Observations and Feedback on the National Cyber Security Strategy From Cyber Cert Labs

General Observations

Alignment with the National Digital Strategy

The alignment of the EU Digital and Cybersecurity strategies ensures that there is cohesion between both, in fact with the Cybersecurity strategy supporting the goals of the digital strategy. The National Digital Strategy was updated in Feburary 2022 and this update to the existing National Cyber Security Strategy (2019 – 2024) should seek to continue to achieve the same alignment.

eHealth

eHealth is specifically called out in the National Digital Strategy as being an area of development in the immediate future. ENISA held a conference in 2022 on eHealth and Cyber security as well as publishing a sectoral review in 2015. Also ENISA published a review on CISRT capabilities in the healthcare sector. A specific working group looking at the unique cyber security challenges in this area could help to provide a framework for all health providers (not just the HSE) to reap the benefits of these developments while at the same time reducing the overall risks in relation to cyber security (note: the section on the CRA may well apply to products and services in this area).

Smart Cities

Just like eHealth the National Digital Strategy points to developments in smart cities, intelligent transport services and 5G connectivity. Together these developments can bring significant benefits to citizens in the context of the infrastructure and services in urban suburban areas. Connected technology could also be an area to develop a specific working group to help ensure that cyber security is included as part of the design, development and operation of these technologies.

New Cyber Regulations

While the Network and Information Security Directive (NIS2) is the backbone of the Cyber Security Strategy in terms of establishing national competent bodies to direct the implementation of the directive, there are other related directives and policies which will need to be considered in the national cyber security strategy into the future. The Digital Operational Resilience Act (DORA), the Cyber Resilience Act (CRA), the Directive on the Resilience of Critical Entities (CRE) and the Joint Communication on EU Policy on Cyber Defence will all be relevant in ongoing evolution of the national cyber security strategy. The updated strategy could reference these documents and point to future strategic initiatives to co-ordinate the integration of these requirements into the national strategy.

DORA

The national competent authority for DORA will likely be the Central Bank of Ireland (CBI) as the act goes further than cyber resilience and encompases the wider aspects of technology and digital resilience. Also the CBI has issued requirements under CP140 - Cross Industry Guidance on Operational Resilience which has similar requirements. Under DORA there are requirements on incident and vulnerability reporting that are similar to NIS2. The strategy could include how the NCSC and the CBI will work together on these overlapping requirements to streamline these reporting requirements.

CRA

The CRA requires certification (under the CE programme) for digital products and services to ensure they meet the technical requirements (to be published) in relation to cyber security. This will require the establishment of both a certification authority and certification bodies. The strategy could include the proposal to create a national framework for both with the National Cyber Competency Centre (NCC) having a role to play in this area.

CRE

The CRE in conjunction with NIS2 place additional cyber security and resilience requirements on Operators of Essential Services (OESs). The NCC could play a role in creating various committees or special interest groups to analyse the different requirements in each sector that these directives apply to. The purpose of these committees or special interest groups would be to develop specific guidance on a national basis for each sector. Linking this with the work that ENISA does through its ad-hoc working groups could help to connect those sectors to other OESs across the EU.

Cyber Defence

The proposed joint policy statement on EU Cyber Defence proposes creating a cyber reserve force through the EU Cyber Solidarity initiative. The strategy could include the establishment of a cyber reserve force that could act at a national level in conjunction with the defence and law enforcement agencies. The recent study by Cyber Ireland has identified that there are approximately 7,500 people working in the cyber security sector in Ireland. If even a small proportion of the sector is interested in volunteer work or through engagement with private enterprises this could unlock a body of talent that could assist with the preparation and response capabilities in the event of serious cyber attack.
For example as an island nation Ireland is particularly vulnerable to threats to our maritime infrastructure which includes the sub-sea cables used to provide almost all of Irelands connectivity to the Internet. Recent exercises by foreign naval forces off the coast of Ireland including vessels capable of cutting sub-sea cables potentially demonstrates that this a real threat. In order to provide adequate defence against this threat will require specific cyber security skills and coordination across a range of organisations.

