National Cyber Security Strategy 2019 - 2024 ('NCSS')

Ibec priorities for Department of Environment Climate & Communications (DECC) NCSS Mid-Term Review

February 7 2023

Contents

Key Messages

On National Cyber Security Strategy 2019-2024 ('the NCSS') Mid-Term Review ('mid-term review'):

Ibec welcome the opportunity to contribute views in response to the Department's (DECC) consultation on the NCSS mid-term review.

Ibec represents a wide range of sectors and businesses[i] across our digitalised economy/society and our cyber security ecosystem who develop, provide, require and deploy cyber security and resilience solutions.

We welcome this important and timely review. Digital readiness is essential in ensuring our prosperity, resilience, and societal well-being. We cannot be complacent. Enhancing our cyber security and resilience is both an economic/societal imperative and an economic opportunity[ii].

While acknowledging progress to date, this paper refers to proposals in the DECC consultation and outlines four main areas for intervention by Government:

1. Lead Ireland's cyber security, resilience and opportunity;
2. Safeguard Ireland's future cyber security, resilience and opportunity;
3. Enable enhanced cyber security, resilience and opportunity; and
4. Include everyone in enhanced cyber security, resilience and opportunity.

Introduction: Ireland's cyber security and resilience matter to Business

1. Ensure our prosperity, resilience, and societal well-being.

Digital readiness, and the cyber security and resilience necessary to safeguard that readiness, are essential in ensuring our prosperity, resilience, and societal well-being. Digital readiness is:

- **A proven enabler to navigate economic and societal headwinds** including health and the twinned green transition.
    - The EU Commission Vice President Margarethe Vestager, speaking to Ibec members in 2022, has rightly said "*There is no turning back. To solve things and shorten [the current crises] we need some of the things the digital and green transition can bring*"[iii].

- **Integral to our economy and society**. The pandemic accelerated our digital transition[iv].
    - The EIB (2022) stated that '*the pandemic has made the digital transformation an integral part of society – and integral to firms' survival*.' EIB research also indicates that overall, more digitally advanced firms tend to perform better in terms of productivity, exports, investment, innovation, growth, and resilience[v].

- **An enabler of our smart, global, and diverse economy.** Our digitally intensive sectors[vi] now directly employ over 270,000 people here[vii].
    - 29% of our manufacturing jobs are in high technology sectors. This is four times the EU average[viii].
    - Ireland has a significant opportunity to become a global hub for digital health, where companies can develop and commercialise products, as well as attract projects and investments[ix].
    - In 2020, 41% of goods and services produced in the economy were transacted digitally. This can take the form of being digitally ordered, digitally delivered or both[x].
    - The Irish Data Protection Commissioner believes that "Every company now is a data company."[xi]

- The OECD recognise Ireland as being part of a group of top global hubs for the import and export of digitally deliverable services[xii]. Ireland is:
    - A global fintech hub[xiii].
    - The current NCSS recognises that "*Ireland is home, according to some estimates, to over 30% of all EU data, and to the European Headquarters of many of the world's largest technology companies. Our economic success is therefore closely bound up with our ongoing ability to provide a secure environment for these companies to operate here*"[xiv]. Domestic companies accounted for almost half of employment in our Information and Communications Technology (ICT) sector in 2019[xv]. Since 2013, the technology sector in Ireland has grown at an average of 12% per annum. Most notably the sector grew by 30% in the period Q4, 2019 – Q4 2021. Approximately 63% of the ICT workforce had a third level qualification or higher, among the highest in the overall economy. The total investment in the ICT sector at the end of 2019 was €103bn (10% of all capital assets in Ireland)[xvi].
    - The cyber security sector employs 7,351 cyber security professionals, across 489 firms, in Ireland. There is a relatively even split between the count of large firms and SMEs in the sector, and almost half of all cyber security firms operating in Ireland are indigenous. It is estimated that Ireland's cyber security sector generated approximately €2.1bn in revenue and €1.1bn in GVA in 2021[xvii].

