Cyber Ireland Submission to National Cyber Security Strategy Mid-Term Review

Cyber Ireland welcomes the publication of the National Cyber Security Strategy (NCSS) Mid-Term Review (MTR) and the Department of Communications engagement with Cyber Ireland members in a webinar on the 20th of January.

Cyber Ireland Progress to Date

Much has changed in just over 3 years since the National Cyber Security Strategy (NCSS) strategy was published in 2019 – from COVID-19, to the HSE ransomware-attack, the war in Ukraine, to policy developments at a European level. During the pandemic, we saw the need for cybersecurity has never been greater. However, with the current economic downturn, companies are asking how they can do more with less, which will impact IT, and thus cybersecurity budgets, particular for SMEs. It is critical we keep the need for cyber security to the forefront of every business, government and citizen in Ireland.

Since 2019, Cyber Ireland has developed from a start-up organisation, which the National Cyber Security Centre was key in establishing, to a national representative body with 150 members nationwide including over 80 Irish start-ups and SMEs, 40 MNCs and 11 Universities; we now provide a collective voice for the cybersecurity sector. The cluster has delivered activities across four workstreams of: 1) Building the community; 2) Developing a sustainable talent pipeline; 3) Enhancing collaborative research and development; and 4) Supporting the growth of the domestic sector and foreign direct investment (FDI).

The inaugural "State of the Cyber Security Sector 2022" report[1] was published last year establishing that there are 489 companies in the sector employing 7,351 professionals, with revenues of over €2bn and contributing €1.1bn to the economy annually. The report highlights the potential growth of the sector to 2030 to support over 17,000 jobs and €2bn in gross value added (GVA). In response to the report findings, Cyber Ireland published a Position Paper, 'Achieving Our Cyber Potential 2030,' with recommendations on how to realise the opportunities and growth targets by addressing key challenges, calling for a collaborative approach from stakeholders across industry, academia and government.

Cyber Ambition – A National Cyber Security Commitment is Required

The European Commission publishes the Digital Economy and Society Index (DESI), which ranks Member States according to their level of digitalisation. Ireland is a digital front-runner in Europe, ranking 5th of the 27 EU Member States in the 2022 edition. However, according to the similar cyber security benchmarks Ireland is laggard internationally. The ITU Global Cybersecurity Index (GCI) measures the commitment of countries to cybersecurity at a global level. In the GCI 2020[2], Ireland ranks 46th globally and 28th out of 36 European Regions. Our lower commitment to national cyber

[1] https://cyberireland.ie/state-of-the-cyber-security-sector-in-ireland-2022/
[2] https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

security is putting Ireland's citizens, government and business at risk of cybercrime, disruption to essential services, and our position of being a safe and secure place to live, work and do business.

A whole of government approach is required to ensure Ireland improves its cyber security commitment and delivers on the NCSS vision of "an Irish society that can continue to safely enjoy the benefits of the digital revolution and can play a full part in shaping the future of the internet". The NCSS vision and objectives outlines the role of Government to develop the capacity of the state and the role of industry under the "Develop" priority.

A mature and diverse cyber security industry can play a significant role in accelerating the actions and meeting the objectives to achieve this vision. This has been demonstrated internationally across leading cyber security nations who have supported and developed strong cyber security industry sectors, according to the GCI 2020 such as the United States of America (Rank No. 1), United Kingdom (2), Australia (12), Netherlands (16), Israel (36), among others. The UK National Cyber Security Strategy[3] outlines a commitment to ecosystem development under Pillar 1, through three objectives: 1) strengthening networks and partnerships, 2) Enhancing and expanding cyber skills, and 3) "foster the growth of a sustainable, innovative and internationally competitive cyber and information security sector, delivering quality products and services, which meet the needs of government and the wider.

Government can also play a central role in the development of the cyber security industry in Ireland, and a stronger industry sector not only drives economic growth, but in turn, supports the state's national cyber resilience. Cyber Ireland's position paper calls for an increased role for government to be a driver of the cyber security industry, as a "Coordinator, Catalyst and Accelerator". This opportunity should be reflected and integrated into the vision and objectives of the NCSS:

- As a coordinator of relevant departments and agencies to drive the development of the cyber security sector, setting out an enterprise development strategy, ambitious targets for growth and branding Ireland internationally.
- As a catalyst of cyber security start-ups and innovation addressing the needs of businesses, government and society.
- As an accelerator of cyber security companies in Ireland to scale and mature, deliverhigh value solutions and become internationally competitive.

