EY, and KPMG, as well as dedicated firms such as Sophos. There is a market opportunity to attract UK companies with cyber operations to establish their headquarters in Ireland to circumvent protectionist regulations enabling continued access to the EU Single Market.

Additionally, cyber security and trust is a key element of Ireland's broader FDI policy required in reassuring MNCs of the differentiated security and stability of Ireland's government, our national physical and digital infrastructure, and our business and social environments by virtue of our national approach to and capabilities in cyber security.

Barriers to Growth

Cybersecurity Preparedness & Government Prioritisation

The Global Cybersecurity Index (GCI)[11] is a trusted reference that measures the commitment of countries to cybersecurity at a global level. In the GCI 2020 Ireland ranks 46th globally and 28th out of 36 European Regions. The GCI notes that Ireland shows relative strength in legal and technical areas, however, it suggests that more can be done to develop national cooperative measures.

Increased engagement with industry and wider networks has the potential to increase awareness of cyber threats in Ireland's business landscape, where 61% of businesses reported that they suffered a cybercrime between 2017 and 2019. This is slightly more than UK businesses, 46% of which reported a breach.[12]

Skills Shortages:

Findings from Cyber Ireland's business survey suggest that over 60% of firms surveyed have staff-related issues, including lack of suitable candidates, skill-level, and unaffordable salaries. CI's Cyber Skills Report 2021 found that 46% of security teams were understaffed, 48% of firms had open or unfilled security roles and almost 20% of roles took 6 months or longer to fill.

With skills shortages and skills gaps already identified, how will we meet the forecasted target of an additional 10,000 professionals by 2030?

Ireland over relies on importing its cyber security talent internationally. The CI Skills Report 2021 found that 43% of new hires are from outside Ireland. COVID-19 has compounded existing skills challenges around recruitment, internationally and locally.

There is high demand for experienced hires (+5 years), however, there are not enough early career positions in industry to attract graduates and professionals into cyber security roles and provide the opportunity to progress to more senior positions.

Many job seekers note the difficulty for those without a typical computer science degree or experience in the IT industry to get their first cyber role. Work is required to improve recruitment process and job role criteria, with hiring and recruitment managers, to tap into a wider pool of talent.

These challenges are amplified for Irish SMEs who must compete with large MNCs for scarce talent in recruiting both graduates and experienced hires. SME's require support to invest in recruitment and training internal staff training and development, required to build capacity in the domestic sector.

11 International Telecommunication Union (2020) Global Cybersecurity Index. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
12 Stryvesecure (2021) 'How The UK and Ireland Compare When it Comes to Cybersecurity?'. Available at: https://www.stryvecure.com/blogs/how-the-uk-and-ireland-compare-when-it-comes-to-cybersecurity

Investment & Scale

The Cyber Ireland business survey found that 26% of firms faced issues with raising or securing finance, such as a lack of finance to grow or expand operations, insufficient scale to serve larger clients, or a lack of cash flow or working capital.

There are less investment opportunities for Irish cyber security companies in comparison to countries who prioritise the development of their domestic cyber security sector and start-up sector, such as the UK. This puts Irish start-ups at a competitive disadvantage and has resulted in Irish cyber security start-ups registering offices in the UK to gain access to supports.

Enterprise Ireland plays a critical role in supporting start-ups and scale-ups in Ireland, however, there is a lack of private investment options for Irish cyber security start-ups, especially those that do not receive investment from Enterprise Ireland.

Ireland requires a strong, domestic sector with companies of scale that can deliver high value services to a) provide cyber resilience for the country and b) compete internationally, in the EU Single Market. This is not the case at present. Ireland's domestic cyber security companies are predominantly micro and small size companies, that do not have the required capacity and expertise.

There has also been a number of Irish SMEs acquired by large European companies, which on the one hand provides investment to grow the business, yet reduces the number of Irish-owned business of scale. This is a critical issue of national cyber security importance that requires the support of Enterprise Ireland, NCSC and all relevant stakeholders.

Public Procurement

Cyber Ireland's business survey highlighted that Public Sector Tenders for cyber security can be too prohibitive for companies, and in particular SMEs and new firms. On the other hand, Irish SMEs need to increase their scale and capacity to be able to deliver high value, critical services to the public sector.

