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.

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, [1] 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.

---

1 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.[2]

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.

---

2 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.