The **Strongest Link** in the Chain:

Ireland's Global Cyber Security Leadership

An American Chamber of Commerce Ireland Position Paper

@americanchamber

AMERICAN CHAMBER *of* COMMERCE IRELAND

CONTENTS

ABOUT THE AMERICAN CHAMBER

The American Chamber of Commerce Ireland is the leadership voice of US business in Ireland. Our mission is to strengthen the US-Ireland-EU business community through advocacy and networking with purpose. American Chamber membership includes US companies operating from Ireland, Irish companies expanding in the US and organisations with strong bilateral links between Ireland and the US.

EXECUTIVE SUMMARY

As a key priority for every sector with the capability of impacting every business size, the American Chamber strongly advocates for Ireland to position itself as a global cyber security leader: *the strongest link in the chain.*

Fast-paced geo-political developments and society's continual reliance on technology in a connected world demonstrate that now is a critical time for promoting and building Ireland's cyber security leadership.

In this position paper, the American Chamber recommends adopting a policy approach to cyber security that is **risk-based; outcome focused; respectful of civil liberties; internationally relevant; adopts international best-practice and embeds security-by-design.** Through consultations with member companies across a range of sectors, the American Chamber has identified **key priorities** to position Ireland's leadership in cyber security, in the context of the next National Cyber Security Strategy. The American Chamber advocates that, by 2020, strides need to be made under each of these specific policy areas:

A

Adequate resourcing and funding of public sector bodies which have a national cyber security mandate and a consistent cross-government approach to information security.

B

Meaningful regulatory measures which have received input from relevant stakeholders.

C

An ongoing and successful public-private dialogue.

D

A plan to address demand for talent; greater collaboration with research bodies and increased public awareness.

'International collaboration is essential. Security within national boundaries doesn't make sense. Everything is globally connected'.[1] 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. Advocacy for Ireland's position as ***the strongest link in the chain*** seeks to leverage Ireland's proven track record as a digital leader and apply these credentials to the global cyber security stage in order for all organisations and citizens to operate in a robust cyber security environment.

1 https://link.springer.com/chapter/10.1057/9781137400529_3

CONTEXT

WHY IRELAND

Ireland continues to punch above its weight when it comes to attracting investment from some of the world's largest and most innovative companies, with US firms accounting for the largest source of new investment. Collectively, US investment in Ireland amounts to $419bn.[2]

As set out in the American Chamber's US-Ireland Business Report 2018[3], there are many factors that draw foreign direct investment to Ireland:

- **Ireland's pro-trade and investment policies** are a key factor in Ireland's attractiveness. Ireland is one the most successful countries in the world at encouraging the development of high-value-added industry clusters.
- **Ireland has been a growth leader** in Europe since the post-crisis era, a position it will maintain in 2018- 2019.
- **Ireland's talent** remains a key attraction. According to the OECD, Ireland has one of the most educated workforces in the world, with 52% of workers between the age of 25-34 having a third level education qualification, 10% higher than the OECD average. Ireland ranks in the top ten globally for the quality of its education system and knowledge transfer between universities and companies.
- **Ireland's membership of the European Union,** the wealthiest and largest economic bloc in the world is attractive for global companies.

2 https://www.amcham.ie/news/us-ireland-business-2018-(1).aspx
3 https://www.amcham.ie/news/us-ireland-business-2018-(1).aspx

WHY IRELAND FOR CYBER

Not only does Ireland have a stellar reputation for attracting Foreign Direct Investment (FDI), it is also home to a growing cyber security cluster comprised of global and indigenous Irish companies. Overall, Ireland has the largest proportion of the Information and Communication sector in its economy compared to all other countries in Europe.[4] Through the hard work of the Government's investment and enterprise agencies, Ireland is building on that reputation to grow its cyber security industry.

There are a number of key features which attracts cyber security companies or companies with a strong cyber security mandate:

- **Ireland has garnered a reputation as a home for global cyber security powerhouses.** The top 5 worldwide security software companies are located in Ireland.[5] This continues to attract more companies from within the cyber security sector. It has also encouraged indigenous Irish companies to establish, collaborate and partner with global companies, in locations such as Cork and Galway.
- **Ireland's reputation as a digital leader[6] is a significant factor for attracting companies in the cyber security sector.** Ireland is an active member of the Digital 9 (D9) group of digital frontrunner countries within the European Union, championing issues such as the free flow of data initiative; consistent elevation through the EU Digital Economy and Society Index (DESI)[7] – currently ranking sixth in Europe; and home to a robust and well respected Data Protection Commission – which has an enhanced role given Ireland's position as a European home to many global data-centric organisations and the implementation of the General Data Protection Regulation (GDPR).
- **Ireland's ranking in the top 10 most innovative countries in the world[8] sets it apart** from competitors as a location of choice for global companies. As a result, Ireland is home to companies from a wide range of sectors that are at the cutting edge of technological and scientific advancements.

Gartner forecasts worldwide enterprise security spending to total $124bn in 2019, which will see 8.7% growth in the market.[9] Organisations are said to be spending more on security as a result of regulations (such GDPR in Europe); shifting buyer mindset; awareness of emerging threats; and the evolution to an e-commerce strategy. There is huge growth potential, therefore, for companies selling products and services which protect the cyber security of individual and private sector users.

