www.amcham.ie @americanchamber

AMERICAN CHAMBER of COMMERCE IRELAND

National Cyber Security Strategy 2019-2024 Mid-Term Review

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

February 2023

The American Chamber of Commerce Ireland

The Voice of US-Ireland Business

The American Chamber of Commerce Ireland (AmCham) is the collective voice of US companies in Ireland and the leading international business organisation supporting the Transatlantic business relationship. Our members are the Irish operations of all the major US companies in every sector present here, Irish companies with operations in the United States and organisations with close linkages to US-Ireland trade and investment.

National Cyber Security Strategy Review

AmCham welcomes the opportunity to respond to the Department of the Environment, Climate and Communications' consultation on the National Cyber Security Strategy Review.

Cyber security is a necessity in an increasingly digitalised world. With changing geopolitical circumstances, it is essential that Ireland is vigilant against cyber attacks. In doing so, Ireland must ensure it is prepared to deter and withstand any potential attack. The reputational risk of cyber attacks could have a severe and costly impact on organisations, and on Ireland's reputation as an investment location. Many of the world's largest companies have operations, and regional headquarters in Ireland. These companies require world-class protection and regulation. Many have global teams, serving global markets, and these markets also require such security.

AmCham acknowledges the publication of the NIS 2 Directive in December 2022 and its entry into force in January 2023. NIS 2 will build on and repeal NIS 1, and crucially addresses deficiencies in the current legal framework. NIS 2 expands the coverage of the current legal framework and clarifies minimum mandatory cyber security measures applicable across the EU, whilst additionally streamlining incident reporting requirements. NIS 2 also bolsters the functions of national cyber security authorities with respect to regulatory oversight, enforcement action, and sanctions. AmCham views the implementation of NIS 2 as an opportunity for Government to firmly and clearly communicate the importance of cyber security to a range of sectors, given the number of industries which will fall under its remit. AmCham looks forward to Ireland's adoption of NIS 2 and its application of those measures in advance of the deadline on 18 October 2024.

AmCham further stresses the importance of responding to criminal actors in the cyber security space. AmCham therefore welcomes the e-Evidence regime and the Second Protocol under the Budapest Convention as mechanisms of enabling the cross-border requests for evidence relating to law enforcement investigations in this space. AmCham looks forward to the transposition of these regimes at the earliest opportunity.

Vision

The National Cyber Security Strategy's vision: "*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*" is still very much relevant today. AmCham suggests that "economy" should be included alongside "society" to emphasise the importance of cyber security to continued economic growth on the island.

As outlined in AmCham's position paper '*The Strongest Link in the Chain: Ireland's Global Cyber Security Leadership': "While on the one hand the digital economy brings great empowerment for citizens and companies, on the other hand there is a heightened vulnerability to attacks which could lead to a range of potential impacts."*[1]

Cyber security is an ever-present concern across all sectors and is not limited by the size of an organisation. Given the reputational and financial costs which could result from a cyber attack, the economic importance of cyber security must be recognised.

AmCham supports the inclusion of Ireland playing a "*full part in shaping the future of the internet*" but believes that this statement could be made stronger. Ireland can and should become a global leader in cyber security, given the number of MNCs which have their European headquarters situated here. Ireland has been chosen as the base for EU HQs or significant operations by 9 of the top ten US technology companies, 9 of the top 10 pharmaceutical companies, the top 5 global software companies, 14 of the top 15 medical technology companies, 8 of the top 10 industrial automation companies, and 20 of the top 25 global financial services companies. These leading companies need the assurance that Ireland will be able to provide them with top of class cyber security going forward. In this regard it would be beneficial to go further in the vision and include the ambition to "*become a global leader in cyber security* " along with a quantifiable understanding of what a leader in the space looks like, and how to measure progress.