- **An enabler of better services.** It is estimated that a 10% increase in the adoption of cloud in the Irish public sector could generate economic benefits in the order of €473 million in the first year alone[xviii].
    - In 2021, the Department of Public Expenditure and Reform announced that by 2030, 90% of applicable public services should be delivered online. More recently, Harnessing Digital: Digital Ireland Framework, seen as Ireland's national digital strategy[xix], and Connecting Government 2030, the new public sector ICT strategy, indicated that this goal would be reached by "taking a cloud-first approach to delivery of all services".

- **A shared ambition by policy makers and business, both in the short-term and over this decade**. Europe, Ireland and business have high ambitions for their green and digital transition to 2030. In many ways these ambitions share similarities and dependencies. Green and trusted digital transitions can be mutually reinforcing, securing, and sustaining physical and digital environments that sustain us.
    - The EU aims to empower businesses and people in a human-centred, sustainable, and more prosperous digital future. Its approach involves 3 pillars, including:
        - *Leadership* on 4 ('digital compass') targets (enhancing digital infrastructure, skills and digital adoption in the public and private sectors) by 2030;
        - *Safeguarding trust* - the development and deployment of 'trusted' digital and data innovation in a manner that safeguards people and the environment[xx] that sustains them (e.g., safeguards security, safety, market fairness human rights and sustainability); and
        - *Excellence,* in other words investing and leading in strategic digital capacities. The Recovery and Resilience Fund was designed to support investment in both our digital and green transition.
    - Ireland's new overarching National Digital Strategy[xxi] and associated initiatives reflect EU ambitions in digital leadership, trust and excellence. In addition, our national targets are broadly complementary to the European Commission's Digital Compass targets to 2030.
    - Ibec[xxii] and its European partners[xxiii] support the EU and Ireland's 2030 digital targets. In recent Ibec surveys, nearly 9 out of 10 Irish CEOs agree or strongly agreed that '*Being prepared for technological change is a key priority for their role*' in 2022[xxiv] and 53% Manufacturers planned to invest in digital in 2023[xxv]. In 2022, Ireland's technology sector outlined a new strategy, central to achieving its vision of securing Ireland's place as a global technology powerhouse and maintaining that place for the years ahead[xxvi].

2. We cannot be complacent on the state or rate of our cybersecurity and resilience

Ireland and other EU frontrunners are well placed to realise further digital opportunity. However, we cannot be complacent on the *state* or *rate* of our digital progress and the cyber security and resilience necessary to safeguard that progress. There are challenges:

- **There are divides, not every region, sector, enterprise, and individual are impacted the same way by digital trends, and gaps**. We have a competitive imperative to keep up with other EU frontrunners and competitors outside the EU on aspects of our digital readiness[xxvii]. Research, by Ibec, Amarach, .IE and CSO, indicates that firms big and small understand further trusted digital innovation is important and are ambitious. However, many firms have further to travel.
- **Cyber security readiness requires further prioritisation**. ITU surveys on international commitments to cyber security[xxviii] rank Ireland as 28th out 36 countries surveyed in the European region[xxix].
- **Cyber threats pose risks to our critical infrastructure, essential services and our digitalised economy and society**. Research indicates cyber threats continue to grow and evolve[xxx] and while progress is being made, there is further work to be done in addressing gaps and divides in cyber security and resilience across organisations and individuals[xxxi]. The National Cyber Security Centre (NCSC), the Garda National Cyber Crime Bureau (GNCCB) and Ibec's Small Firms Association have warned business owners of an increased threat of ransomware[xxxii]. The cost of Irish Cybercrime was estimated to exceed €10 Billion in 2022[xxxiii].
- **The EU's policy and regulatory landscape on cyber security and resilience continues to evolve and grow**[xxxiv], increasing requirements on Member States and enterprise.
- **There are competing visions of the internet**. In Europe, there is a political ambition for greater strategic autonomy, while other regions are pursuing tech-industrial policies to strengthen their capacities in strategic digital technologies. Potential divisions of the internet may present choices between an open versus a closed internet[xxxv].