Worldwide enterprise security spending to total $124bn in 2019.

Irrespective of the business sector, however, cyber security is a real and ever-present reality for all organisations of all sizes – from large global companies to SMEs (small and medium enterprises). Cyber security impacts far beyond 'tech' companies. From healthcare to retail, every industry faces cyber security threats.[10] Indeed, the extent to which a country invests and prioritises cyber security can determine many critical FDI decisions.

Irrespective of the business sector, however, cyber security is a real and ever-present reality for all organisations of all sizes.

Positive steps have been taken in Ireland in recent years to safeguard organisations and the public from cyber attacks. Ireland's **National Cyber Security Centre (NCSC),** established in 2011, has operational responsibility for cyber security, which sits in the Department of Communications, Climate Action and Environment (DCCAE). The publication of **Ireland's first National Cyber Security Strategy 2015-2017 set the scene in terms of the Government's approach to cyber security.**

4 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
5 https://www.idaireland.com/how-we-help/resources/infographics/ida-cyber-security
6 https://ec.europa.eu/digital-single-market/en/desi
7 https://ec.europa.eu/digital-single-market/en/desi
8 https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2018.pdf
9 https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019
10 https://www.globalsign.com/en/blog/top-industries-preparing-for-evolving-cybersecurity-threats/

A top priority for Government has been the implementation of the **Network and Information Security (NIS) Directive** which came into effect on 10 May 2018. As the first EU-wide legislation on cyber security, its aim is to strengthen the overall level of cyber security and harmonise the variances in related legislation across member states. In order to achieve this, NIS imposes security measures and incident reporting obligations for Operators of Essential Services (OES) and Digital Service Providers (DSP). The Directive also requires member states to designate national points of contact in the event of cyber crises, and to publish national cyber security strategies.

Another legislative development for Ireland is the upcoming **EU Cyber Security Act.**[11] The aim of this Act is to increase the cyber security of the European digital economy by empowering the European Union Agency for Network and Information Security (ENISA) and creating an EU cyber security certification framework.

DIGITAL ECONOMY

The **Digital Single Market** 'is the strategy of the European Commission to ensure access to online activities for individuals and companies under conditions of fair competition, consumer and data protection, removing geo-blocking and copyright issues'. [12]

Ireland has become a leading digital economy within the EU.[13] Sustaining Ireland's digital leadership requires a best in class ecosystem designed to protect the privacy and security of digital users. This is especially relevant as the world faces new challenges associated with the rapid expansion of digital services and an increasing dependency on technology by consumers, enterprises and governments. Indeed, Ireland's participation in the development of the EU's Digital Single Market is integral to the success of Ireland's digital economy. The digital economy is an increasingly important driver of economic growth globally as ICT related technological developments transform and disrupt business models.

Sustaining Ireland's digital leadership requires a best in class ecosystem designed to protect the privacy and security of digital users.

The presence of Internet of Things (IoT) objects and the emergence of innovative technologies such as artificial intelligence (AI) and machine learning (ML) has connected humans with technology and increased the efficiency of industrial operations. In order to make this digitised ecosystem thrive, **it is fundamental to make privacy, security and trust a priority.** Confidence in the digitised networks on which we all depend is integral to the success of the Digital Single Market. Disruption to services, as a consequence of a cyber attack, undermines the confidence in a connected economy. This has the potential to harm the aims of the digital single market, which could in turn result in further economic impacts with users ceasing to conduct business online.

As already highlighted, Ireland has done exceptionally well at attracting significant global companies. As this is especially true when it comes to the ICT industry (Ireland is home to 8 of the top 10 global software companies and 4 of the top 5 IT Services Companies[14]) there is potential to leverage the significant expertise in the private sector to elevate and lead the cyber security agenda in Ireland.

11 https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-eu-cybersecurity-agency-and-cybersecurity-act
12 https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market
13 https://ec.europa.eu/digital-single-market/en/desi
14 https://www.idaireland.com/doing-business-here/industry-sectors/ict

THREATS AND RISKS

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. As mentioned previously, it is crucial to recognise that cyber security risks are not just a concern of 'tech' companies or indeed simply large companies, **cyber security is an ever-present issue across all sectors and knows no bounds in terms of organisation size.** As will be discussed in this section, cyber attacks can have serious implications for an organisation resulting in financial and reputational loss.

The growing prominence of cyber threats is highlighted in the Global Economic Forum's Global Risks Report 2018, with **large-scale cyber attacks now ranked third among a range of risks in terms of likelihood.**[15] In the same research, rising cyber-dependency is ranked as the second most significant driver shaping the global risks landscape over the next 10 years.[16]

In Ireland, the Government's 2018's National Risk Assessment deems cyber threats as posing a serious strategic risk to the country.[17] Well-documented examples of recent global attacks include WannaCry and NotPetya, which caused quarterly losses of $300 million for a number of companies[18], have contributed to a more open public conversation about the security on which companies, public services and daily lives depend.

The main trends in the 2018 cyberthreat landscape, as identified by the European Union Agency for Network and Information Security (ENISA)[19] showcase a range of hot-button issues, including:

- Increased complexity of attacks and sophistication of malicious actions;
- Impact of state-sponsored agents;
- Emergence of IoT environments;
- Lack of a pipeline of relevant skills necessary to defend against increasingly sophisticated cyber attacks.

