Microsoft Ireland Operations Ltd
One Microsoft Place
South County Business Park
Leopardstown
DUBLIN D18 P521

30 January 2023

National Cyber Security Strategy MTR Consultation
Cyber Security and Internet Policy Division
Department of Communications, Climate Action and Environment
29-31 Adelaide Road
Dublin D02 X285
Email: cyberconsult@dccae.gov.ie

Re: Submission to the Cyber Security and Internet Policy Division of the Department of Communications, Climate Action and Environment with respect to the National Cyber Security Strategy 2019-2024 Mid-Term Review Consultation

To Whom It May Concern:

Microsoft respectfully submits the following comments in response to the Department of Communications, Climate Action and Environment's Consultation with respect to the National Cyber Security Strategy 2019-2024 Mid-Term Review.

We have set out some overall comments which we believe are appropriate to this critical area of National Cyber Security and we have also provided responses, where appropriate, to the review questions that the Department has posed.

We appreciate the opportunity to provide our input to this consultation and welcome follow-up discussions with the Department on our response below.

Respectfully submitted,

[redacted]

[redacted]

/ctd.

Microsoft

Microsoft's submission to the Cyber Security and Internet Policy Division of the Department of Communications, Climate Action and Environment with respect to the National Cyber Security Strategy 2019-2024 Mid-Term Review Consultation

Executive Summary

Microsoft's view on cyber security is that it is a constantly evolving landscape that requires organisations to take a proactive and holistic approach to protecting their systems and data. The Microsoft Digital Defense Report 2022[1] highlighted the sheer scale of the challenge, particularly in light of the hybrid warfare being conducted by Russia in its illegal war in Ukraine.

The numbers are startling:

- 65 trillion signals tracked daily by our systems to understand and protect against cyber attacks globally (was 43 trillion, now revised[2]);
- 37 billion individual email threats blocked in a year;
- 34 billion identity threats blocked; and
- 921 password attacks per second: up 74% in one year.

Irish specific research shows that 7 in 10 Irish businesses have experienced cyber attacks and 9 in 10 Public Sector Bodies (PSBs) fear they have inadequate cyber security systems.[3]

In an Irish context much of our political and public awareness of cyber threats comes from the ransomware attack on the Health Service Executive (HSE) in 2021. The PwC report into the attack stated that more than 80% of the HSE's IT infrastructure was affected[4] and there were severe impacts on health services in Ireland with a financial cost estimated at over €100m[5] allied to the physical and mental health impacts on both patients and staff alike.

Crucially, a PwC report into the attack found that the hackers gained access to the HSE's systems eight weeks before the ransomware was detonated. They were also able to

[1] Microsoft Digital Defense Report 2022 | Microsoft Security

[2] Plan for the future with Microsoft Security - Microsoft Security Blog

[3] Infographic: The state of cybersecurity in Ireland (microsoft.com)

[4] PWC Report: conti-cyber-attack-on-the-hse-full-report.pdf at p. 15.

[5] HSE computers only monitored for viruses during daytime hours prior to cyberattack, report reveals – The Irish Times

achieve their objectives "*with relative ease*" due to the "*frailty*"[6] of the HSE's IT estate, according to the report.

It is in this context that the review of the NCSC Strategy is taking place and where Microsoft wants to continue to play its part in keeping citizens and institutions data secure.

In that regard, the Microsoft Digital Defense Report 2022 highlights the following key points:

1. The increasing sophistication of cyber attacks: cyber criminals are using more advanced tactics, such as using multiple stages of attacks, leveraging cloud services, and using artificial intelligence to evade detection;
2. The need for a comprehensive security strategy: organisations need to implement a security strategy that covers all aspects of their operations, including people, processes, and technology. This includes using a combination of preventative measures, such as multi-factor authentication and security software, as well as detection and response capabilities to quickly identify and respond to threats;
3. The importance of visibility and control: organisations need to have visibility into the devices and applications that are connecting to their networks, as well as control over who has access to sensitive data;
4. The role of threat intelligence: organisations need to be able to quickly and accurately identify and respond to threats, which requires access to high-quality threat intelligence; and
5. The importance of security culture: building a security culture within an organisation is critical to ensuring that all employees understand the importance of cyber security and are aware of their role in protecting the organisation's systems and data.

With reference to Ireland's best approach for an effective national cyber security strategy, the following areas are of the utmost importance.