3. Cyber security and resilience are an imperative and opportunity

Cyber security and resilience are an economic/societal imperative and an economic opportunity. We must ensure policy makers, statutory bodies, business and technology stakeholders work together to address gaps and divides that:

- Safeguard and enable our smart, global, and diverse economy.
- Grow our economic opportunity in cyber security.
- Ensure a safe, secure, and trusted internet while keeping it open and free to address shared generational challenges to our economy and well-being.

Ibec has welcomed the Government's National Digital Strategy (NDS) and NCSS, as important steps in enabling a more innovative, sustainable, and competitive Ireland, that is part of an outward-looking and successful EU; that provides conditions for organisations and individuals to adapt to the twin Digital and Green transitions and reach their full potential.

In this context, the NCSS mid-term review is welcome given the opportunity and changes in our threat and regulatory landscape since 2019. Acknowledging progress to date, Ibec recommends four main areas for further intervention by Government:

- Lead Ireland's cyber security, resilience and opportunity;
- Safeguard Ireland's future cyber security, resilience and opportunity;
- Enable enhanced cyber security, resilience and opportunity; and
- Include everyone in enhanced cyber security, resilience and opportunity.

Recommendations

1. Lead Ireland's cyber security, resilience and opportunity.

Provide political leadership to prioritise, co-ordinate and enhance Ireland's cyber security, resilience and opportunity. Intensify cyber leadership at home and with our international partners. Develop our 'centralised' institutional infrastructure to engage, lead and co-ordinate government and non-governmental stakeholders in a shared and renewed vision that enhances further cyber security, resilience, and opportunity. Specifically:

- **Support the need for a whole of government (co-ordinated) approach and enterprise engagement in the design as well as the delivery of a renewed NCSS and related strategies and initiatives.** In this context:
    - Enable meaningful engagement that enhances national cyber security and develops economic opportunities. We welcome the progress made on Ireland's cyber cluster and the whole of government approach and enterprise engagement provided for in the NDS[xxxvi]. Ibec welcomes the proposal in this consultation to establish an advisory group to provide the NCSC with independent perspectives and input on strategy and policies. The advisory group must be reflective and representative of policy/regulatory, technology, research, and business perspectives.
    - We would welcome further engagement on the proposed NCSS 3.0 and transposition of EU requirements.

- **Lead on digital Government and public services, provide a catalyst for growth. Develop Ireland's cyber security sector.** Engage the industry and the public sector. Act on the Cruinniú GovTech report recommendations. Address any administrative barriers to procurement in cyber security services. Encourage partnerships between large and small firms in our cybersecurity ecosystem.

- **Embrace Irelands international role as an 'Regulatory and Digital Hub'.** Work with likeminded international partners to deepen international co-operation in identifying and strengthening capacities to address the evolving cyberthreat landscape Shape EU policy and regulation on cyber security and resilience.
    - **Ibec and the other main business federations across Europe support a 'smart technological sovereignty[xxxvii]' approach that encourages indigenous capacities while remaining open to co-operation and trade with likeminded international partners.**
        - We welcome comments made by Minister Smyth at the Joint Committee on EU Affairs[xxxviii] and TELE Council[xxxix] and the Ibec Global Cybersecurity Summit in 2021, in relation to the EU cybersecurity strategy, on the importance of deeper international co-operation in identifying and strengthening capacities to address the evolving cyberthreat landscape. As the Minister rightly pointed out, we should develop our indigenous cybersecurity ecosystem, while '*preserving an open economy*' and that '*while it is important to develop the European cyber security ecosystem, we cannot lose sight of the need to take positive steps today and tomorrow, to deploy best-in-class hardware and software to defend networks and systems, whether these come from Europe, the US or elsewhere.*'
        - Work with likeminded partners to deepen international co-operation and trust in cyber security and resilience. Advance multi-stakeholder international co-operation[xl]. Leverage the EU-US Trade and Technology Council (TTC) and the EU-US Cyber Dialogue.
        - Ensure the free movement of cloud services across Europe through the development of an European Cloud Certification Scheme (EUCS), in accordance with the Cyber Security Act[xli] which will help the EU economy prosper at home and abroad, contribute to Europe's digital ambitions, and strengthen its resilience. We restate our principled approach to the development of the EUCS[xlii]. EU legislators should ensure the impacts of all proposed requirements in the draft EUCS scheme on businesses and the Single Market are thoroughly considered and addressed. Political considerations should not be delegated as per the ECJ ruling[xliii].