Cyber breaches recorded by companies have almost doubled in five years, from 68 per company in 2012 to 130 per company in 2017[20] and the financial impact of such breaches is rising. Some of the largest costs in 2017 related to ransomware attacks, which accounted for 64% of all malicious emails. The annual cost of responding to cyber attacks is reported at £11.7mn per company, a year-on-year increase of 27.4%.[21] The cost of cybercrime to companies over the next five years is expected to reach US $8tn.[22]

Cost of cybercrime to companies over the next five years is expected to reach US$8 trillion.

Well-publicised cyber attacks, mentioned previously, have raised fears that attackers could significantly disrupt the systems that keep societies functioning. Many of these attacks are thought to be state sponsored.[23] Cybercriminals also have an exponentially increasing number of potential targets. This is highlighted in Gartner's research that the use of conected "things" is expected to expand from an estimated 8.4 bn devices in 2017 to a projected 20.4 bn in 2020.[24] As IoT devices begin to bridge the digital and physical worlds, the security challenge increases. Interconnected IoT devices already control physical infrastructure, such as production lines, supply chains and utilities, as well as airplanes and cars, resulting in potentially life-threatening impacts as a result of cyber threats.[25]

15 https://www3.weforum.org/docs/WEF_GRR18_Report.pdf
16 https://www3.weforum.org/docs/WEF_GRR18_Report.pdf
17 https://www.taoiseach.gov.ie/eng/publications/publications_2018/national_risk_assessment_2018_-_overview_of_strategic_risks_-_final.pdf
18 https://www3.weforum.org/docs/WEF_GRR18_Report.pdf
19 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
20 https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
21 https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
22 https://www3.weforum.org/docs/WEF_GRR18_Report.pdf
23 https://www3.weforum.org/docs/WEF_GRR18_Report.pdf
24 https://www.gartner.com/newsroom/id/3598917
25 https://parisinnovationreview.com/articles-en/sandy-verma-has-iot-increased-our-exposure-to-cyber-threats

As the terminology implies, Critical Information Infrastructures (CIIs), are vital to the functioning of societies.[26] CIIs include telecommunications and data networks, financial systems and process control systems. These infrastructures are connected to every part of the world through the internet and other networks. Therefore, there is a dependency on each other's security, as the weakest link can cause vulnerabilities for the other infrastructures. **Any potential unavailability of CIIs would have a debilitating effect on the security, economy and health of society as a whole.** Cyber-physical systems' integration is resulting in an increased likelihood of cyber attacks, leading to "a new chapter in information security; one that can be called Security of Things".[27]

Of course, another real risk is the **targeting of the public sector and the subsequent impact on provision of state services** (as was evidenced during the WannaCry attack) and loss of data. Given that a number of key government departments hold a substantial quantity of citizens' personal data in order to provide essential public services, the theft or compromising of such data is a significant risk and threat to the State. Ensuring confidence and trust in the public sector bodies that collect and process critical data is key, otherwise the process of digitisation within the public sector could be compromised.

Substantial risks also emerge from a lack of awareness in the workplace and in society. It is crucial that employees and internet users are equipped with the right knowledge and basic skills to protect themselves online. A lack of basic cyber skills is a key risk. Data shows that **approximately 90% of all cyber claims are the result of some type of human error or behaviour.**[28]

A stark risk facing the global cyber security community is the number of unfilled cyber security roles and therefore a shortage of skilled talent in both the public and private sector. **In the US alone, there are 350,000 open cyber security positions**[29] and a predicted global shortfall of 3.5 million cyber security jobs by 2021.[30]

A predicted global shortfall of 3.5 million cyber security jobs by 2021.

75% of all companies which suffer a cyber attack also incurred reputational damage or loss.

In all of the above cases, maintaining the integrity of an organisation's reputation, whether it be in the public or private sector, is key. The reputational risk of a cyber attack could have a severe and costly impact on the organisation. Data shows that 75% of all companies which suffer a cyber attack also incurred reputational damage or loss.[31]

26 https://www.thegfce.com/initiatives/c/critical-information-infrastructure-protection-initiative
27 https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis/
28 https://www.willistowerswatson.com/en/press/2017/03/when-it-comes-to-cyber-risk-businesses-are-missing-the-human-touch
29 https://www.cyberseek.org/heatmap.html
30 https://www.herjavecgroup.com/wp-content/uploads/2017/06/Jobs_info.pdf
31 https://www.agcs.allianz.com/insights/expert-risk-articles/arb-2018-major-risks-in-focus-cyber-incidents/

PRIORITIES

Through consultations with member companies across a range of sectors, the American Chamber has identified key priorities to position Ireland's leadership in cyber security.

