www.amcham.ie @americanchamber

AMERICAN CHAMBER of COMMERCE IRELAND

Consultation on the Draft Cyber Industrial Strategy

Response from the American Chamber of Commerce Ireland (AmCham) to the Department of Environment, Climate, and Communications

April 2024

The Strategy and Pillars

1. Do you think sustained state intervention and support is crucial for advancing research and innovation in cybersecurity, fostering professional workforce development, and bolstering enterprise supports within the community? How could this be achieved?

AmCham welcomes the opportunity to respond to the Department of the Environment, Climate and Communications' consultation on its Draft Cyber Industrial Strategy.

Cybersecurity is a core priority of AmCham and its members. The digitalisation of Ireland's economy necessitates increased investment in, and further development of Ireland's cyber industry. Ireland must be to the forefront of global efforts to identify, withstand and tackle cyber threats.

Ireland is home to the EMEA headquarters or significant operations of many of the world's largest companies. There are over 970 US companies in Ireland who directly employ over 210,000 people and indirectly support a further 168,000 jobs in the Irish economy. The presence of multinationals in Ireland also significantly benefits our indigenous business environment, our local communities, and supports balanced regional development. Ensuring Ireland is a global leader in cybersecurity is important for both indigenous and FDI companies and must be a priority going forward.

As the consultation document acknowledges "*multinational companies, both pure play cybersecurity and the large digital firms, are the economic powerhouse of the Irish economy*."[1] Given the reputational and financial costs which could result from a cyber attack, the economic importance of cybersecurity must be recognised. Indeed, the reputational repercussions of the attack on the HSE in 2021 are evident in research carried out by the Department of Defence. Research from the 2023 National Risk Assessment found that "*the public rated cyber attack as* Department's *the highest rated key risk facing Ireland. Cyber attack was also one of four risks receiving the highest rating from the Expert Focus Groups*."[2] Providing confidence in relation to Ireland's ability to counteract and withstand cyber attacks will be key to protecting and strengthening Ireland's attractiveness as a location for further growth. As such, an ambitious approach is needed to build confidence in Ireland's ability to uphold cybersecurity.

Without sustained state intervention and support, Ireland's government, economy, and citizens face significant risks going forward. As Government's National Risk Assessment 2023 notes, "*Ireland is an attractive target in respect to cyber attacks*."[3] Intervention and support

[1] Consultation on the Draft Cyber Industrial Strategy, DECC: https://www.gov.ie/en/consultation/bc4f2-consultation-on-the-draft-cyber-industrial-strategy/.

[2] National Risk Assessment 2023: https://www.gov.ie/en/press-release/3da9e-tanaiste-publishes-results-of-national-risk-assessment-2023/

[3] Ibid.

to advance research and innovation in cybersecurity, fostering professional workforce development, and bolstering enterprise supports within the community will all be important to enhancing Ireland's cyber industry. The draft Cyber Industrial Strategy is therefore a positive step in the right direction.

Key to achieving a successful cyber industrial strategy will be the adequate resourcing of relevant bodies, such as the National Cyber Security Centre (NCSC), collaboration across industry, academia, and government, and an ambitious approach to the task at hand.

2. Do you think that (a) Skills, (b) Research and Innovation, and (c) Indigenous Industry represent the three key pillars of this Cyber Industrial Strategy? If not, what is missing?

AmCham regards the three pillars as laid out in the consultation document to be key in developing a cyber industrial strategy. Each of these pillars are of considerable importance in building a resilient cyber industry in Ireland.

AmCham would note that these pillars should not be approached in isolation, but rather the interconnectedness between each should be considered. In this regard, AmCham suggests that collaboration should be central to the focus and implementation of each of these three pillars. There is a need for greater collaboration across government departments, industry, both indigenous and MNC, and academia. Ongoing consultation is both welcome and essential, and the continued dialogue facilitated by the NCSC is beneficial. Enhanced multistakeholder engagement will be crucial to the successful implementation of this strategy.

