Press release

National Cyber Risk Assessment published by Government

From Department of the Environment, Climate and Communications (/en/organisation/department-of-the-environment-climate-and-communications/)
Published on 21 June 2023
Last updated on 17 July 2023

The Minister for the Environment, Climate and Communications, Eamon Ryan, and Minister of State with responsibility for Communications, Ossian Smyth, have today published the National Cyber Risk Assessment 2022, (/en/publication/5a871-national-cyber-risk-assessment-2022/) which outlines the cyber security risks faced by Ireland and the measures required to strengthen our cyber resilience.

This report, led by the National Cyber Security Centre (NCSC), includes an analysis of the risk that Ireland faces from a range of threats such as espionage and destructive cyber attacks posed by nation state actors, criminal organisations and hacktivist groups. The report also highlights the importance of supply chain security in digital technologies, which has become a key focal point of cyber risk in recent years.

The report makes three key recommendations to strengthen the cyber resilience of Ireland's critical national infrastructure (CNI)* and services, and to mitigate systemic cyber risks in the State:

1. Strengthen legislative provisions to ensure that the operators of essential and important services, service providers, and technology vendors embed appropriate cyber security measures in their products and services from the outset

2. Develop a framework to manage strategic supply chain dependency risks for critical and sensitive services

3. Establish a central register of all essential and important entities in the State

The report supports the ongoing development of measures to strengthen cyber resilience within Ireland's CNI. It does this by identifying pathways that could lead to systemic cyber risks — which have the potential to adversely affect the State's essential services.

Speaking upon the publication of the report, Minister Ryan stated:

> "We've taken the decision to publish the National Cyber Risk Assessment, which was drafted in 2022, to inform people of the cyber risks Ireland faces.

> "Today's increasingly inter-connected world is dependent on digitalised processes, and it is vital that we work cohesively to ensure there is a high-level of cyber resilience across the State's critical services. This can be achieved through a number of measures, including by strengthening the potential for current and upcoming cyber security-related statutory regulations.

> "By examining potential cyber-risks across a range of sectors, this work provides an invaluable insight into an ever-evolving geo-political and technological environment and protects against potential threats posed. The report was carried out by my department's National Cyber Security Centre (NCSC), with the assistance of the Defence Forces and An Garda Síochána, along with other members of the report's steering group."

Minister of State Smyth added:

> "The cyber risks facing a country, economic sector or individual party are intertwined with each other and with other types of risks. As a response to the pandemic, there was a rapid acceleration in the digitalisation of commercial, educational and social activities, which allowed these activities — which would otherwise have stalled — to continue.

> "A large-scale digital breakdown post pandemic could cause more societal harm than it otherwise might have pre-pandemic, further underscoring the importance of robust cyber resilience across all sectors. The publication of today's report provides a robust assessment of systemic cyber risks."

The completion of a National Cyber Risk Assessment was one of the key measures identified in the National Cyber Security Strategy 2019-2024. (https://www.ncsc.gov.ie/pdfs/National_Cyber_Security_Strategy.pdf) Measure four of the strategy stated that the National Cyber Security Centre (NCSC), with the assistance of the Defence Forces and An Garda Síochána, perform a detailed cyber security-focused risk assessment of all critical national infrastructure (CNI) within the State.

The National Cyber Risk Assessment 2022 report was prepared by the NCSC, with the assistance of a steering group consisting of members from An Garda Síochána, the Office of Emergency Planning, the Defence Forces, the National Security Analysis Centre, the Central Bank of Ireland, the Commission for Regulation of Utilities (CRU), and the Commission for Communications Regulation (ComReg).

The report can be viewed and downloaded on the Department of the Environment, Climate and Communications website. (/en/publication/5a871-national-cyber-risk-assessment-2022/)

*Critical National Infrastructure are the essential systems that underpin the daily life of a country, essentially enabling it to function in as smooth a manner as possible. The areas traditionally considered as CNI include the energy, transport, financial services, healthcare and telecommunications sectors, along with the government IT systems that deliver many of these services.

Notes

National Cyber Security Centre (NCSC)

The National Cyber Security Centre (NCSC) was founded in 2011 and is an operational cyber security unit within the Department of the Environment, Climate and Communications. The NCSC is responsible for advising and informing Government, critical national infrastructure providers, business and the general public of current threats and vulnerabilities associated with network information security.

The main roles of the NCSC are to lead in the management of major cyber-security incidents across Government, provide guidance and advice to citizens and businesses on major cyber-security incidents, and develop strong international relationships in the global cyber-security community for the purposes of information sharing.

Cyber risks

Digital services, processes and systems are part of a larger whole; the global digital domain. The 2008 financial crisis and the 2020 COVID-19 pandemic show that certain events can rapidly have a global impact on other domains and strike at the heart of society and the economy. This is also true for cyber incidents and especially so when incidents occur on a large scale and in conjunction with other incidents. For example, a combination of a large-scale cyber incident and the COVID-19 pandemic had major consequences in the health sector.

As a response to the pandemic, there was a rapid acceleration in the digitalisation of commercial, educational and social activities, which allowed these activities (which would otherwise have stalled) to continue. The flip side of this is the unprecedented and rapid change across society, which has ushered in new ways of working; and social, educational, and commercial interactions that are increasingly underpinned to a large extent by the digital domain. A large-scale digital breakdown post pandemic could cause more societal harm than it otherwise might have pre pandemic, further underscoring the importance of robust cyber resilience across all sectors.

Practically all critical processes and services are entirely dependent on ICT. Due to a significant reduction in analogue or manual alternatives and the absence of fallback options, dependence on digitised processes and systems has increased to such an extent that any impairment to these systems and processes can cause socially disruptive damage.

Geo-political developments can also affect cyber risks due to the concentration of companies producing key technologies such as 5G communications systems, cloud computing, artificial intelligence and semi-conductor production in territories outside of the EU. This can lead to over-reliance on supply chains for key technologies which could be adversely affected by geopolitical developments such as trade sanctions, regional conflicts or national strategic interests.

There is a high dependency on a relatively small number of providers of hardware and software, cloud services, and service providers, with a significant reliance on service suppliers outside of the State.

Part of

Policies

Communications and Digital (/en/policy/435802-communications-and-digital/)

Accessibility (/en/help/accessibility/)

Privacy policy (/en/help/privacy-policy/)

Who does what (/en/help/e170a-who-does-what/)

Rialtas na hÉireann
Government of Ireland

Manage cookie preferences

Manage preferences