ADOPTING FOUNDATIONAL POLICY PRINCIPLES

The American Chamber advocates for the adoption of the following foundational principles to underscore the key cyber security policies:

- **Risk-based:** A risk-based approach should be incorporated into processes and projects from the start; whereby risks, threats, vulnerabilities, and consequences are identified, then managed through mitigations, controls and similar measures. Not all applications and systems pose the same level of cyber security threats to the economy. Finding a balance between harnessing innovation in the development of products and services and ensuring the ongoing security of the tech ecosystem is crucial.
- **Security-by-design:** Security needs to be integrated in the overall process and cannot be a mere afterthought, gatekeeper or bolt-on at the end. Organisations across all sectors must therefore integrate security throughout their development processes to significantly reduce the security risks and long-term costs of development. A security-by-design approach should be cultivated throughout the organisation.
- **Outcome-focused:** There should be a clear focus on the desired end state, rather than adopting a prescriptive approach to implementation.
- **Respect for privacy and civil liberties:** As with all policy initiatives, a respectful approach to protecting the privacy and civil liberties of individuals needs to be adopted by adherence to the relevant legislative frameworks and practices.
- **Internationally relevant:** International standards should be integrated to the maximum extent possible, always keeping the goal of harmonisation to the fore.
- **Learning from best-practice:** Keeping a close watch on other like-minded countries; learning from those countries and adopting their successful cyber security policies is prudent, similar to many other policy initiatives. Sweden and Finland are Ireland's fellow members of the D9 group and therefore 'like-minded' digital leaders.[32] Keeping a watching brief on their cyber security practices is therefore prudent, given their cyber security leadership.

A | BUILDING PUBLIC SECTOR CAPABILITIES

Confidence in the abilities of Ireland's public sector entities to detect and respond to threats and attacks is integral to building citizens' trust in the systems on which the public sector operates. Given the widely publicised global attacks which have taken place in recent years, it is crucial that these entities operate and function effectively for Irish citizens and companies. To facilitate this sense of trust and ensure greater understanding of how the public sector approaches cyber security, the ***American Chamber advocates for the publication and dissemination of a stakeholder chart which outlines the roles and responsibilities of the various government departments, public agencies and bodies,*** similar to the US Federal Cyber Security Operations Team document.[33]

Confidence in the abilities of Ireland's public sector entities to detect and respond to threats and attacks is integral to building citizens' trust in the systems on which the public sector operates.

The American Chamber greatly welcomes the work which has been undertaken by the **National Cyber Security Centre** in its early inception years, especially with regard to implementation of

32 https://ec.europa.eu/digital-single-market/en/desi
33 https://www.dhs.gov/sites/default/files/publications/csd-ttp-finance-two.pdf

the NIS Directive. While the Department of Communications, Climate Action and Environment does not release specific details in relation to the staff or precise funding allocated to the NCSC for operational security reasons, the American Chamber acknowledges that additional funding was granted to the NCSC in 2018. The American Chamber also welcomes the NCSC's current recruitment programme. The American Chamber considers it absolutely necessary that ***the NCSC receives significant support to ensure it is staffed by skilled and experienced staff and to enable it to increase public cyber security awareness.*** This is in line with the American Chamber's long-held position regarding the capabilities and reputation of competent authorities in Ireland. The NCSC has a crucial role and its significance needs to be further acknowledged and endorsed by Government.

The American Chamber welcomes the establishment of the **Garda National Cyber Crime Bureau (GNCCB)** in 2017, stemming from the Garda Cyber Crime Investigation Unit, and the establishment of regional units throughout the country. The American Chamber recognises the important role of this Bureau and the Defence Forces' Communications and Information Services (CIS) in relation to Ireland's defence against cybercrime. Resourcing of teams and retention of talent is a challenge for An Garda Síochána and the Defence Forces, similar to private sector experiences in this regard. This must be an absolute priority for Government as the race to access skilled talent intensifies, across both public and private sectors. ***Robust investment in technology is also crucial for these public bodies.*** The American Chamber therefore welcomes the related recommendations made in the 'Future of Policing in Ireland'.[34]

The American Chamber welcomes the engagement and collaboration which has been undertaken by Irish officials in the NCSC, An Garda Síochána, the Defence Forces and a range of government departments, agencies and bodies with their European and international counterparts, such as Europol's European Cybercrime Centre (EC3) in countering cyber threats. Operating on a European and global stage is crucial and the ***American Chamber encourages the deepening and strengthening of international relationships,*** especially in light of expected changes at European level via the upcoming EU Cyber Security Act. Engagement at European and international levels can also allow for best-practice sharing and increased knowledge development which is critically important in this global team effort.

The American Chamber recognises the role of the national emergency management system overseen by the Government Taskforce on Emergency Planning and the Office of Emergency Planning in the Department of Defence, both in situations where there is an emergency situation relating to cyber attacks or indeed where incidents may have a cyber security dimension. ***The publication of a stakeholder chart, as mentioned above, would be useful to illustrate the role of the Taskforce and Office in such situations and how this national emergency management system interreacts with other relevant public bodies.***

There are many players and important public bodies that have a stake in ensuring Ireland is cyber secure: the Central Bank, the Data Protection Commission and the Commission for Communications Regulation, to name but a few. ***The continued prioritisation of and resourcing for cyber security within these bodies is essential.***

There is an **important role for the Office of the Government Chief Information Officer (OGCIO)** in ***ensuring consistent standards are met by the information security systems across the breadth of government departments, public agencies and bodies.*** Given that the OGCIO is 'responsible for developing and implementing an ICT Strategy for Government that ensures an integrated approach to the exploitation of ICT across all Departments and Public Service Bodies, accelerating the delivery of digital services across Ireland and a transformation in the use of the Government's information assets'[35] – measuring risks and maturity of capabilities across the various information security systems would fit within this remit. This could be achieved by ensuring adherence to the NIST Cyber Security Framework.[36]