NIS2

The requirements in NIS2 around vulnerability and incident disclosure as well as the development of Cyber Threat Intelligence (CTI) capabilities provides the base information to develop a national Cyber Threat Landscape (CTL) report. Such a report could provide an

overview of the evolving threat landscape and in conjunction with the previously mentioned special interest groups or committees sector specific threat information. The national CTL would be a good basis for organisations to start mapping their own threat landscape and would be beneficial to the development of CTI capabilities. Also the CTL would inform the cyber risk assessment as part of the overall annual national risk assessment. The strategy could include plans to develop the CTL and to also develop a national CTI capability that all OESs can integrate with.
The NIS2 provides national competent authorities with new powers to ensure that OESs have an adequate level of cyber resilience and security. The national CTL and CTI capabilities would provide a basis for ensuring that this is the case. The strategy could outline how the NCSC will implement these new powers.
Funding for the national cyber security strategy and the NCSC should be based on the nature and level of threats facing the nation. Again the CTL and CTI capabilities could be used as a basis to understand the appropriate level of funding at a national level. The strategy could also incorporate this aspect to the national responsibility under NIS2 to implement the EU Cyber Security Strategy.

Specific Observations

Section 2 - Vision

The actions in relation to Protect, Develop and Engage are perhaps too passive given how the cyber threat landscape has evolved since the strategy was written in 2019. For example the rising threat of ransomware attacks began back in 2016 with a steady rise in different sectors being affected by these attacks. While the HSE attack in 2021 was the most publicised, many other sectors, companies and organisations in Ireland have also been affected.
A more proactive set of objectives could be developed that emphasises the ability to resist and defend against cyber threats so that the impact to the state, public and private sector organisations and the people of Ireland is minimised.
The cyber regulations detailed in the previous section will provide government and the state the ability to ensure that into the future Ireland will continue to develop these capabilities inline with the evolving cyber threat landscape.

Section 3 - Objectives

Following on from the previous section again the objectives could be more proactive. For example in the first objective to update it to include the ability to identify cyber threats in order to prepare for them before they occur. Also perhaps to link this preparation to the EU CyCLONe initiative to continue to run national level incident management testing.
In terms of education and skills perhaps the development of a national cyber security skills framework could be useful. This could be a cross industry and include educational institutions to develop career paths linked to specific cyber security skills.
New emerging technologies such as Cloud Computing, Artificial Intelligence and Quantum Computing have the potential to radically change the cyber threat landscape. Using the NCC

and ad-hoc working groups or committees to prepare for such developments. This could also feed back into the cyber skills framework.

Section 6 - National Capacity Development

The development of the sensor network could be expanded to include active ways that organisations can share technical and tactical threat intelligence from cyber security capabilities within their organisations. Common standards for CTI sharing could be used (STIX/TAXII) which would enable the sharing of common elements such as observables and reports. Some of this information could be used in terms of curated intelligence which in turn would feed into the national CTL report.
Vulnerability management in conjunction with quality CTI can be foundational elements to perform detailed cyber risk assessments (based on credible threat scenarios). This could help to direct organisations to remediate or mitiage vulnerabilities that are on the critical path to serious cyber security incidents. Using technical risk assessments helps to provide concrete remediation actions that the NCSC can track.
The development of a national skills framework in conjunction with a cyber reserve capability would also link with the previous objectives to create a cyber ready capability in the event of a significant incident.

Section 9 - Skills

A lack of sufficient cyber security skills or the application of those skills to national cyber defence is in itself a risk. A national skills framework would provide both a map of required skills against specific cyber security competencies and an ability for orgnisations to develop specific educational and training programmes to meet these needs. Second and third level education may not be the only route to develop the require cyber skills that are needed. For example developing cyber security apprenticeship programmes would allow for developing the much needed hands on experience that organisations need.

Section 10 - Enterprise Development

The NCC could be the right forum to align industry and enterprise with the national cyber security strategy and to allow all sectors to contribute. Of the approximately 7,500 cyber security professionals working in Ireland a significant proportion work in the private sector and are usually part of a wider technology function. Harnessing this pool of talent could be pivotal to making the national cyber security strategy a reality.
As stated previously the CRA will have a significant impact on enterprise development as it will introduce mandatory certification for certain digital products and services. Again the NCC could play a role in preparing companies for this new legislative requirement and help to develop the certification bodies needed.