There has been significant progress made on the actions of the NCSS to date, as well as the development of the National Cyber Security Centre with increased funding and recruitment following the Capacity Review 2021. Of note in the NCSS, are some measures that have not seen the same progress, in particular:

- Measure 14 – a significant research initiative funded through the Science Foundation Ireland (SFI) programmes, and
- Measure 16 – a cyber security programme to facilitate collaborative links between enterprise and the research community, to be developed by Enterprise Ireland (EI)..

This highlights the need for a whole of government approach to cyber security, led by the NCSC within the Department of Communications, with buy-in from DFHERIS, DETE, DPER, DoJ and DoD, including

[3] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

relevant agencies from SFI, EI, IDA, An Garda Síochana, Defence Forces, Office of Government Procurement among others.

Cybersecurity risks are increasingly borderless and cannot be prevented by any single stakeholder. Cooperation and collaboration remain an essential tool to tackle cybersecurity challenges, requiring interagency and public-private partnerships. The GCI notes that Ireland shows relative strength in legal, technical and organisational areas, however, our cooperative measure scored lowest (12.11/20).

By acknowledging the rapid change in the digital landscape since the NCSS strategy was published in 2019, we must plan accordingly for future technological developments and transformation. Thus, the NCSS must be forward looking and a foresight analysis of technological, economic and societal trends impacting cyber security should be undertaken to plan appropriately for what will be required by 2030 to ensure Ireland's national cyber resilience.

To address current challenges, support coordination and ensure future cyber resilience, Ireland should invest in a cyber security campus bringing together the key stakeholders across government, industry and academia that contribute to our national cyber resilience under one roof. The campus will provide a centre of gravity for cyber security in the state, coordinating government departments and agencies, supporting enterprise development from start-ups, SMEs to MNCs, providing training and enhancing technological innovation. It should also engage with the public, supporting cyber security awareness and education, strengthening a digital society. International examples already exist, such as the French Cyber Campus[4], Hague Security Delta Campus[5] Netherlands, the Cybercampus Sweden[6], and CSIT in Belfast[7] - the UK's Innovation and Knowledge Centre (IKC) for secure information technologies.

Further detail on specific measures to achieve the NCSS vision through public-private partnerships and enterprise development is provided under the relevant sections of the strategy below.

8. Public Sector Data and Networks

1. **NCSC accreditation scheme for companies providing cyber security services to the public sector**

Cyber Ireland supports the proposal to establish an NCSC accreditation scheme for companies providing cyber security services to the public sector in Ireland. Setting clear requirements, based on accepted cybersecurity best practices and relevant international standards, will build maturity of the cyber security providers to the public sector. Additionally, an NCSC accreditation would provide validation and credibility to cyber security SMEs to support international exports. The availability of references and case studies from public sector customers will greatly support this.

2. **Cybersecurity Baseline Framework for companies supplying the public sector**

Further, all companies providing services to the public sector in Ireland which involve handling sensitive and personal information or the provision of certain technical products and services should meet a cyber security baseline standard. This would address supply chain risk for the public sector and improve the cyber security posture of businesses, in particular for SMEs. A similar programme to the

[4] https://campuscyber.fr/en/
[5] https://securitydelta.nl/about/hsd-campus
[6] https://cybercampus.se/
[7] https://www.qub.ac.uk/ecit/CSIT/

UK's Cyber Essentials and Cyber Essentials Plus, backed by government (NCSC and NSAI) and delivered by the private sector is required in Ireland.

Cyber Ireland recently commenced a pilot programme with the Small Firms Association (SFA) to provide a baseline cyber security framework for Irish SMEs, called the Cyber Ireland 4 Pillars (CI4). The cyber security guidelines of the framework will protect SMEs from the most common cyber-attacks, resulting in reduced cyber risk. We have partnered with a lead insurer, who will provide a discount on cyber insurance premiums to SMEs who have completed the CI4 self-assessment. There is potential to scale this pilot nationally with the addition of a 2nd phase that would provide increased cyber security protection with a cyber security consultancy, which could be done at no-cost to SMEs through utilising the Local Enterprise Office (LEO) digitalisation voucher (€5k) and Enterprise Ireland Digitalisation Voucher (€10k).