The American Chamber welcomes the passage of the Criminal Justice (Offences Relating to Information Systems) Bill last year which marked the first piece of Irish legislation dedicated specifically to dealing with cybercrime. The legislation gives effect to relevant provisions of EU Directive 2013/40/EU[37] on attacks against information systems and to key provisions of the Council of Europe Convention on Cybercrime (Budapest Convention).[38] However, Ireland still has not fully ratified the Budapest Convention and is one of the only European countries not to do so. ***The American Chamber calls on Government to ensure the remaining provisions in the Budapest Convention are ratified.***

34 https://policereform.ie/en/POLREF/The%20Future%20of%20Policing%20in%20Ireland(web).pdf/Files/The%20Future%20of%20Policing%20in%20Ireland(web).pdf
35 https://www.per.gov.ie/en/minister-howlin-launches-new-office-of-the-government-chief-information-officer-ogcio/
36 https://www.nist.gov/cyberframework
37 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN
38 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

B | ENSURING REGULATION IS MEANINGFUL

At European level, there have been clear moves to elevate the importance of cyber security.[39] This has been embodied in the upcoming EU Cyber Security Act. Currently across the EU, there are variances in policy approaches and institutional capacities to address cyber security.

At European level, there have been clear moves to elevate the importance of cyber security.

The ***American Chamber welcomes the agreement which has been made among EU negotiators to convert ENISA into a permanent EU cyber security agency; strengthen its powers and increase its resources.*** It will enable the agency to contribute more substantially and effectively to awareness-raising on cyber security in the EU and strengthen collaboration between public and private stakeholders across the EU and beyond to tackle cyber threats. As the responsibilities of ENISA grow, and it plays an increased role in integrating the Digital Single Market from a cyber security standpoint, it should aim to continuously reinforce its stakeholder engagement. It will be crucial for ENISA to keep and enhance its ability to cooperate with industry, in an inclusive and transparent way. In many cases, industry plays a leading role in providing software, services and hardware that protect public and private organisations from cyber threats. ***It will also be necessary to maintain cooperation with international partners and standards certification bodies such as the US National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO).***

CERTIFICATION FRAMEWORK

At the moment, a number of different security certification schemes for ICT products exist throughout the EU. Without a common framework, there is an increasing risk of fragmentation in the EU's single market. The proposed certification framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. This will be based on agreement at EU level for the evaluation of the security properties of a specific ICT-based product or service.

The American Chamber is of the view that ***when approaching the concept of certification, a risk-based approach is necessary.*** It is not the case that all applications and systems pose the same level of cyber security threats to the economy. It is important for ENISA and the European Commission to work actively with stakeholders to prioritise and refine any scope of categories and corresponding requirements under a certification scheme. ***The proposal should focus on areas where there are currently gaps and no existing schemes. As it currently stands, the proposed framework is too broad as it encompasses all 'ICT products and services'.***[40]

Certification should rely to the extent possible on standards in place and, in particular, international standards (for example ISO 27001 and its extensions).[41] If there is a need to define new standards and thereby new certifications, ENISA should consider in the first place if international standards exist. Standards such as ISO 27017 may, if needed, be transposed into European standards.

It should also be recognised that although certification is useful, it will not in itself protect against threat actors.

39 https://europa.eu/rapid/press-release_IP-17-3193_en.htm
40 https://eur-lex.europa.eu/resource.html?uri=cellar:1985b4b4-985e-11e7-b92d-01aa75ed71a1.0001.02/DOC_4&format=PDF
41 https://www.iso27001security.com/html/iso27000.html

C | ESTABLISHING PUBLIC-PRIVATE DIALOGUE

Clear, open and rapid methods of communication and sophisticated information sharing across the full range of stakeholders is critical.

Cyber security crosses national borders and involves private and public stakeholders. Indeed, it is the responsibility of both sectors. Developing and maintaining strong relationships between private and public stakeholders is therefore vital. At the heart of these relationships is a sense of trust and confidentiality. Clear, open and rapid methods of communication and sophisticated information sharing across the full range of stakeholders is critical.

As identified by ENISA, there are many different ways throughout Europe by which the public and private sectors interact and collaborate when it comes to cyber security:[42]

- **United Kingdom:** Cybersecurity Information Sharing Partnership (CiSP) sits as part of the UK's NCSC and is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure and confidential environment;[43]
- **Germany:** UP KRITIS is a joint initiative of critical infrastructure operators and governmental agencies involved in critical infrastructure protection and is also used as a platform for fast and reliable communication in crisis management;[44]

And Beyond Europe, there are further examples.

- **United States:** Several versions of public private partnerships exist through various federal agencies, such as the Department of Homeland Security's National Cybersecurity and Communications Integration Centre (NCCIC).[45]

There is no doubt that there is a need for interaction and collaboration across public and private sectors in all countries. There is, however, a need to tailor such a model to suit the profile of a country and its particular security environment.