A Fragmented R&D Landscape

As cyber security research is being conducted across several SFI Centres and HEI research groups, there are a diverse range of cyber security research domains, application areas and projects. However, this has resulted in a fragmentation of expertise and capacity, a lack of focused research domains and small-scale projects. There is no national R&D centre for cyber security, nor is cyber security a central research theme with dedicated funding in existing SFI Centres.

These challenges are a barrier to engaging with industry to develop and address enterprise research challenges. Often, cyber security is a bolt-on to an existing research project as opposed to its own research project.

Additionally, Ireland has a lower capacity and capability to leverage the increased European funding through competitive programmes, such as Horizon Europe and Digital Europe.

It is not clear as to the level of cyber security R&D spending in Ireland as it is not tracked at present.

Ireland is competing with similar small, advanced economies such as Denmark, Finland and Israel, who have prioritised cyber security R&D investment. For example, Finland spends approximately €40M per annum on R&D in cyber security. Northern Ireland have prioritised the growth of its cyber security sector and invested in a leading cyber security research centre in Queen's University Belfast that is attracting investments in cyber security over Ireland. A strong research base is essential to develop a globally competitive domestic sector, attract and grow FDI, and support high value jobs.

Recommendations - Achieving our Cyber Potential

1. Government as a Driver: Coordinator, Accelerator, Catalyst

The Irish government can be a coordinator, incubator and business catalyst to drive the development of Ireland's cyber security cluster. It is important to demonstrate at government and political level that Ireland is a secure place in which to do business with, has a strong, resilient digital government and economy, understands and takes cyber security seriously. This messaging is of critical importance in establishing both national, and international, political credibility and models undertaken in countries such as the UK, Estonia, USA and Israel (see the review in the "State of the Cyber Security Sector in Ireland 2022").

Government as a coordinator of key agencies in Ireland's cyber security ecosystem (including the NCSC, An Garda Siochana, Defence Forces and Office of Government Procurement). The government has already funded coordination initiatives such as Cyber Ireland, through IDA Ireland and Enterprise Ireland. Developing these public-private partnerships is critical to development of the sector and national cyber security.

Government as a start-up incubator and accelerator can learn from examples such as UK NCSC 4 Start-ups programme, whereby the government sets challenges that are mission-critical to society and our economy and collaborates with companies to develop their solutions and adapt their current technology to a new cyber challenge and pilot solutions.

Government as a business catalyst by prioritising the growth of Ireland's cyber security sector and setting ambitious targets to be a leader internationally. The public sector is also a key buyer of products and services and there is an opportunity for future procurement activity to be tailored to support sector entry, scale-up, and partnerships between larger firms and SMEs. The Office of Government Procurement could engage with Cyber Ireland to help co-create inclusive and impactful tender opportunities, which would support the development of the domestic sector.

2. Scaling the Domestic Cyber Security Industry

Ireland requires a strong domestic cyber security sector with companies of scale that can deliver high value services to: a) provide cyber resilience for the country and b) compete internationally, in the EU Single Market. To do so, we must scale the size and operations of indigenous companies so that they can compete with the offerings and services of MNCs. There is a need to develop the capacity, both technologically and organisationally, of the domestic sector to be able to deliver high value services.

A dedicated programme to support the development and application of cyber security technologies is required, learning from the UK's Cyber Runway, [14] to help entrepreneurs and businesses access business masterclasses, mentoring, product development support, and secure investment so they can turn their ideas into commercial successes and trade internationally.

There is a need for increased investment funding and options for Irish SMEs to allow them to compete internationally with other strong cyber security regions. Specialist investment firms should be identified and partnerships built to foster the necessary investments and advice to Irish SMEs. Targets should be set to grow the number of investments into Irish companies and the amount in investment rounds, with ambition to create an Irish grown unicorn (valuations > $1bn).

Further export missions and initiatives, such as the Enterprise Ireland Cyber Innovation Series, can encourage increased international spend on Irish cyber security products to build on Ireland's reputation as a technology leader, targeting markets informed by EI's European Cybersecurity Market opportunity mapping exercise.

Specific measures are required to support SMEs to upskill and invest in staff training, which would benefit from targeted government grants and training programmes.