Beyond the three pillars, AmCham would further stress the importance of focusing on, and maintaining, best practice. AmCham acknowledges the inclusion of several best practice case studies within the consultation document in this context. Important here will be the implementation of mechanisms to measure Ireland's progress in this area, and the formalisation of benchmarking Ireland against global best practice standards for cyber. Ireland must be able to adapt as expectations alter in future years.

3. Do you think Ireland should balance its interests in attracting foreign direct investment and an open trading economy at global level with the EU's preference for 'technological sovereignty' in cybersecurity? How can this balance be achieved?

The consultation document states that "*A more assertive approach to protecting our national interests at EU level may also be needed to protect our economic model.*"[4] AmCham supports this sentiment and would note that this is not a "*may*" but rather a "*must*". AmCham

[4] Consultation on the Draft Cyber Industrial Strategy, DECC: https://www.gov.ie/en/consultation/bc4f2-consultation-on-the-draft-cyber-industrial-strategy/.

appreciates the Department's acknowledgement of the importance of American MNCs to Ireland's economy, and that given the EU's focus on 'technical sovereignty "*incentives for multinational firms to continue to invest and retain existing operations and services in the State will need to be smart and nimble, taking account of the changing international environment*."[5] AmCham would encourage the exploration of how best this can be achieved, and dialogue with MNCs operating in Ireland will be key in navigating how best to maintain Ireland's competitiveness.

For Ireland's economy to continue to grow, it is crucial that any form of protectionist approach is avoided to the greatest extent possible. Ireland, and the EU, need to continue to be open to foreign direct investment and engagement with likeminded countries and partners such as the US.

AmCham has advocated for a continued focus on the deepening and strengthening of international relationships and collaborations on cybersecurity at governmental, agency and public body levels to leverage, and learn from the expertise and experiences of Ireland's partners. AmCham would therefore echo the Department's view that "*there is also a need for Ireland to strengthen relationships with likeminded international partners, recognising that some of the state of the art in cybersecurity technology and innovation lies beyond the EU's borders*."[6] Indeed, US companies are world leaders in cyber innovation. Ireland and the EU must recognise this and continue to facilitate the expansion of US MNCs in this sector. Conversations and partnerships with international players will be key if Ireland is to keep up to speed with global advancements in the space.

International information sharing in relation to cybersecurity is paramount. Cybersecurity challenges traverse borders, and companies and individuals work across national boundaries on a daily basis. Given the global connections which take place each day, it does not make sense to pursue cybersecurity in a vacuum, or in the absence of international engagement. As AmCham outlined in its paper 'The Strongest Link in the Chain: Ireland's Global Cybersecurity Leadership': "*Cybersecurity is a global, interdependent ecosystem which has no land or sea borders. This cybersecurity ecosystem is in itself a global supply chain and, as is widely known, a chain is only as good as its weakest link*."[7]

Pillar 1: Proposals in relation to Skills

[5] Ibid.

[6] Ibid.

[7] American Chamber of Commerce: The Strongest Link in the Chain: Ireland's Global Cyber Security Leadership: https://www.amcham.ie/media/z0ppgklh/amcham-ireland-the-strongest-link-in-the-chain-irelands-global-cyber-security-leadership.pdf

4. Do you think the key actions for skills development are ambitious enough to create a diverse workforce with all the necessary skills to meet the needs of the cyber industry? Please provide any additional comments about skills.

A recent report by Cyber Ireland found that 66% of organisations have skills, recruitment or retention issues. Further, in 2022 there were 6,707 unique job postings for cybersecurity professionals in Ireland, which marked a trebling in demand from 2019.[8] Developing a workforce with the relevant skills to fill these positions urgently needs to be a prioritised. The development of cyber skills is important for those working directly in the industry, but also for those working within organisations that could come under threat, or indeed for any citizen who could face a personal attack.

In this regard the proposals as laid out in the draft strategy are a positive step in the right direction. AmCham particularly acknowledges the strategy's commitment to "*forging partnerships between academia, industry, and government to create apprenticeships, internships, and hands-on learning experiences, facilitating the transition of talent into the cybersecurity workforce.*"[9] Given the number of companies and specialised professionals in this space that operate in Ireland, more must be done to tap into the expertise of industry. As the consultation notes, "*there are 489 firms offering cybersecurity products or services with 7,351 cybersecurity professionals employed in the Sector in the State.*"[10] This expertise could be leveraged to greater effect.

