NIS and NIS2

National Cyber Security Centre

with
Donal Carroll

NCSC – Who are we?

- Found in 2011 – Staff based on UCD campus
- Part of the Department of Environment, Climate & Communications (DECC)
- Responsible for advising and informing Government and Critical National Infrastructure of current cyber security threats
- Managing and assisting in cyber security incidents across government
- Provide guidance and advice to citizens and businesses
- Government accredited CSIRT as part of CSIRTs network
- National compotent authority under EU directive 2016/1148 as the primary point fo content for receiving notification of national incidents
- Feed into the Nation Emergency Coordination Centre during national cyber incidents

Donal Carroll – Who am I?

- Operations team of the NCSC (GovCSIRT)
  - Risk Operations
- Previous experience
  - Incident response management
  - SOC engineering (SOAR, SIEM development)
  - DevOps
- Reserve Defence Forces (Communications and Information Services)

Network and Information Systems
- Directive EU 2016/1148

What are the origins of NIS?

" In 2013, the Commission released the Cybersecurity Strategy of the EU, which laid out a number of fundamental principles underlying the EU approach to cybersecurity, followed by 5 strategic priorities. The proposal for the NIS Directive is made under the first strategic priority 'Achieving Cyber resilience' "

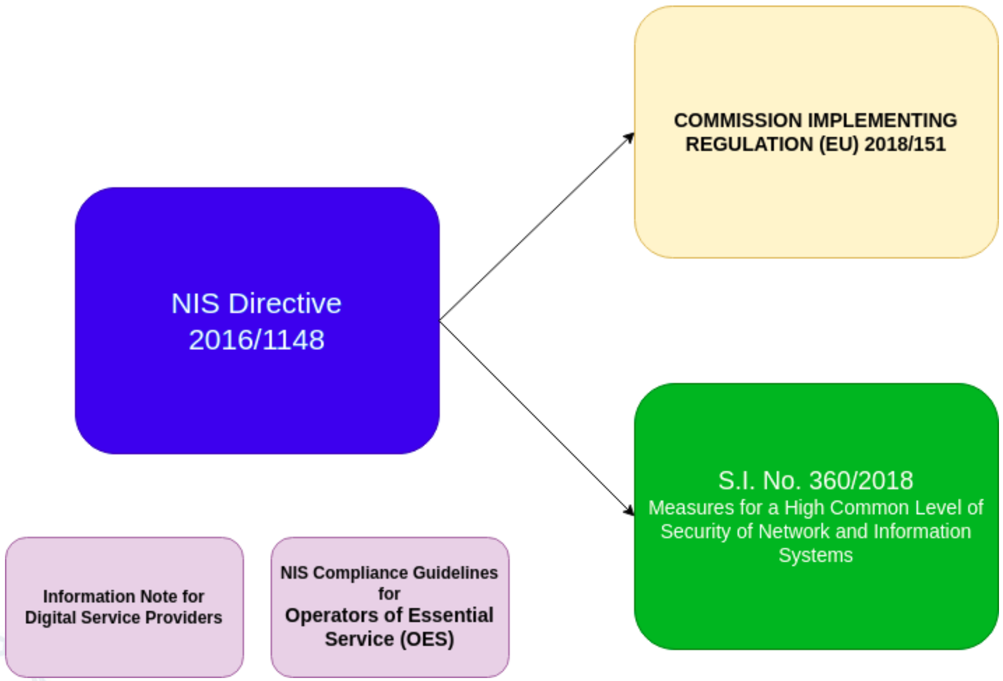
- 2009 publication by the EU Commission:
  "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"

Source: www.enisa.europa.eu

Network and Information Systems - Directive EU 2016/1148

- **Improving Cybersecurity:** improve the overall level of cybersecurity within the European Union targeting critical services in partical
- **Ensuring Security of Essential Services:**
  - Utility – Water, Energy
  - Transport – Shipping, rail, road, air
  - Finance - Banking
  - Health – Hospitals & other health care providers
- **Promoting Cooperation:** Establishes a framework for collaboration, ensuring that relevant authorities and entities are working together to prevent and respond to cybersecurity incidents effectively.
- **Risk Management:** It promotes a risk-based approach to cybersecurity, encouraging organizations to assess and manage their cybersecurity risks.