9. Skills (incl. R&D)

Ireland's cyber security sector and employment is growing rapidly, reflecting global growth in the cyber security market, with potential for a further 10,000 roles in the sector by 2030.[8] However, existing cyber security skills shortages and skill gaps are the number one challenge facing the cyber security sector in Ireland. This shortage impacts all digitally intensive sectors of the economy, as well as the public sector. How we meet this demand given the existing skills shortages and skills gaps will be central in making Ireland a safe and security place to live and work.

3. **Multi-annual Cyber security skills in the Irish labour market Report**

To meet the potential demand for an additional 10,000 cyber security professionals by 2030, Ireland requires research on current and future industry demand (skills shortages and skills gaps) and supply in the market to understand the workforce gap, similar to the UK annual "Cyber security skills in the UK labour market" Report[9]. The objectives of the report should gather demand-side evidence on skill gaps and skill shortages, location of roles, staff turnover and diversity in the sector. Additionally, the research should gather supply-side evidence on: supply of skills from further and higher education institutes, the available recruitment pool and the workforce gap. A Cyber Security Skills in the Irish labour market Report is required, and Cyber Ireland requests government to partner with industry to produce a multi-annual report to track trends and trajectory.

4. **NCSC Accreditation of 3rd level Irish cyber security courses**

To produce a high-quality talent pipeline, cyber security courses must meet international standards. With many third-level providers offering degrees containing cyber security content, it can be difficult for students and employers alike to assess the quality on offer and to identify the degree that best suits someone's preferred career path. NCSC-certified degrees will help:

- universities to attract high quality students from around the world,
- employers to recruit skilled staff and develop the cyber skills of existing employees,
- prospective students to make better informed choices when looking for a highly valued qualification.

5. **A national cyber education and career programme for young people (11-18 year olds)**

[8] https://cyberireland.ie/state-of-the-cyber-security-sector-in-ireland-2022/
[9] https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2022

With worldwide shortages of cyber security professionals, we will need to plan for the long-term and attract the next generation of cyber security professionals. Funding for a national cyber security education and careers programme targeted at secondary schools (11-18 year olds) is required to achieve this, which should leverage and coordinate existing initiatives such as the DECC facilitated CyberWise junior cycle short course, Cyber Futures project funded by SFI Discover Programme, as well as the Secondary Schools Capture The Flag (CTF) competition run by ZeroDays CTF.

6. Research & Development, EU Funding

Cyber Ireland supports the proposals for further measures to develop a cyber security research and development (R&D) ecosystem. There is significant potential to leverage the cyber security industry base and develop an enterprise-focused R&D ecosystem to drive the next phase of the cyber security sector's growth and significantly contribute to Ireland's cyber resilience and national security.

6.1 Strategic Advisory Group of Cybersecurity Research Stakeholders

A National Cybersecurity Research Advisory Forum should be established to include representatives from key government stakeholders, funding agencies, SFI Centres and Higher Education Institutes (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.

A dedicated R&D call in cyber security for collaborative industry-academic projects is required to build the R&D base. 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.

6.2 'National Cyber Security Support Centre'

Cyber Ireland supports the establishment of the 'National Cyber Security Support Centre' to promote industry awareness of EU public funds for improving cybersecurity capabilities and availing of state-of-the-art cybersecurity solutions. The cluster can contribute to the objectives of the centre and implementation of the activities as it already provides cooperation platform bringing together the key stakeholders across industry, government and academia. The cluster organises regular regional events through its regional chapters (South, West, North-West and Dublin) and annual national conference. It provides updates on funding calls through the CI Funding Portal[10] and organises regular R&D workshops on upcoming calls. The cluster is connected in Europe as a member of the European Cyber Security Organisation (ECSO) and internationally through the Global EPIC network of over 30 cyber security ecosystems worldwide.

6.3 Establish a European Digital Innovation Hub on cybersecurity

The European Digital Innovation Hubs (EDIH) are one-stop shops supporting companies to respond to digital challenges and become more competitive disseminate the latest advances in cybersecurity,

[10] https://cyberireland.ie/funding-calls/

Artificial Intelligence (AI) and High-Performance Computing (HPC). Four EDIHs have been approved by the state, yet none have a pure focus on providing cyber security solutions for businesses, putting Irish industry at a disadvantage to European counterparts with cyber EDIH. Thus, Cyber Ireland calls for the state to support European Digital Innovation Hub on cybersecurity.