14 https://www.plexal.com/cyber-runway/

3. Developing a Pipeline of Homegrown Cyber Security Talent

To achieve our cyber potential in terms of employment growth to over 17,000 professionals working in the sector by 2030, an increase of 10,000, we need to supply the required skills meeting industry demand. A bi-annual Cyber Security Labour Market Report is required to understand industry demand (Skills Shortages and Skills Gaps) and supply in the market (new graduates, conversions, international attraction and attrition), similar to the UK.[15]

We need to raise awareness of cyber security careers and develop cyber security skills in students and young people, while providing opportunities for young people from diverse backgrounds. This needs to start with the inclusion of cyber security as a module in the Computer Science leaving certificate curriculum. A national cyber training programme for secondary school students (11-18 year olds), similar to the UK's Cyber First programme would greatly increase cyber security skills and interest in careers for you young people, and in particular girls.

In third-level, cyber security should not only feature in computer science courses, but become embedded across IT and STEM courses with the option to take cyber security modules across all domains.

Continued and increased engagement between higher and further educations institutions with industry is vital to ensure existing courses offer a curriculum that prepares students for a career within the sector, teaching them the skills necessary to engage at an entry-level.

Existing conversion programmes are making good progress training up people with cyber security skills. Industry must increase the number of entry-level career positions, through internships and graduate roles, to meet the supply of students and attract people into cyber security roles. The scope of entry-level positions needs to be expand beyond accepting third level students from only computer science or cyber security degree programs, for career changers new to the industry where 'no experience in security is required' and people who do not hold a formal third level education.

The funding of the HEA HCI Cyber Skills project is much welcomed and has the opportunity to train up hundreds of industry professionals into specific cyber security roles. Further support is required for SMEs to develop internal staff training to build capacity in the domestic sector and compete with large companies.

15 https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2021

4. Building a Cyber Security R&D Ecosystem

There is significant potential to leverage the cyber security industry base identified and develop an enterprise-focused R&D ecosystem. An investment in fundamental research will drive research "upwards" to exploitation, leading to greater opportunities in applied research and greater capacity for collaborative R&D industry focused projects on emerging research topics related to cybersecurity and digital, grounded and supported through the existing SFI research centres.

Building greater capacity in fundamental research will also make Ireland a more attractive location for researchers and will make researchers more competitive in attracting non-exchequer funding such as Horizon Europe and Digital Europe programmes.

Measure 14 in the National Cyber Security Strategy reflects the importance of building a more comprehensive cyber security R&D ecosystem stating that "Science Foundation Ireland, along with DBEI and DCCAE, will explore the feasibility through the SFI Research Centre Programme, the Research Centre Spoke programme or other enterprise partnership programmes, to fund a significant initiative in Cyber Security Research." Towards this goal the following recommendations are proposed:

A National Cybersecurity Research Advisory Forum should be established to include representatives from key government stakeholders, funding agencies, SFI Centres and HEIs with expertise in cyber security, which has been done successfully in other research domains such as quantum. Based on research domain expertise, this group could strategically target a combination of existing R&D funding mechanisms (national, all-island and European) to build capacity and capability across HEIs. It would advise government and funding agencies on policy, mechanisms and measures to build greater capacity in cyber security research.

A mapping of cyber security expertise and projects across research groups and centres should be undertaken to track investment in cyber security R&D and raise awareness of the research capabilities available for industry to engage in. An investigation of industry R&D needs in cyber security is also required, with one-to-one engagement with companies, to develop enterprise-focused R&D programmes and matchmake industry to the public sector research expertise across the SFI centres and HEIs.

A dedicated research call in cyber security, applied to sectoral applications where Ireland is a leader, would stimulate research, coordinate partners and engage industry. This has been utilised in other critical areas of importance, such as the SFI-Defence Organisation Innovation Challenge (€2.4m) or the Disruptive Technologies Innovation Fund (DTIF) Call 5 targeting the Advanced and Smart Manufacturing sector. domains.

A nationally available cybersecurity infrastructure would allow advanced R&I in cybersecurity. In particular, a national Cyber Range would support both public and private sector organisations to test, in a secure sandboxed environment, the cyber-resilience of their digital systems against cyber-attacks, allowing weaknesses to be identified and remedied before cybercriminals can exploit them.

The development of our cyber security R&D ecosystem will drive the next phase of the cyber security sector's growth and will significantly contribute to Ireland's cyber resilience and national security.