Further, there needs to be a greater connection between what is being taught on courses with the needs of industry. AmCham notes that the strategy acknowledges this in stating there "*is a misalignment between the training offered by educational institutions and the skills needed by the industry*."[11] Important here will be the inclusion of mechanisms to make it easier for industry to engage with skills training. As such, the provision of the adequate framework to facilitate industry involvement is essential. AmCham members are energised and keen to engage with educational institutions and Government in relation to cyber skills and look forward to greater collaboration on this point in the future.

AmCham further notes the need to embed cyber into education at an earlier age. It is therefore positive that the strategy includes the aim to invest *"in cybersecurity education at primary and secondary levels to provide a basic level of cyber hygiene to our digital natives while encouraging openness to exploring careers in cyber by our diverse student population."*[12] The earlier that cyber is embedded into the curriculum, the better. It is necessary that teachers

[8] Cyber Ireland Labour Market Report 2023: https://cyberireland.ie/wp-content/uploads/2023/09/Cyber-Labour-Market-Report-2023.pdf

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] Ibid.

and schools are provided with the adequate resources to ensure that the inclusion of cyber in the curriculum is meaningful and impactful.

AmCham suggests that key bodies are provided with the necessary training in place to adequately manage cybersecurity. For example, there needs to be training and equipping of Gardai and the judicial infrastructure to effectively detect and prosecute cybercrime.

AmCham would finally note that several organisations are active in skills training, but their activity isn't necessarily visible. This needs to change if Government is to have a comprehensive overview of what is working well and what needs to change going forward. Again, this comes back to the need for great collaboration and communication between various bodies. In general, there needs to be a greater degree of joined-up-thinking if Ireland is to fully leverage its potential in this space.

Pillar 2: Proposals in relation to Research and Innovation

5. Do you think there should be a dedicated 'bricks and mortar' facility for cybersecurity research, development, and innovation in the State along the lines suggested in this consultation paper? If so, please outline below.

AmCham agrees with the Department's view that "*collaborative innovation is missing from the Irish landscape.*"[13] There needs to be a more cohesive approach across the board when it comes to developing Ireland's cyber industry. The establishment of a 'brick and mortar' facility for cybersecurity research, development, and innovation can be viewed as a welcome initiative.

The opening of such a facility is one way in which to concretely appoint an overseer for research and innovation in this space. In many ways the creation of a dedicated building with "*teams of Principal Investigators at Post Doctorate level working collaboratively with industry and the NCSC*"[14] is one way to solidify the collaboration that is needed whilst centralising oversight.

However more information and a clearer vision is needed in order to fully understand what such a facility will look like and how it will operate. For example, issues such as the geographical location, as noted in the consultation document, will need to be resolved.

[13] Ibid.

[14] Ibid.

6. Do you think the key actions for research are ambitious enough to create a mature research community generating globally recognisable research? Please provide any additional comments about research and innovation.

Again, AmCham stresses that collaboration will be key in successfully implementing the action items of the strategy. In strengthening Ireland's position as a centre for research, it is essential that there is alignment between funding opportunities and the research priorities of business and academia.

In terms of research and innovation, AmCham would like to see a more focused and ambitious approach from the Department. There needs to be greater clarity on what Ireland's goal is within certain timeframes. As noted in AmCham's 2024 pre-budget submission, Ireland should aim to be number 1 in the EU for cyber research by 2050.[15] AmCham would like to see concrete short- and long-term goals from the Department to assist Ireland in reaching its full potential.

In terms of funding, AmCham suggests that the Department considers using a proportion of the National Training Fund surplus (which stands at €1.37 billion as of November 2023)[16] to fund the relevant cyber research and innovation programmes. The opportunity exists to utilise this surplus to advance research and training in cybersecurity, and as a result, to provide significant benefits to Ireland's business and investment ecosystem. There needs to be a more comprehensive multi-annual investment plan, providing the necessary financial backing to enhance Ireland's research infrastructure, facilitate collaboration between academia and industry, and stimulate the development of cutting-edge technologies. This will help to ensure that Ireland's research in cybersecurity has the sufficient funding to make a real impact.