10. Enterprise Development

7. Strategy on the development of the cyber security industry in Ireland

Government can play a central role in the development of the cyber security industry, and a stronger industry sector not only drives economic growth, but in turn, support the state's national cyber resilience. Cyber Ireland's position paper calls for an increased role for government to be a driver of the cyber security industry, as a "Coordinator, Catalyst and Accelerator". An enterprise development strategy for the cyber security sector is required to drive its development and realise the opportunities and growth targets set out in the "State of the Cyber Security Sector Report 2022". It should include an international branding of Ireland as a cyber security hub indigenous technologies, pure-play cyber security MNCs and diversified MNCs cyber operations.

8. National Cyber Innovation Hub

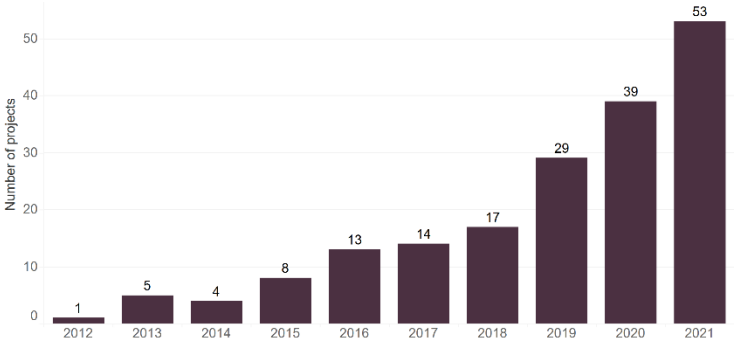
A foresight analysis of technological, economic, societal trends impacting cyber security should be undertaken to plan appropriately for what will be required by 2030 to ensure Ireland's national cyber resilience.

Ireland should invest in a cyber security campus bringing together the key stakeholders across government, industry and academia that contribute to our national cyber resilience under one roof. The campus will provide a centre of gravity for cyber security in the state, coordinating government departments and agencies, supporting enterprise development from start-ups, SMEs to MNCs, providing training and engaging technological innovation. It should also engage with the public, supporting cyber security awareness and education, strengthening a digital society. International examples already exist and are in development, such as the French Cyber Campus[11], the Cybercampus Sweden[12], CSIT[13] - the UK's Innovation and Knowledge Centre (IKC) for secure information technologies.

[11] https://campuscyber.fr/en/
[12] https://cybercampus.se/
[13] https://www.qub.ac.uk/ecit/CSIT/

9. Improving Cybersecurity Public Procurement for sector development

Figure: Number of publicly procured tenders in cyber security



The public sector can play a critical role in being a business catalyst and maturing the cyber security sector as a key buyer of products and services. An analysis of tenders published publicly in Ireland[14] between 2012 and 2021 saw a significant increase in publicly procured cyber security projects.

Cyber Ireland's Business Survey 2021 found that public procurement tenders for SMEs were restrictive and inhibiting newer firms and small companies from participation. Cyber Ireland worked with InterTradeIreland to run a Go2Tender workshop specifically focused on the Public Sector market for Cyber Security. This workshop, which had input from the Office of Government Procurement and CPD Northern Ireland, highlighted the significant opportunities emerging, and also identified some of the challenges that SME Cyber specialists face in accessing public sector Cyber security contracts. After the workshop, a list of the perceived challenges was collated, verified by the Cyber Ireland SME Committee and a survey of SME members identified the top-ranking perceived challenges in cyber security tenders.

The government should utilise public procurement to build cyber security capability within industry in Ireland, ensuring national cyber resilience. Engagement between the Office of Government Procurement with the cyber security sector, through Cyber Ireland, should aim to address existing challenges and co-create inclusive and impactful tender opportunities. Public Procurements should prioritise Irish-based service and product providers for specific needs, to build cyber security capacity and capability in the country.

[14] Etenders (2022). 'Published tenders'. Available at: https://irl.eu-supply.com/ctm/Supplier/PublicTenders