2. Safeguard Ireland's future cyber security, resilience and opportunity.

Sustain trust online and safeguard business, services, and individuals online.

- **Invest further in national cyber security capacities and ensure Ireland continues to play a strong role internationally in these areas.** Engage, co-ordinate and strengthen our cyber security ecosystem. Research by William Fry and Amarach highlights that data-driven regulatory issues have become a major investment attractor[xliv]. Consequently Ibec:
  - Welcomes the Government expansion of the NCSC to date[xlv].
  - Supports further and appropriate resources for national cyber security capacities, as signalled in our on-going stakeholder engagement and pre-budget submissions[xlvi]. Further resources will be necessary to fulfil (a) the recommendations of the NCSC Capacity review, the NSCC activities proposed in the mid-term review and the proposed expansion of NCSC functions in response to upcoming EU requirements e.g., NIS2; and (b) the Commission on the Defence Forces' recommendations accepted by the Government[xlvii].

3. Enable enhanced cyber security, resilience and opportunity.

Support what is essential 21st century enterprise infrastructure. Enable further opportunity.

- **Boost national R&D capabilities to support our cyber security ecosystem.** Ireland's cyber security cluster reports Ireland has an 'emerging R&D ecosystem' and a 'fragmented R&D landscape'[xlviii]. Scale public investment for research and innovation. Explore all-island co-operation. Provide dedicated research calls. Position Ireland to realise emerging opportunities. Develop our network of Digital Innovation Hubs and incubation centres to support our cyber security, resilience and opportunity. We support the proposed establishment of an incubator facility and the exploration of a European Digital Innovation Hub (EDIH) on cyber security under the Digital Europe facility. We welcome further engagement on this.
- **Develop our cyber security industry.** We support a proposed strategy on the development of the cyber security industry in Ireland and measures to support further industry, research, business and government collaboration. We welcome further engagement on this.
- **Intensify absorptive capacity and adoption across enterprise.** We support the development and implementation of a proposed SME support programme. This would support the Government ambition for 90% of Irish SMEs to be digital by 2030. We welcome further engagement on this.

4. Include everyone in enhanced cyber security, resilience and opportunity.

Foster the skills, talent and inclusion necessary[xlix] to enhance our cyber security, resilience and opportunity. Ireland's technology sector has placed talent as its number one priority in the period 2022-2026[l]

- **Continue to gather intelligence on technological trends, our evolving labour market and consequent cyber security skills needs to inform supply.** There are several ongoing strategies and initiatives aimed at bolstering digital skills and while progress is being made, gaps remain. Several pathways are required to meet needs.
- **A strategic approach to addressing digital (including cyber) skills should mobilise and coordinate the whole education and training system around three key pillars:** responding to existing skills needs of industry through upskilling and reskilling programmes; building a strong talent pipeline with multiple and varied opportunities to develop digital (including cyber) skills; and supporting digital inclusion through lifelong learning and digital (including cyber) literacy.

