Cyber Ireland Oireachtas Statement 31st May 2023

Chairperson, Committee Members, it is my pleasure to attend this committee once again, this time in my role as chairperson of the advisory board of Cyber Ireland, give an opening statement and answer any questions you may have today. Cyber Ireland raison d'etre is collaboration, co-ordination, and leadership to develop our sector. We are delighted to be here today with this wider and diverse group, a number of whom are Cyber Ireland members. Our commons purpose is to articulate and execute a common vision for cyber security for Ireland. We believe that Cyber Ireland as an already established and functioning resource is best placed as the tip of the arrow to help develop, coordinate and lead on this common vision.

Cyber Ireland Overview:

Cyber Ireland is the national cyber security cluster organisation of Ireland, an industry representative body launched in 2019 to bring together industry, academia and government to represent the needs of the cyber security sector in Ireland and support its growth.

The cluster is industry-led, hosted at Munster Technological University, and is supported by government through the National Cyber Security Centre, with funding from IDA Ireland and Enterprise Ireland.

The cluster has over 160 member organisations nationwide, with 50 MNCs and 90 SMEs, as well as 10 Universities.

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

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) (further detail on workstreams below):

Cyber Ireland Goals & Workstreams:

1. **Building the Community** – Bringing the cyber security cluster (industry-academia-government) together to facilitate networking, sharing of knowledge and collaboration through our regional chapters and national events. Last year we hosted our first national conference attended by over 250 from industry.
2. **Promotion** – Ensuring strong national branding and promotion of the cluster.
3. **Talent & Skills** – Supporting a sustainable supply of cyber security professionals to meet current and future industry needs.
4. **Innovation** - Enhancing cyber security research and innovation between industry and with academia
5. **Grow & Export** – Increasing international competitiveness to support indigenous start-ups and SME's and attract FDI.
6. **Influence** – Provide a collective voice, research and policies to represent the cyber security cluster in Ireland and advocate on behalf industry needs, working with partners in government and industry.

International Picture:

Cybersecurity is a rapidly growing industry internationally, for which there are a number of opportunities and challenges:

- $250billion worldwide cybersecurity spending predicted by 2023, growing 12% CAGR
- The annual global cost of cybercrime has exceeded $10.5 trillion annually, the 3rd largest economy in the world after US and China and increasing globally by 15% CAGR
- 0% – the unemployment in cyber security and 3.5 million unfilled jobs predicted
- Increasing global competition for talent & investment

Risks & Challenges for Ireland:

- Data Centre of Europe w/ MNC presence
- Increased Cyber Crime globally & in Ireland, the economic impacts of cyber crime puts our Indigenous SME sector at risk and has knock effects on our FDI brand
- Digital Leader & Security laggard - 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[1], Ireland ranks 46th globally and 28th out of 36 European Regions.

Ireland Strengths

Ireland has become a significant base of international technology and security companies.

The inaugural "State of the Cyber Security Sector 2022" report[2] was published in 2022 by Cyber Ireland, mapping the size and make-up of the cyber security sector for the first time:

- 6 of the top 10 software security companies are based here
- 160 pure-play cyber security companies & 300 companies with cyber operations in Ireland
- Employing 7,500 people, with revenues of > €2bn p.a. and contributes €1.1 bn in gross value add to the economy p.a.
- Strong talent pool, highly skilled multi-lingual workforce & Talent development programs.
- We are a digital Leader, attracting FDI, hosting much of EU's Data - Dublin is Europe's largest data hosting market

Ireland's Opportunity

Ireland is uniquely placed to benefit from increased global investment, it has an opportunity to position itself as a global leader for cyber security talent, innovation and investment. Cyber Ireland aims to facilitate the cyber security ecosystem to capitalise upon this opportunity.

The report highlights the potential growth of the sector to 2030 to support over 17,000 jobs and €2bn in gross value added (GVA).