There further needs to be a greater focus on the recruitment of leading global researchers and educators within Ireland's third level education framework. This will be essential if Ireland is to grow its cyber research base. There is a pressing need to bolster the attractiveness of doctoral programs, and further invest in the PhD model to make it a compelling choice for talented individuals.

AmCham would finally note that consideration must be given to how best to structure cyber research programmes, given the speed of at which technology is evolving and industry is advancing. Timeframes that are reflective of this pace of change will be important.

Pillar 3: Proposals in relation to Indigenous Industry

[15] AmCham 2024 Pre Budget Submission: https://www.amcham.ie/media/eftf1rfr/1896-pre-budget-submission-report-fa-digital.pdf

[16] Committee of Public Accounts: https://www.oireachtas.ie/ga/debates/debate/committee_of_public_accounts/2023-11-23/6/

7. Do you think the key actions for industry are ambitious enough to create a vibrant and thriving indigenous industrial sector? Please provide additional comments about indigenous industry.

The success of MNCs can have a directly positive impact on indigenous industry and the entire cyber ecosystem, as is demonstrated by the Estonia case study in the consultation document.

In terms of building Ireland's indigenous cyber industry, the question of priorities is again key. Ireland needs to approach this pillar with a concentrated focus in mind. AmCham therefore believes the Department's commitment "*to making targeted strategic investments to build partnerships*" is important. [17]

As is the case in other sectors, EU regulation in this space (NIS2 transposition/DORA/Cyber Resilience Act) will place a significant burden on SMEs, as many are positioned in the downstream supply chain of larger companies. It is important that Government provides indigenous companies with the relevant tools to be able to manage EU regulation coming down the line. AmCham suggests that this is more strongly incorporated into the strategy in relation to indigenous industry and beyond. The earlier companies can begin to plan for their compliance, the more efficient and cost-effective it will be for them. Many companies, particularly SMEs, lack awareness of what laws are coming down the line and when. AmCham suggests that there is a focus on raising awareness via campaigns and direct engagement with companies of all sizes but particularly within indigenous SMEs. AmCham supports the work that the NCSC has done with its quick reference guide for NIS2 and suggests that similar is carried out for other cyber regulations.

Closing Questions

8. Do you think there is anything missing from this draft strategy? Note that resilience matters, like vulnerability management, supply chain security, cyber hygiene, & awareness raising will be handled through a new National Cyber Security Strategy.

AmCham would stress the importance of clear communication from the Department on its works in this space going forward.

For example, greater consolidation of approach would be beneficial. The use of various documents and strategies risks causing confusion. Continued updates on the progress of the strategy will also be key in keeping industry informed.

[17] Consultation on the Draft Cyber Industrial Strategy, DECC: https://www.gov.ie/en/consultation/bc4f2-consultation-on-the-draft-cyber-industrial-strategy/.

9. How effective do you believe this strategy will be? Please explain why you believe this strategy will be effective or ineffective.

The success of this strategy will depend on how it is implemented, particularly with regard to funding mechanisms, of the oversight of coordination, and the communications strategy that accompanies the strategy's rollout.

Further, greater unification of responsibility for cybersecurity would be beneficial in delivering a joined-up approach between innovation and cyber response and protection. For example, AmCham notes that cyber falls under the remit of the Department of Environment, Climate, and Communications, whereas digital is taken care of by the Department of Enterprise, Trade, and Employment. AmCham would stress the importance of collaboration with all relevant governmental actors when it comes to the further development of this Cyber Industrial Strategy.

10. What more do you think Government could do to help stimulate investment in cyber?

Government needs to take a whole of society approach to cyber. The importance of ensuring Ireland has a resilient cyber industry cannot be overstated. Given the importance of cyber at present, and into the future, it is necessary that the appropriate funding is ringfenced to provide for the delivery of the strategy on a multiannual basis.