Vision

- Protect the State, its people and critical national infrastructure from threats in the cyber security realm in a dynamic and flexible manner, and in a way that fully respects the rights of individuals and proportionately balances risks and costs.
- Develop the capacity of the State, research institutions, businesses, the public sector and of the people to both better understand and manage the nature of the challenges we face in this space and to ensure that businesses and individuals can continue to benefit from economic and employment opportunities in information technology, and in particular in cyber security.
- Engage nationally and internationally in a strategic manner, supporting a free, open, peaceful and secure cyber space, and ensuring that cyber security is a key component of our diplomatic posture across the full range of engagement.

Recognising the deterioration in the global cyber threat landscape and our growing reliance on digital technologies across Irish society and the economy, a process accelerated during the COVID-19 pandemic, the vision for this Strategy could be extended to encompass the cyber security of businesses, educational institutions, the community and voluntary sector, as well as households and citizens.

Q: Is the vision in the Strategy still relevant? How should it be updated to reflect recent developments?

It depends what we see as the role of the NCSC. The consultation document feels like a response to international and State-sponsored escalations. What about the growing sophistication of internal capability?

The statement highlighted above could be read to reflect our previous point but could also mean that organisations outside NIS 2 are protected from international actors when possibly the biggest danger is sophisticated internal criminal gangs.

Q: Are the objectives in the Strategy still relevant? How should they be updated to reflect recent developments? Are there new objectives which should be included?

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” should now be strengthened to reflect ensuring that those businesses that hold personal data protect it adequately. This better aligns with GDPR and the NDS’ ambition (5.1 in this document refers but doesn’t deal with detail) to grow the % of businesses that trade online.

Public Sector Data and Networks

An initial point, and relating to something we have increasingly been finding, it whether these requirements are for the full Public Sector (i.e. all organisations funded or part-funded by the taxpayer) or just the Public Service?

We understand that there is a little confusion around the implementation of Measure 8 “The NCSC will develop a baseline security standard to be applied by all Government Departments and key agencies” where the authors saw this as a journey and auditors are seeing this as an “exam pass mark”, which we are informed will be impossible to achieve for many organisations.

Perhaps an additional measure should be an implementation guidance pack? Such a pack should emphasise that the standard is intended to allow organisations to use the implementation as a journey to a mature sustainable security posture.

So we suggest that section 8 includes two further proposals for new measures as follows:

- The steering group or sub group of Government Cyber Security Coordination and Response Network will prepare an implementation guidance note for the standards to include a bar/baseline, context, direction, timelines etc.
- PSBs will be encouraged where feasible to attain and retain recognised industry and international standards e.g. ISO27001; maintained certification against these standards will be taken as evidence of meeting the CS baseline standards.

Obviously, what we are seeking to do is achieve general agreement between service providers, auditors and accounting officers of a general direction that takes the whole of public service to a better place without duplicating cost or effort or creating unattainable short-term targets.

Skills

Should mention building upon the Government ICT Apprenticeship for Cyber Security, which is an excellent initiative.

Should NCSC work with IPA to develop something aimed at Accounting Officers/Senior Public Servants? It is essential they understand NIS2 etc. and are sufficiently aware of risks.

Enterprise Development

As touched on above, time to roll the Baseline Security Standard into (small) business – notwithstanding previous comment about application guide.