Public and private sectors working together is also an opportunity to foster innovation. To this end, the ***American Chamber recommends the establishment of a Centre of Excellence for Cyber Security,*** providing an opportunity for the public sector, academia and the private sector to engage in dialogue, exchange ideas and explore topics, solutions and policies. It will also offer an opportunity to carry out regular 'cyber-exercises' to simulate an attack, thereby contributing towards a high level of preparedness. This would be similar to the Digital Policing Innovation Centre as recommended by the Future of Policing in Ireland.[46]

As mentioned previously, the American Chamber is very supportive of the public sector entities which have been tasked with cyber security remits. Fortunately, in Ireland, there is a tradition of **adopting a consultative and collaborative approach.** Indeed, one of the benefits of Ireland's small geographic and population size is that it facilitates effective and meaningful stakeholder relationships, especially across the public and private sectors. Indeed, this has been the case in industry's interactions with the National Cyber Security Centre. ***The American Chamber is of the view that this consultative approach should continue.***

42 https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models
43 https://www.ncsc.gov.uk/cisp
44 https://www.kritis.bund.de/SubSites/Kritis/EN/activities/national/cipimplementationplan/cipimplementationplan_node.html
45 https://www.dhs.gov/blog/2009/10/30/n-kick
46 https://policereform.ie/en/POLREF/The%20Future%20of%20Policing%20in%20Ireland(web).pdf/Files/The%20Future%20of%20Policing%20in%20Ireland(web).pdf

D | DEVELOPING AN ECOSYSTEM

FOSTERING SKILLS

Across all sectors and functions, investing in people will be a key driver for Ireland's continued economic successes. Ireland must protect and enhance its hard-earned reputation for its high-quality talent pool. This factor is at the heart of FDI decision making. Fostering, attracting and retaining talent in both the public and private sectors must be top of the agenda in creating a robust cyber security environment.

Women account for just 7% of the current European cyber security workforce

As stated previously, there is a clear global shortage in highly technical skills required to fill cyber security roles. In the US alone, there are **350,000 open cyber security positions**[47] and a predicted global shortfall **of 3.5 million cyber security jobs by 2021.**[48] It is important to note that **women account for just 7% of the current European cyber security workforce.**[49] ***It stands to reason, therefore, that addressing the clear gender gap in cyber security would go a long way to filling future roles in this sector.***

Within many public and private sector organisations, ***there is also an opportunity to cross-train existing technically trained staff,*** leveraging their existing computer science credentials in order to meet the demand for highly skilled staff in the cyber security sector. This could be achieved through current programmes as the Springboard+[50] upskilling initiative.

The American Chamber greatly welcomed and indeed called for the inclusion of computer science as part of the Leaving Certificate curriculum, which was introduced on a phased basis from September 2018. The ***American Chamber is eager to see a strong focus on information security in the Leaving Certificate Computer Science curriculum –*** both the inclusion of principles relating to protecting one's own data online and also developing the skills necessary to embark on further study in this area.

Embedding security skills from a young age, even younger than secondary school, will be a crucial investment in the future workforce. Indeed, ***the American Chamber advocates for STEM skills, including computer science, to be taught at primary level, especially targeted at girls who would not traditionally be exposed to such subjects.*** It is also vital that ***parents are educated about the range of disciplines within STEM –*** introducing them to the diverse range of career paths and value-adding roles within cyber security.

American Chamber member companies take an active role in the education process, whether it is welcoming a Transition Year student into the organisation for a week or two; participating in programmes aimed at encouraging girls to consider STEM subjects; offering scholarships to second and third level students; or giving college students an opportunity to work within their organisations as part of an internship or work placement programme. These are all important aspects of the education curriculum and member companies of the American Chamber are eager to play a role in this process, across all sectors. Such initiatives will develop the pipeline of STEM graduates, especially for cyber security, with a more diverse cohort.

47 https://www.cyberseek.org/heatmap.html
48 https://www.herjavecgroup.com/wp-content/uploads/2017/06/Jobs_info.pdf
49 https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf
50 https://springboardcourses.ie/

The American Chamber is an advocate for the application of the apprenticeship model to a range of non-traditional career paths. **The American Chamber therefore welcomes the apprenticeship programme for cyber security** which is operated by FastTrack to Information Technology (FIT).[51] ***The American Chamber would like to see a greater promotion of this programme and a more expansive rollout throughout the entire country.*** This also contributes to achieving a commitment in the Government's Action Plan for Education to enrol 31,000 people on apprenticeship programmes in the period 2016-2020. The American Chamber welcomes the Cybersecurity Skills Initiative (CSI) which was launched in 2018 and will provide for cross-skilling and upskilling opportunities for IT professionals across all sectors to a recognised standard.* *More on developing skills at third level and industry-academic relationships further in the paper.*

ATTRACTING TALENT

In tandem with ensuring the necessary technical skills are taught at various levels within the Irish education system, it is also crucial that we have an economic migration system which is fit for purpose.

To attract returning Irish or new talent, issues such as the provision of quality and affordable rental accommodation; access to schooling and personal taxation play a vital role. The American Chamber continues to advocate on behalf of its member companies in these areas and has produced many related research and position papers.

Ireland's migration policy also plays a key role. In order to ensure Ireland remains a welcoming place to work and live, there must be ***continued resourcing of Ireland's work permit system*** with the aim of making Ireland's regime the international benchmark in terms of alignment with forecasted skills needs; ***continued investment in IT infrastructure for processing permits and visas*** to reflect Ireland's tech and innovation credentials.