Ireland has become a leading digital economy within the EU. In order to sustain and grow this position, Ireland must be focused on ensuring it has a best-in-class ecosystem for privacy and security, and that the protection of Ireland's position as an EU regulatory hub for digital businesses in Ireland is a priority at EU level. The actions set out to realise the vision of the strategy – to protect the State, develop capacity, and engage nationally and internationally in a strategic manner are essential. Protecting critical national infrastructure is pivotal to ensuring business and people in Ireland are secure from cyber threats. Developing capacity to understand and manage challenges is vital in an environment where threats are ever evolving and where the State must be successful every time a threat emerges while malicious actors need only be successful once.

National and international engagement is important in informing Ireland's actions in this regard. AmCham has advocated for a continued focus on the deepening and strengthening of international relationships and collaborations on cyber security at governmental, agency and public body levels to leverage, and learn from the expertise and experiences of Ireland's partners.

[1] American Chamber of Commerce: 'The Strongest Link in the Chain: Ireland's Global Cyber Security Leadership'

Objectives

AmCham considers all the objectives stated as remaining relevant today. However, Ireland should be more ambitious in its objectives. For example, a potential additional aim could be to "strengthen Ireland's reputation as a destination for cyber security excellence". Ireland needs take cyber security seriously to avoid criticism from its European neighbours. As cyber security becomes increasingly important, more and more companies will consider Ireland's reputation in this field to be a deciding factor in locating investment here. Therefore, Ireland's reputation must be enhanced in this regard in order to ensure Ireland remains an attractive destination for FDI.

AmCham believes the focus on response to cyber security incidents in the list of objectives is particularly important. Whilst mitigation is essential, attacks cannot always be prevented and so the management of the disruption caused by a cyber attack must be a priority. The key to minimising damage from cyber attacks is to focus on cyber resiliency. A resiliency strategy is one that balances active detection and prevention of attacks with being prepared for a breach and able to recover operations quickly after an attack. This can involve a wide range of activities, such as conducting risk assessments, implementing security controls, developing incident response plans, and training for enterprise recovery. For example, in order to successfully recover critical data and systems after a cyber incident, unaffected copies of applications and data sets must be available. The challenge becomes how an organisation ensures that clean data and unaffected applications exist.

In order to achieve the objective to "*continue to improve the ability of the State to respond to and manage cyber security incidents, including those with a national security component*" emphasis must be placed on having a resiliency strategy in place. AmCham believes the objective to "*identify and protect critical national infrastructure by increasing its resilience to cyber attack and by ensuring that operators of essential services have appropriate incident response plans in place to reduce and manage any disruption to services*" is vital and suggests that resiliency is further incorporated into the awareness strategy as it is crucial that businesses and individuals are made aware of its importance.

Evolving Global Cyber Risk & Policy Developments

As is recognised within the consultation, the cyber threat level has increased considerably in recent years. The rapid transition to remote working as a result of the COVID-19 pandemic, the attack surface for cyber threats significantly increased. In conjunction with this, cyber threats themselves continue to evolve and Ireland must

be focused on staying ahead of this evolution. Cyber security is not only a perquisite for the digital transformation, but as we look to greater innovation to tackle societal and economic challenges, it will be essential to support actions across all sectors, and to ensure the resilience of infrastructure and networks.

In ensuring cyber security, an organisation, regardless of size must now be cognisant of its supply chain and the identified increased prevalence of supply chain attacks, as outlined in the consultation. While the benefits many organisations have gained by outsourcing digital services and security services is identified, the strategy must also acknowledge the risk posed by supply chains where other services are outsourced. For many companies, the cyber security of providers in their value chain is essential in adequately protecting their operations. Actors within the supply need certainty in relation to the standards they will be held to. There is a need for higher auditable standards for actors within supply chains.

In terms of policy developments, the publication of the new National Digital Strategy to drive the digital transition was positive. Focus must now firmly be on turning the ambition of the National Digital Strategy into reality.

AmCham notes the Government's commitment to expand the headcount in the NCSC to 70 by the end of 2024. AmCham strongly recommends that this commitment is kept under constant review to keep pace with Ireland's cyber security needs, particularly in the context of our strategic importance as a hub in the transatlantic digital economy. Further, there needs to be a continuous assessment into the critical skills in the makeup of these roles, to ensure that expansion is happening in a productive way.

