Ergo Submission

National Cyber Security Strategy 2019-2024

About Ergo

Ergo is delighted to submit the below response to the National Cyber Security Strategy 2019-2024 mid-term consultation review.

Ergo is the largest privately-owned IT services company in Ireland, headquartered in Dublin, with offices in Cork and Limerick as well as the UK, US, Romania and Columbia. We excel at the intersection of business and technology with market-leading multi-cloud solutions, managed services and IT resourcing. For nearly 30 years, CIOs and IT leaders have relied on Ergo for a powerful combination of agility and resilience – agility to grow and continually improve; resilience to withstand whatever disruption comes next.

2. Vision

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

Response:

Ergo recommend that the National Cyber Security Centre (NCSC) provide clear differentiated guidance and support on a tiered basis for:

- Citizens
- SMEs/Community/Charity Sector
- Larger Organisations
- Public Sector
- Organisations providing Critical National Infrastructure

- There are significant challenges with providing services to these disparate groups. Potentially citizen support (M20) should be provided by another agency, such as Citizens Information. Citizen engagement in particular needs significant improvement across all the state bodies. For example, it is difficult to report cybercrimes digitally.
- DORA regulation and guidance should now be included in the vision.
- NCSC support for Skills, (M12/M13/M14) may be a distraction from its core task of protecting Critical National Infrastructure.
- The National Cyber Security Strategy (NCSS) Vision mentions the future, but the strategy needs to focus on investigating specific topics that will have a significant impact on cyber security, for example, ChatGPT/ OpenAI, quantum computing, blockchain or other emerging technologies. While Ergo appreciates this may be covered by Threat Intelligence, there needs to be a forward looking functional team at the NCSC examining and disseminating information about the potential impact of these technologies on Irelands cyber landscape. (i.e. a research group). This could go out to academia, but there is a need to build up knowledge in these areas and understanding of how they affect cyber security in the medium to long term.

3. Objectives

Question: 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?

Response:

- There should be State-level certification scheme to assess a company's competence/ capabilities in dealing with cyber incidents. e.g. type of incident, size of incident. Having such accreditation in place would allow for companies to quickly identify appropriate measures to help them respond to a serious a cyber incident. For example, like the program available in the UK: https://www.ncsc.gov.uk/information/cir-cyber-incident-response. This scheme in the UK provides customers with assurance that the members of the scheme meet the NCSC's standard for high quality incident response.
- Similarly, the NCSC in Ireland could set up an accreditation scheme for ICT security professionals. Training for this scheme could then be spearheaded by the education (third level and professional development bodies) and private sectors.

4. Evolving Global Cyber Risk

No Question

Response:

- Ergo recommends that the ENCIT focuses on awareness and bringing a set of actions/ outcomes to NCSC.
- Ireland's telecoms sector is an industry that impacts business and citizens greatly. However, the sector is not providing enough assistance to report, block or prevent instances of smishing/ vishing. Statistics and monitoring of abuse are necessary at a state level
- It would be very beneficial to see a list of the biggest cyber threats to Ireland, similar to the ENISA Threat Landscape report. This could include a table of how many cyber-attacks were reported in Ireland, the most prominent causes, and the type of threat experience.
- There also should be more detail here on what to expect with upcoming EU regulations and acts such as DORA. The NCSC should be actively working to provide artifacts to help prepare Irish businesses.

5. Policy Developments

No Question

6. National Capacity Development

Question: Are the proposed measures appropriate and relevant to the current situation? Are there further proposals which should be considered? Which, if any, proposals should be prioritised?

Response:

- We suggest that there is a more detailed explanation developed as to the exact role of the National Security Analysis Centre, as well as its relationship with the NCSC.
- There is no detail of OGCIO in any of the above strategy aims. We would suggest that their role and relationship with NCSC is outlined and clear roles and responsibilities are established between the two bodies.

7. Critical National Infrastructure Protection

Question: Are the proposed measures appropriate and relevant to the current situation? Are there further proposals which should be considered? Which, if any, proposals should be prioritised?

Response:

- Measure 4: We would suggest that a civil body be established and responsible for conducting cyber risk assessments for civil agencies that can work in tandem with the Gardai
- Measure 6 – Threat sharing with the wider industry should be further developed (e.g an alerts system)
  - A Risk Assessment framework (including timelines) needs to be firmly established and published, for example how the NCSC Vulnerability Assessment will be rolled out and if the industry partners will get the opportunity to participate in this programme, as it is unlikely NCSC will have adequate resources to do this in-house.
  - Alternatively, industry may wish to conduct their own risk assessments internally. It would seem more appropriate for NCSC to come up with a certification programme to validate that business partners have the skills and expertise to conduct a standard risk assessment process for Critical Infrastructure. Putting in place a certification programme would be an appropriate measure to fast-track this whole process.

8. Public Sector Data and Networks

Question: Are the proposed measures appropriate and relevant to the current situation? Are there further proposals which should be considered? Which, if any, proposals should be prioritised?

Response:

- Measure 8 includes no mention of VM images or other mechanisms to standardise and streamline baselines. This needs to be automated wherever possible. e.g. with full use of standard VM images.
- There is also a need for a specific set of cloud security standards to be established.

9. Skills

Question: Are the proposed measures appropriate and relevant to the current situation? Are there further proposals which should be considered? Which, if any, proposals should be prioritised?

Response:

- There is no pathway or measures outlined for upskilling experienced ICT staff into cyber-specific roles. We would suggest that this be included.
- The roles and responsibilities of the NCSC and its relationship with other government agencies should be very clearly defined.

10. Enterprise Development

Question: Are the proposed measures appropriate and relevant to the current situation? Are there further proposals which should be considered? Which, if any, proposals should be prioritised?

Response:

- We would suggest that references to Cyber Ireland events are included.
- As previously mentioned, the establishment of a National Cyber Innovation Hub may potentially be better managed by a different state agency than the NCSC.
- Ergo is of the opinion that the establishment of a National Cybersecurity Certification Authority function at NCSC is fully in line with international best practices and we look forward to hearing more about this development in future.

11. Engagement

Question: Are the proposed measures appropriate and relevant to the current situation? Are there further proposals which should be considered? Which, if any, proposals should be prioritised?

Response:

- There is little mention of data governance or establishing best practices around data governance. There is an increasing convergence of ICT systems and data governance-type systems which should be a separate measure.
- On a similar note, this could also include data governance in the cloud, to include security guidance for data residency.

12. Citizens

Question: Are the proposed measures appropriate and relevant to the current situation? Are there further proposals which should be considered? Which, if any, proposals should be prioritised?

Response:

- Measure 20 should include working closely with Citizens Information Ireland to provide information on cyber security to citizens on an already trusted platform.
- This strategy makes little reference to privacy concerns. It may be worth investigating if there is an opportunity for the NCSC to work with the Data Protection Commission?

13. Governance Framework and Responsibilities

Question: Are the proposed measures appropriate and relevant to the current situation? Are there further proposals which should be considered? Which, if any, proposals should be prioritised?

Response:

- Will the National Standards Authority of Ireland be involved in the planned rollout of the National Certification Authority for certification schemes pursuant to the European Cybersecurity Act?
- Ergo recommends that there is a central source provided to citizens and business that lists all cyber resources available through Government and EU initiatives. This document 'NCSS Consultation paper' references multiple resources, bodies, regulations, frameworks etc. These can be overwhelming. A clear messaging campaign to direct organisations (public and private) and

citizens to one location where they can begin their search for information most relevant to their circumstance would be most useful.

- For example – If a citizen wants to ask something like: I think my data has been stolen, what can I do? There should be an easy and simple way to find these resources.