Leadership and governance demands a clear and comprehensive cyber security strategy which should be developed and implemented at the national level, with dedicated leadership and oversight to ensure its success. We see both the existing measure and proposed additional measures giving effect to this. In addition we would welcome the elevation of the cyber threat within the National Risk Assessment review of risk threats given its live, recent, immediate, and known capacity to impact across governance systems[7]. It is not an isolated, siloed risk to be 'left' to the NCSC to deal with, rather it needs a whole of government prioritisation and engagement.

[6] PWC Report, Op. Cit., p. 7.

[7] gov.ie - National Risk Assessment 2021/2022 – Overview of Strategic Risks (www.gov.ie) at p. 67.

In terms of risk management, Ireland should conduct regular risk assessments to identify and prioritise potential cyber threats, and develop and implement measures to mitigate those risks. The proposed measures in the strategy give effect to this.

With respect to cyber incident response, countries should have well-coordinated incident response plans in place to quickly and effectively respond to cyber incidents and this should also leverage good information sharing practices where countries should have solid mechanisms in place for sharing cyber threat information between government agencies, private sector organisations, and international partners. Again, the overall approach from the NCSC reflects these imperatives.

Cyber security education and awareness is absolutely critical across society, public, and private sector. Ireland should further invest in cyber security education and awareness programs to educate citizens and organisations about the importance of cyber security and how to protect themselves from cyber threats. In addition to the proposed measures outlined in the Mid-Term Review, Microsoft has suggested other measures to complement and augment these.

Cyber defence and protection: Countries should invest in and develop capabilities to detect, prevent and respond to cyber attacks on critical infrastructure and national security.

In terms of international cooperation, Ireland should work together with and cooperate with other countries and international organisations to share information and best practices and to develop common approaches to addressing cyber security challenges.

Implementing an effective national cyber security strategy requires a coordinated effort across different sectors and levels of government, as well as active participation from the private sector and international partners. It also requires ongoing monitoring and adaptation to stay ahead of the constantly evolving cyber threat landscape.

In summary, Microsoft's view on cyber security is that it is an ongoing process that requires organisations to take a proactive, holistic approach to protecting their systems and data. This includes implementing a comprehensive security strategy, gaining visibility and control over devices and applications, leveraging threat intelligence, and building a strong security culture within the organization.

Responses to the Consultation Questions

1. Objectives (s. 3, p. 7)

The proposed objectives are still relevant.

However, Objective 5 (‘*To raise awareness of the responsibilities of businesses around securing their networks, devices and information and to drive research and development in cyber security in Ireland, including by facilitating investment in new technology*’) appears to exclude PSBs. While this may to some extent be picked up in other objectives, including Objective 3, Microsoft believes that there should be a specific focus on the Public Sector, given the need for Public Sector (and Government in particular) to lead and act as role models; the sensitivity of the data that is often under their custodianship; and the relative lack of maturity in this sector in this area.

Furthermore, Microsoft suggests that while the objectives remain valid, there is scope to augment them with more meaningful and tangible characteristics including targets/milestones/dates, in the same way as is done later in the Consultation Paper. For example, an objective might be time-bound, such as, ‘*To improve the resilience and security of public sector IT systems to better protect data and the services that our people rely on, such that XX% of such organisations must demonstrate NN% of improvement by DD-MM-YY*’).

2. National Capacity Development (s. 6, pp. 16-17)

The proposed measures are appropriate.

Microsoft further suggests that continued close engagement with industry to complement and augment NCSC capabilities would be beneficial for the overall cyber security posture of the State. Such activities might take the form of improved information sharing, joint activities, assessments, etc.

The NCSC’s enrollment in the Microsoft Government Security Program is a good example of such an industry engagement.

Additionally, there are publicly available resources that can help build capacity and wider understanding across PSBs, including the UCD Centre for Digital Policy video series[8], in which the NCSC participated. Leveraging and promoting, and indeed developing more of the same, of these types or resources, in UCD or elsewhere, across PSBs is a relatively easy and cost-effective means of building capacity.

It is also worthwhile considering establishing some form of 'advisory forum' where the NCSC, other state entities, and industry bodies could share ideas and develop such proposals.

3. Critical National Infrastructure Protection (s. 7, pp. 18-20)

The proposed measures are appropriate.

The NCSC may wish to further consider, building on the additional recommendation above, some form of partnership with industry expertise with respect to the vulnerability assessment service.

4. Public Sector Networks and Data (s. 8, pp. 21-23)

The proposed measures are appropriate.

Microsoft further suggests considering some mechanism to accelerate the digital transformation of Public Sector services and in particular the faster adoption of public cloud technologies which offer a more secure and reliable service for the Public Sector itself and the citizens that avail of these services.

The NCSC may further wish to consider aspects of the accreditation service and certification program to include public cloud-based services, specifically the certification of such public services to facilitate easier and more rapid adoption of those technologies by PSBs.