For many companies working in the cyber security sector in other jurisdictions, vetting is a common feature of the hiring process. ***By working with An Garda Síochána, there is an opportunity to explore a dedicated process for staff to be Garda vetted.***

BUILDING A RESEARCH REPUTATION AND RELATIONSHIPS WITH THIRD LEVEL INSTITUTIONS

The American Chamber encourages the strengthening and enhancing of industry-academic partnerships to ensure there is sufficient talent to fill cyber security roles in both public and private sectors. A number of American Chamber member companies have worked very closely with universities and Institutes of Technology to develop relevant curricula and modules, ensuring the third level courses are relevant to the roles in industry. This has allowed deep collaborative relationships between industry and third level institutions to evolve.

The American Chamber strongly recommends a greater focus on information security in all computer science and engineering courses. Indeed, **all third level computer science and engineering courses should comprise mandatory information security modules** to elevate the importance and proliferation of knowledge in this area. ***There should also be an increased number of targeted courses for key cyber skills, including Security Analysis, Incident Response and Threat Intelligence –*** targeting the highly technical skills that are in- demand in the digital economy.

Strengthened industry-academic relationships would allow for knowledge and best-practice sharing to support the broader research agenda of the cyber security sector. The proposed establishment of a **Centre of Excellence for Cyber Security,** mentioned earlier, would provide an opportunity for academia to work impactfully with the public and private sector to engage in dialogue, exchange ideas and explore topics, solutions and policies.

Now is an opportune time for increased industry-academic collaborations and partnerships with the rollout of the Government's Disruptive Technologies Innovation Fund.

51 http://www.education.ie/en/Press-Events/Press-Releases/2017-Press-Releases/PR17-12-08.html
* https://www.siliconrepublic.com/enterprise/cybersecurity-skills-ireland

Indeed, now is an opportune time for increased industry-academic collaborations and partnerships with the rollout of the Government's **Disruptive Technologies Innovation Fund**[52]: a €500 million challenge-based fund to be implemented through the Department of Business, Enterprise and Innovation and its agencies, working with other research funding bodies to develop Ireland's innovation ecosystem and responsiveness. The aim of the fund is to attract investment in the development and deployment of disruptive innovative technologies and applications, on a commercial basis, targeted at tackling national and global challenges. ***The American Chamber recommends addressing cyber security challenges through the Disruptive Technologies Innovation Fund which would meet societal, in addition to commercial, priorities and enhance Ireland's global research reputation.***

The American Chamber welcomes the new **Science Foundation Ireland (SFI) research programme 'ENABLE'.**[53] This research programme, which is conducted in collaboration with industry, will examine how the Internet of Things can be used to improve the quality of life for ordinary citizens living in urban environments, with a focus on cyber security.

Ensuring that Ireland has a reputation for research when it comes to cyber security will be a major pull for companies when making significant investment decisions. However, it must also be acknowledged that the talent pool limitations also impact the number of graduates available to work in academia. **Therefore, ensuring the skills agenda is top priority will mean that a range of interrelated issues are addressed.**

INCREASING PUBLIC AWARENESS

In this age of GDPR, the public is more aware and informed than ever about their use of data online. With this increasing awareness of personal data online, comes an opportunity to increase basic cyber security standards among the public. In fact, data shows that approximately 90% of all cyber claims are the result of some type of human error or behaviour.[54]

With this increasing awareness of personal data online, comes an opportunity to increase basic cyber security standards among the public.

European Cyber Security Month (ECSM)[55] is an EU initiative which has been deployed every October for the last several years. The aim of which is to raise awareness among the general public of cyber security threats; promote cyber security among citizens and organisations; and provide resources to protect themselves online, through education and sharing of good practice. It also encourages the concept of acting as 'EU digital citizens'. Indeed, the Swedish National Cyber Security Strategy stresses the importance of raising the awareness and ability of all users of IT systems and to create conditions for 'developing a security culture throughout society'.[56]

The American Chamber strongly advocates for the NCSC to be tasked with undertaking a greater public awareness raising and online safety remit via the next Cyber Security Strategy. In increasing public awareness, **use of appropriate and targeted communications tools should be adopted via strategic campaigns.** This should include **targeted assistance for the Small and Medium Enterprise (SME) sector,** similar to what the UK Government has put in place for SMEs.[57] Moreover, in recognising growing cyber threats to democratic institutions and processes, the NCSC should place particular emphasis on tackling the related threats, by working with and leveraging the expertise of all relevant stakeholders: from the private sector, academia and civil society.

Indeed, the stakeholder chart mentioned previously would provide greater clarity to citizens and companies about the various government departments, public agencies and bodies that are tasked with a cyber security remit; their roles and responsibilities. Such a stakeholder chart would then need to be communicated effectively to the public via appropriate channels.

52 http://www.gov.ie/en/campaigns/disruptive-technologies-innovation-fund/
53 http://www.enable-research.ie/
54 http://www.willistowerswatson.com/en/press/2017/03/when-it-comes-to-cyber-risk-businesses-are-missing-the-human-touch
55 http://cybersecuritymonth.eu/
56 http://www.government.se/4ac8ff/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213
57 http://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know

RECOMMENDATIONS SUMMARY

A Building public sector capabilities

- The continued support for the **National Cyber Security Centre (NCSC)** with significant funding and resources.
- Robust investment in technology for the **Garda National Cyber Crime Bureau (GNCCB) and the Defence Forces' Communications and Information Services (CIS).**
- **Deepening and strengthening of international relationships and collaborations** at governmental, agency and public body levels.
- **The continued prioritisation of and resourcing for cyber security within relevant public bodies,** such as the Central Bank, the Data Protection Commission and the Commission for Communications Regulation.
- The ratification of the remaining provisions in the **Budapest Convention.**
- The publication and dissemination of a **stakeholder chart** which outlines the roles and responsibilities of the various government departments, public agencies and bodies that have a role in national cyber security.
- **Measuring risks and maturity of capabilities** across the various information security systems of government departments by the Office of the Government Chief Information Officer (OGCIO), such as adhering to the NIST Cyber Security Framework.