In several of its recent submissions to Government, AmCham has stressed the importance of continuing to increase investment and resourcing for the National Cyber Security Centre (NCSC). It is crucial that the NCSC has the sufficient resources to carry out its functions to the best possible standard.

National Capacity Development

As outlined above, AmCham believes the resourcing of the NCSC must be kept under constant review to ensure the NCSC can address challenges arising as threats evolve.

AmCham welcomes the NCSC's plan to implement a graduate internship programme in 2023. As part of this, the NCSC should broaden its approach to staffing to include recent graduates with degrees in disciplines outside of computing and applicants with backgrounds in other sectors.

AmCham notes that these candidates bring different and valuable skillsets which are essential as cyber security is not just a technical endeavour: it is people-centred work

that involves understanding human behaviour. For instance, professionals and recent graduates with backgrounds in psychology, business, and geopolitics can be especially useful for understanding the motivation behind cyber attacks since these attacks are often motivated by a variety of factors. If an incident is detected at the outset, these professionals can play a crucial role in deducing the motivation of the actors responsible and in preventing them from achieving their goals.

AmCham member companies have voiced a willingness and enthusiasm to support national capacity development in a meaningful way. AmCham welcomes the drafting of legislation for the NCSC and looks forward to the completion of the related policy paper currently being drafted by the Department in relation to the NCSC.

Critical National Infrastructure Protection

AmCham is of the view that investment in ensuring vital national infrastructure, including the energy grid, is protected from potential cyber threats is of the utmost importance.

In terms of the proposals for further measures outlined, the offering by the NCSC of a vulnerability assessment service to critical infrastructure and government entities in 2023 is important. Following this, action must be prioritised to address any identified weaknesses. Further, such assessments must take account of evolving threats on the part of malicious actors and ensure the required actions can be taken into the future to enhance the security of vital infrastructure. NIS 2 provides a vehicle through which the protection of critical national infrastructure can be enhanced. Regular vulnerability assessments to secure against potential threats are essential. It is vital that stress tests are conducted on all bodies responsible for the operation of critical infrastructure, to ensure the necessary security is in place. Further, on-going mapping of potential threat scenarios is essential in ensuring the security of vital infrastructure keeps pace with the changing threat landscape.

AmCham notes the aim for sectoral regulators to integrate cyber security compliance into their existing regulatory roles. Clarity in relation to regulators will be key, there is a risk that Ireland could end up with multiple regulators without the specific expertise needed to carry out the job effectively. As such, AmCham is of the view that the resourcing of cyber security within key public and regulatory bodies must be prioritised to ensure sectoral regulators are supported with the expertise and staffing levels required to effectively execute cyber security functions.

Skills

It is crucial that individuals with the relevant skillset are employed by the bodies responsible for cyber security.

AmCham welcomes the proposals put forward by the strategy to ensure that the necessary educational and training outlets are available. The more Ireland positions itself as a key hub and learning centre for cyber security, the more we will benefit.

Having a robust team from a variety of backgrounds within the NCSC would be supportive of the development of a comprehensive approach to cyber security – for instance, with expertise in incident response, diplomacy and law enforcement. Additionally, AmCham recommends that further resourcing for the NCSC takes account of the need for expertise in backgrounds including psychology, geopolitics, and behavioural sciences.

Cyber personnel are in demand and the field has a labour shortage. It is vital that resourcing for the NCSC prepares the body for resiliency in the face of attrition. AmCham notes the plan to increase the NCSC's headcount to 70 personnel, however, it must be considered as to whether 70 employees will be sufficient to cover key roles should attrition occur.