While applicable not only to PSBs but also to private sector entities, the NCSC may wish to consider the development of some form of certification requirement relating to the procurement and delivery of services by suppliers to customers to ensure a sufficient level of capability by such suppliers.

Importantly, Microsoft recommends that some form of measure be introduced to better lead or drive the adoption of improved cyber security practices across all PSBs. Certainly, while the NCSC does an excellent job of identifying the right measures to be adopted, there is something of a vacuum in relation to the rapid adoption of such measures, the monitoring of adoption progress, and the

[8] The UCD Centre for Digital Policy presents our cyber security series - UCD Center for Digital Policy

advancement of cyber security maturity in general across PSBs.

In addition, and in relation to Measure 8 (‘*The NCSC will develop a baseline security standard to be applied by all Government Departments and key agencies*’), Microsoft welcomes the proposed further measure to review and update the Standard by Q4 2023 in light of the revisions to the NIS Directive but would also highlight the recent and indeed ongoing updates to the NIST Cybersecurity Framework[9] which should be kept under review and included as appropriate.

5. Skills (s. 9, pp. 24-26)

The proposed measures are appropriate.

Further, the NCSC may wish to consider engagement with industry to extend and complement the existing schools-focused initiatives. For example, the Microsoft Dream Space program[10] already has a number of initiatives including a Dream Space Academy for Primary, a Dream Space Academy for Post-Primary, Dream Space TV, Dream Space Digital Academy, and Dream Space Teacher. Education vehicles such as these, which are primarily focused on building core STEM awareness, could be leveraged to include important cyber security messaging and education.

In addition, industry is also engaged with other educational institutions on cyber security skilling programs, for example, the Microsoft collaboration with the Technical University of Dublin (TUD). The involvement of the NCSC in programs such as these or the adoption and/or enhancement of such programs would go a long way to help address the cyber security skills deficit.

Such additional initiatives could flow from participation by the stakeholders in the ‘Engage industry skills challenge’.

Further, closer industry participation in the both the Strategic Advisory Group of Cybersecurity Research Stakeholders and National Cyber Security Support Centre would yield benefits.

The NCSC may also wish to consider a skills-program specifically targeted at existing staff in PSBs to significantly raise the level of awareness and capability across the Public Sector.

Furthermore, the NCSC may wish to consider a specific skills recruitment program

[9] NIST Cybersecurity Framework 2.0 Concept Paper: Potential Significant Updates to the Cybersecurity Framework

[10] Dream Space - Home (microsoft.com)

aimed at bringing new talent into PSBs. Such a program should have an intake drawn from a wide range of demographics and capabilities, not necessarily having a technology degree as an entry requirement. Such programs have been successfully developed elsewhere on the island with a focus on those from disadvantaged backgrounds, those wishing to return to the workforce, and those with neuro-diverse characteristics[11]

6. Enterprise Development (s. 10, pp. 27-29)

The proposed measures are appropriate.

However, consideration should be given to forging even closer links and alignment with other State entities such as Enterprise Ireland to better support and leverage a developing cyber security SME and start-up ecosystem.

Enhanced cooperation with the Centre of Secure Information Technologies (CSIT)[12] at Queen's University Belfast is recommended given the success that CSIT has enjoyed in developing such an ecosystem.

7. Engagement (s. 11, pp. 30-32)

The proposed measures are appropriate.

Microsoft recommends that closer formal relationships are established with Science Foundation Ireland (SFI). This would have a two-fold benefit: first, identifying opportunities for the NCSC to take advantage research and development activities in the cyber security areas that SFI may undertake, or in the alternative, establishing a well-understood mechanism for developing new research and development projects from well-known funding sources; and second, providing a set of opportunities for SFI to expand its current research and development program.

8. Citizens (s. 12, pp. 33-34)

The proposed measures are appropriate.

Again, the NCSC may wish to give consideration to engagement with industry partners to enhance and extend the reach and impact of the proposed measures,

[11] Minister announces Microsoft to establish Cyber Security Centre in Northern Ireland | Department for the Economy (economy-ni.gov.uk)

[12] CSIT | ECIT | Queen's University Belfast (qub.ac.uk)

either through existing industry capabilities or through new capabilities jointly defined with industry via some form of advisory body.

9. Governance Framework and Responsibilities (s. 13, p. 35)

The proposed measures are appropriate.

Closing

Once again, Microsoft thanks the Department of Communications, Climate Action and Environment for the opportunity to provide our input to this consultation and we welcome follow-up discussions at the Department’s convenience.