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

Cyber Ireland published a Position Paper, 'Achieving Our Cyber Potential 2030,' in 2022 with recommendations on how to realise the our Cyber Potential and growth targets by addressing key challenges, calling for a collaborative approach from stakeholders across industry, academia and government.

Challenges:

1. Need for better government coordination on cyber security across departments led by NCSC
2. Scale and mature the indigenous cyber security sector
3. Address the cyber security skills shortages in industry and public sector
4. Address the fragmented, and under-support R&D landscape, Low level of collaborative security R&D between industry – academia in Ireland.

Ask

A mature and diverse cyber security industry will play a significant role in supporting Ireland's National Cyber Resilience. This has been demonstrated internationally across leading cyber security nations who have supported and developed strong cyber security industry sectors, such as the United States of America, United Kingdom, Australia, Netherlands, Israel, among others.

1. **Government Coordination** - A whole of government approach is required to ensure Ireland improves its cyber security commitment and delivers on the National Cyber Security Strategy 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". This highlights the need for better coordination in government to cyber security, which should be led by the NCSC within the Department of Communications, with buy-in from DFHERIS, DETE, DPER, DoJ and DoD, including relevant agencies from SFI, EI, IDA, An Garda Síochana, Defence Forces, Office of Government Procurement among others.

2. **Cyber Security Campus** - 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 branded entity. The campus will provide a centre of gravity for cyber security in the state, coordinating government departments and agencies (across NCSC, AGS & DF), supporting enterprise development from start-ups, SMEs to MNCs, providing training and enhancing technological innovation in most likely some form of hub and spoke model. 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[3], Hague Security Delta Campus[4] Netherlands, the Cybercampus Sweden[5], and CSIT in Belfast[6] - the UK's Innovation and Knowledge Centre (IKC) for secure information technologies.
    a. Min investment of €40M a year for a Cyber Security Campus required to ensure that the gap between Ireland's Digital Index and cyber security preparedness is addressed.[7]

[3] https://campuscyber.fr/en/
[4] https://securitydelta.nl/about/hsd-campus
[5] https://cybercampus.se/
[6] https://www.qub.ac.uk/ecit/CSIT/
[7] CYBER-EXPLORE (2020) Proposal to Science Foundation Ireland by Cyber Ireland, Munster Technological University & University College Dublin.

b. To ensure that Ireland maintains its competitive advantage as a safe place of doing business and to establish national trust needed for future inward investment greater investment of up to €80m per year is required.

3. Train up 10,000 new professionals with cyber security skills to create a sustainable pipeline of talent for the private and public sector.
    a. Funding for a national cyber education and career programme for young people (11-18 year olds)

4. Deliver a Cybersecurity Baseline Certification for all companies in Ireland (e.g. Cyber Essentials / CI4), and a requirement for companies supplying public sector bodies. Three goals:
    a. Improved Cybersecurity Protection - To support all organisations to mitigate their cyber security risks, with the priority that it is an effective means for SMEs to protect themselves (UK Cyber Essentials prevents around 80% of cyber attacks).
    b. Demonstrate supply chain security - To be an effective tool for large organisations and government to help manage third-party cyber security risks (Potential for public sector bodies' suppliers dealing with data or confidential information to require the certification)
    c. Reduce cyber insurance premiums through a certified cyber security baseline.

5. Cyber Security to be designated as one of 5 National Clusters under the Department of Enterprise's National Cluster Programme by 2025.

Ensure that Cyber Security is incorporated into strategic government funding mechanisms to support our cyber ambition, such as:

- Enterprise Ireland – Enterprise Supports
- PeacePlus - €1.1bn
- SFI Research Centre Programme

Target European Funding

- Digital Europe – €8.2 billion, with €1.8 set aside for cyber security capacity building.

Investing in Cyber security is unique amongst National Security Spend. If we can move our National Cyber Security capabilities to European and Global leadership status we will secure our digital economy, our digital society and our citizens. In doing so we will project Ireland as leader in Cyber Security practice and innovation, with a very real opportunity to generate 5 to 10X orders of magnitude of return on this national investment.