B Ensuring regulation is meaningful

- Increased funding for the **European Union Agency for Network and Information Security (ENISA)** to enable its effective conversion into a permanent EU cyber security agency.

Certification Framework

- Avoiding duplication of certification standards by **adopting international standards** already in place (for example ***ISO 27001 and its extensions).***
- Cooperation by ENISA with international partners and standards certification bodies such as the **US National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO).**

C Establishing public-private dialogue

- **Clear, open and rapid methods of communication and sophisticated information sharing** between public and private sectors.
- **The exploration of the establishment of a Centre of Excellence for Cyber Security,** providing an opportunity for the public sector, academia and the private sector to engage, exchange ideas and develop solutions.
- The continuation of the National Cyber Security Centre's **consultative approach to industry engagement.**

D Developing an ecosystem

Fostering skills

- **Cross-training** of existing technically trained staff to meet skills gaps in public and private sectors, through such programmes as the Springboard+ upskilling initiative.
- A strong focus on information security in the **Leaving Certificate Computer Science curriculum.**
- Inclusion of computer science on the **primary school curriculum.**
- **Educating parents** about the range of disciplines within STEM.
- Encouraging **greater uptake of STEM subjects among girls** in order to rectify the gender imbalance in cyber security roles.
- **Greater promotion and broader rollout of the apprenticeship programme for cyber security** which is operated by FastTrack to Information Technology (FIT).

Attracting Talent

- **Continued resourcing of Ireland's work permit system and continued investment in IT infrastructure for processing permits and visas** to facilitate easier corporate immigration practices where vacant roles need to be filled.
- Working with An Garda Síochána to explore a **dedicated process for staff to be Garda vetted.**

Building a research reputation and relationships with third level institutions

- Greater focus on information security in all third level computer science and engineering courses by including **mandatory information security modules.**
- **Increased number of targeted courses for key cyber skills, including Security Analysis, Incident Response and Threat Intelligence –** targeting the highly technical skills that are in- demand in the digital economy.
- Tapping into the **Disruptive Technologies Innovation Fund** by adopting a cyber security focused challenge which would meet societal, in addition to commercial, priorities and enhance Ireland's global research reputation.

Increasing public awareness

- **Tasking NCSC with a greater awareness raising and online safety remit.**

OUTCOMES FOR IRELAND

This position paper has aimed to highlight the criticality of addressing cyber security in Ireland but also the great opportunity in leading cyber security globally. As such, the American Chamber advocates that by 2020, strides need to be made under each of these specific policy areas:

- Adequate resourcing and funding of public sector bodies which have a national cyber security mandate and a consistent cross-government approach to information security.
- Meaningful regulatory measures which have received input from relevant stakeholders.
- An ongoing and successful public-private dialogue.
- A plan to address demand for talent; greater collaboration with research bodies and increased public awareness.

CONCLUSION

With the rapid pace of change in technology, it is critically important that policies keep pace and remain relevant for this digitised world. Ireland is well positioned to leverage the presence of many global and indigenous companies to show leadership as ***the strongest link in the chain*** when it comes to cyber security. However, it is crucial that the policy environment and a robust infrastructure is in place to support this goal.

Although there have been significant developments in recent years to build Ireland's capacity to deal with cyber attacks from a public sector point of view, we must also be conscious that **cyber threats are ever-evolving and require constant prioritisation by all levels of Government.** Any challenge to the quality of Ireland's data environment, which has been key to the continuing expansion and growth of the digital economy in Ireland, creates a risk of business disruption as well as reputational damage. Ireland needs to build on the digital leadership position it has garnered and apply this to cyber security.

In order to achieve the ambition of strong cyber security leadership, in the context of the next National Cyber Security Strategy, and for strides to be made by 2020, there must be adequate resourcing and funding of public sector bodies which have a national cyber security mandate and a consistent cross-government approach to information security; meaningful regulatory measures which have received input from relevant stakeholders; an ongoing and successful public-private dialogue; a plan to address demand for talent; greater collaboration with research bodies and increased public awareness.

Any challenge to the quality of Ireland's data environment, which has been key to the continuing expansion and growth of the digital economy in Ireland, creates a risk of business disruption as well as reputational damage.

As evidenced throughout this paper, cyber security is truly a team sport. Therefore, it is relevant and necessary for all stakeholders to ensure the policy environment is conducive to the strongest link in the chain.

The American Chamber's Cyber Security Network

... brings together a cross sectoral group of senior policy, legal and technical professionals focused on strengthening Ireland's reputation as a secure investment location.

The Network maintains close collaboration with policy stakeholders to make an impactful contribution to Ireland's national cyber security environment.

AMERICAN CHAMBER *of* COMMERCE IRELAND