- **While ensuring that appropriate second and third level training in computer science and cybersecurity is available (Measure 12), it is also important that modules relating to Operational Technology and the securing of the same are included in these courses.** We understand there is an uplift in entry-level resources from cybersecurity courses, however there is no specific modules or projects mentioned which illustrate an understanding of OT environments.
- **On Measure 13, there could be additional engagement with primary school students achieved through partnership with local bodies such as "Coderdojo" clubs where young students are engaging with coding and robotics.** Development of specific material on these dojo platforms for use could ensure that security measures and concepts are included alongside their first engagement with these science areas.

- **The surplus of the National Training Fund (NTF) should be leveraged to underpin a strategic approach to addressing the immediate digital (including cyber security) skills needs of business (including the cyber security sector).** There was a €855 million surplus in the NTF in 2022, which is estimated to increase by a further €150 million this year and to as much as €1.9 billion by 2025. This is unsustainable in the context of a tight labour market and increasing business costs. A mechanism is urgently needed to prevent the further untargeted accumulation of employer contributions and to utilise the surplus to address training costs for business, incentivise SME upskilling, and drive innovation in digital (including cyber security) skills delivery.
- **Attract and retain mobile cyber security talent.** Resource and continue the reform of visa and work permit processes. Ensure our tax system fosters talent. Support retention by addressing housing challenges.

Endnotes

[i] Ibec is Ireland's largest lobby and business representative group. Our purpose is to help build a better, sustainable future by influencing, supporting and delivering for business success. Ibec positions are shaped by our diverse membership, which range from small to large, domestic to multinational and our 39 trade associations cover a wide range of industry sectors. Ibec members employ over 70% of the private sector workforce in Ireland (www.ibec.ie/digitalpolicy).
[ii] Ibec (2021) Backing our digital future – Business priorities for a digitised Ireland 2021-2025
[iii] Ibec (2022) Ibec Global Conference, TCD, Supporting an improved digital future for Ireland and Europe and https://ireland.representation.ec.europa.eu/news-and-events/news/keynote-address-european-commission-executive-vice-president-margrethe-vestager-ibec-conference-2022-09-30_en
[iv] McKinsey (2020) https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever and (2021) https://www.mckinsey.com/featured-insights/future-of-work/the-future-of-work-after-covid-19.
[v] EIB (2022) Digitalisation in Europe 2021-2022
[vi] Sectors that intensively use digital goods and services (very high shares of digital capital, labour, and intermediate inputs relative to total inputs, above the 80th percentile)
[vii] Technology Ireland (2022a) Technology Ireland submission to the Joint Committee on Enterprise, Trade and Employment on challenges facing the technology sector
[viii] Ibec (2022) Manufacturing in Ireland
[ix] https://www.ibec.ie/digitalhealth
[x] CSO (2022) Digital Transactions in the Irish Economy 2020
[xi] Silicon Republic (2017) The five-minute CIO: Helen Dixon, Data Protection Commissioner.
[xii] OECD (2020) https://www.oecd-ilibrary.org/science-and-technology/perspectives-on-the-value-of-data-and-data-flows_a2216bc1-en;jsessionid=kIR7SLL0s_gZhGSqmjVPf6tx.ip-10-240-5-171
[xiii] Financial Services Ireland (2021) Ireland: Financial services powerhouse for now and the future
[xiv] https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf
[xv] CSO (2022) Information and Communications Technology: A Value Chain Analysis 2019
[xvi] Technology Ireland (2022a) ibid.
[xvii] Cyber Ireland (2022a) State of the Cyber Security Sector in Ireland.
[xviii] Technology Ireland (2022b) The sky is the limit - How cloud computing is the key to better public services in Ireland
[xix] Department An Taoiseach (2022) https://www.gov.ie/en/press-release/3a922-online-launch-of-harnessing-digital-the-digital-ireland-framework/
[xx] Both physical and digital environments.
[xxi] Department An Taoiseach (2022) ibid.
[xxii] Ibec (2021) Ibid. and https://www.ibec.ie/influencing-for-business/ibec-campaigns/eu-campaign
[xxiii] https://www.ibec.ie/-/media/documents/influencing-for-business/digital-policy/business-9-digital-ministerial-paperdecember-2022.pdf
[xxiv] Ibec (2022) Business in 2022 and beyond A CEO perspective
[xxv] Ibec (2022) Ibid.
[xxvi] Technology Ireland (2022c) Technology Ireland Strategy 2022-2026
[xxvii] European Commission (2022) DESI https://digital-strategy.ec.europa.eu/en/policies/desi