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

Further, Government should look to best practice models in terms of skills development. For example, the UK's Cyber Security Council has a focus on qualifications and cyber skills. Through the identification of 16 different specialisms, the Council is examining the skills and qualifications which are most applicable to each specialism, which will allow for the development of a qualification framework for those focused on a career in cyber. The UK's Cyber Security Council has provided, on its website, information on each specialism including an introduction to each specialism, information on the typical responsibilities and tasks, the skills and knowledge required, and information on useful prior experience for those hoping to enter the specialism from outside cyber security. This material is presented in an accessible and coherent manner. The development of a similar resource would be highly beneficial in communicating the possible career trajectories with cyber security in Ireland.

Enterprise Development

The focus on supporting collaboration between industry, academia and Government in relation to cyber security is important both in strengthening Ireland's resilience in this area and supporting the development of Ireland's ecosystem to support innovation in the cyber sector. Ireland should look to the likes of Scotland, which has a formalised industry advisory board. Such an approach will provide greater opportunities to leverage the expertise of industry in Ireland to best enhance cyber security in Ireland - 6 of the top 10 cyber security software companies are located in Ireland.[2]

The presence of cyber security powerhouses in Ireland can encourage more companies from the sector to consider Ireland as an investment location and also support indigenous innovation through the opportunities which exist for Irish companies to collaborate and partner with global companies on cyber security projects.

Further, cooperation between Government, industry, and academia is needed to prepare for upcoming EU cyber security regulations, namely the NIS2 Directive and the Digital Operational Resilience Act (DORA). AmCham looks forward to engaging with Government on the future transposition of both legislative initiatives and urges Government to consult early and regularly with relevant stakeholders towards an efficient and consistent application of the NIS2 and DORA.

Engagement

International information sharing in relation to cyber security is paramount. Cyber security 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 cyber security in a vacuum, or in the absence of international engagement.

AmCham has advocated for a continued focus on deepening and strengthening international relationships with regard to cyber at governmental, agency and public body levels. The focus on international engagement, and the NCSC formalising its engagement with relevant bodies in states with which Ireland has a close standing relationship is welcome.

As AmCham outlined in its paper 'The Strongest Link in the Chain: Ireland's Global Cyber Security Leadership':

[2] Why Ireland For Cyber Security | IDA Ireland | IDA Ireland

> *"Cyber security is a global, interdependent ecosystem which has no land or sea borders. This cyber security ecosystem is in itself a global supply chain and, as is widely known, a chain is only as good as its weakest link."*[3]

Through continued engagement, Ireland can leverage the experiences of international partners to enhance its cyber security and resilience. Ireland can learn from the success and mistakes of others who have cyber security centres. By continuing to deepen international engagement at governmental, agency and public body levels, Ireland can ensure its approach to cyber security is informed by best-practice.

Further, a focus domestically in public-private dialogue, and information sharing with experts in industry will work to enhance Ireland's cyber security protections, counteract potential threats, and support Ireland's reputation as a location for investment and business.

Finally, AmCham acknowledges and supports Government's concerns in relation to the potential inclusion of digital sovereignty provisions in the draft EU Cyber Security Certification Scheme for Cloud Services (EUCS). Such measures would impact cloud service providers operating in Ireland and across Europe. Their introduction would limit the choice to buy cloud services, increasing costs and reducing the quality of offer.

Citizens

A continued focus on building public awareness of cyber threats is essential. The provision of information on how individuals can better protect themselves from cyber threats and increase their cyber security awareness is essential. As the workplace has become ever more digitalised and as key services citizens access have transitioned to being digital services, the potential attack surface through which citizens engagement can come under attack has increased. As such, enhancing citizens' knowledge of how best they can use digital and online environments safely is perhaps now more important than ever before.

Governance Framework and Responsibilities

The constant reshaping of Government portfolios has had significant, and very positive impacts, ensuring the Cabinet reflects matters of importance to our economy and society. AmCham notes the creation of the Department of Further and Higher Education, Research, Innovation and Science, and how this Department has been

[3] American Chamber of Commerce: The Strongest Link in the Chain: Ireland's Global Cyber Security Leadership

beneficial in fostering stronger links between tertiary education, industry, and the innovation ecosystem. AmCham has recommended that future reshaping of government portfolios should reflect the importance of cyber, data and digital to the Irish economy.