[xxviii] A higher score in the Global Cybersecurity Index indicates that a country has put in place more measures as measured by the GCI to strengthen its cybersecurity posture across the five pillars: Legal, Technical, Cooperative, Organizational, and Capacity Building Measures. It does not indicate that a country has fewer cybersecurity attacks.
[xxix] ITU (2021) Global Cybersecurity Index 2020 Measuring commitment to cybersecurity.
[xxx] ENISA (2022) Threat Landscape; WEF (2023) Global Risks Report and ongoing NCSC advisories.
[xxxi] Microsoft & Amarach (2020) Securing the Future; Grant Thornton (2021) The cost of cybercrime; and PWC (2022) Global Digital Trust Insight Survey 2023 and IoD (2023) https://www.iodireland.ie/resources-media/research-publications/research-reports/director-sentiment-monitor-q4-2022
[xxxii] DECC (2022) https://www.gov.ie/en/press-release/58df1-increased-threat-of-ransomware-for-small-and-medium-businesses/ and SFA (2022) https://www.ibec.ie/sfa/news-insights-and-events/events/2022/ransomware-and-phishing/event-tab
[xxxiii] Grant Thornton (2022) The cost of cybercrime 2022
[xxxiv] European Commission (2020) Cybersecurity Strategy for the Digital Decade etc., see NCSS MTR consultation paper.
[xxxv] IIEA (2022) Cyber Security and European Strategic European Autonomy: Coherence and Capability Challenges
[xxxvi] Enterprise Digital Advisory Forum
[xxxvii] https://www.businesseurope.eu/publications/technological-sovereignty-eu-must-resist-inward-looking-approach
[xxxviii] https://www.oireachtas.ie/en/committees/33/european-union-affairs/documents/
[xxxix] https://video.consilium.europa.eu/event/en/25132
[xl] Ibec Global (2021) Cybersecurity Summit – The Transatlantic Reboot.
[xli] Article 54. Elements of European cybersecurity certification schemes

[xlii] B9+ (2022) https://www.ibec.ie/-/media/b9-joint-statement---navigating-the-headwinds_220919.pdf
[xliii] Recent information provided at ENISA's Certification conference in June 2022 points to the inclusion of a political requirement for digital sovereignty in the draft EUCS although the notion of "sovereignty" is not yet defined at a European level. The CJEU (Case C-355/10) states that "provisions which, in order to be adopted, require political choices falling within the responsibilities of the European Union legislature cannot be delegated".
[xliv] https://www.irishtimes.com/sponsored/ibec/digital-readiness-is-the-growth-lever-ireland-needs-to-invest-in-fast-1.4654941
[xlv] RTE (2021) https://www.rte.ie/news/business/2021/0713/1234843-cyber-security-centre-to-get-budget-and-staff-boost/
[xlvi] Ibec (2022) https://www.ibec.ie/-/media/documents/ibec-campaigns/budget-2023/ibec-budget-submission-2023.pdf
[xlvii] Section 5.3. of the consultation.
[xlviii] Cyber Ireland (2022b) Achieving our cyber potential 2030
[xlix] Ibec (2022) Investing further in digital skills to enable further opportunity and inclusion
[l] Technology Ireland (2022c) Ibid.