Network and Information Systems
- Directive EU 2016/1148



Network and Information Systems
- Directive EU 2016/1148

- Designation of National Compotent Authorities:
  - Minister for Communications, Climate Action and Environment for alll sectors excluding banking and finance
  - Central Bank of Ireland – banking and finance

Network and Information Systems – Who it affects

- **(OES) Operators of Essential Services:**
  - Energy: (ESB, Gas Networks Ireland, Bord Gais etc)
  - Transport: (Iarnrod Eireann, CIE, DAA)
  - Banking: (Central Bank of Ireland, BOI, AIB, KBC, PTSB)
- **(DSP) Digital Service Providers:**
  - Cloud service providers: Microsoft, Google, Amazon
  - Online market places, Search engines, e-commerce platforms

Network and Information Systems – What are their obligations

- **Incident reporting**: They must report on incidents of “significant impact” which are sufficient “size”

- **Security measures**: They must implement security measures to ensure the resilience of their networks and information systems.

- **Cooperation**: OES and DSPs are expected to cooperate with the compotent national authorities sharing information and collaborating on matters related to cyber security

Network and Information Systems – Consequences

NIS Directive 2016/1148 (EU) – Article 21

"Member States shall lay down the rules on penalties applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive. Member States shall, by 9 May 2018, notify the Commission of those rules and of those measures and shall notify it, without delay, of any subsequent amendment affecting them."

NIS Directive points 2016/1148

- First iteration of a common cyber security policy across the EU

- Puts much of the definition onus on EU member states
  - Penalties
  - Security controls
  - OES

- No mention of thresholds for legal terminology
  - Significant impact
  - Size and reach

- None specific and high level. Vague use of language

- Operationally challenging to implement

NIS2 vs NIS (Motivation)

Why create a new NIS directive?

- Insufficient level of cyber resilience of businesses operating in the EU
- Inconsistent resilience across Member States and sectors
- Insufficient common understanding of the main threats and challenges among Member States
- Lack of joint crisis response

Source: https://digital-strategy.ec.europa.eu

NIS2 vs NIS (Objectives)

- **Strengthen security measures**: Enhancing the overall cybersecurity posture of essential entities.
- **Harmonizing obligations:** Establishing uniform incident reporting requirements to improve transparency and enable a coordinated response to cyber threats
- **Expanding the scope of regulation:** Covering a wider range of sectors and digital service providers, reflecting the evolving nature of cyber risks.
- **Cooperation:** Strengthening national supervisory measures and fostering EU-wide collaboration to effectively respond to cyber incidents.

NIS2 vs NIS (Scope)

- Additional sectors and entities defined
- Clarity on business category thresholds
- Breakdown into additional categories
  - Essential (>= 250 employees or €50 million+ revenue)
  - Important (40 – 249 employees or €10 million+ revenue)
  - Not in scope
- High criticality sectors (deemed essential)
  - Food production/distrubition
  - Postal services
  - Manufacturing
  - Research
  - Biochemical
- Removal of language such as OES and DSP
  - Replaced by Essential and Important Entities

NIS2 vs NIS (Incidents)

24h — **EARLY WARNING**
Is it a suspected malicious act with potential cross-border impacts?

72h — **OFFICIAL INCIDENT NOTIFICATION**
Assessment of the incident, severity and impact, plus indicators of compromise.

as requested — **INTERMEDIATE STATUS REPORT**
At the request of CSIRT or relevant competent authority.

1 month — **FINAL REPORT**
Or if incident ongoing at time of final report a progress report
and final report 1 month after end

NIS2 vs NIS (Enforcement)

- Warnings issued for non-compliance
- Binding instructions can be issued
- Cease conduct orders for non-compliance
- Reporting on risk management measures
- Order to inform on cyber threats
- Designated monitoring officer (similar to DPO)
- Order to make public non-compliance
- Cessation of certification for essential entities

NIS2 vs NIS (Penalties)

- **Essential Entities:**
  - Maximum of up to €10,000,000
  - Or 2% of total worldwide turnover

- **Important Entities:**
  - Maximum of up to €7,000,000
  - Or 1.4% of total worldwide turnover

- Now on par with GDPR fine structure

NIS2 vs NIS (Risk Management)

Clearer guidelines on assessment categories

- Risk analysis & information system security
- Incident handling
- Business continuity measures
- Supply Chain Security
- Vulnerability handling and disclosure
- Policies and procedures on cybersecurity
- Basic computer hygiene and trainings
- Policies on appropriate use of cryptography and encryption
- Human resources security, access control policies and asset management
- Use of multi-factor, secured voice/video/text comm & secured emergency communication

NIS2 Readiness for businesses – What's needed

Conduct a cyber security risk assessment	Have an incident response plan
Have implemented security controls	Be aware of have established reporting mechanism
Have awareness of the compotent authority	Supply chain security*
Documentation & recording of cyber security strategy	Training & awareness
Legal compliance	Monitoring & auditing

NIS2 - Key dates

- December 14th, 2022 – NIS2 Directive published
- January 16th, 2023 – NIS2 adopted by the European Union
- October 17th 2024 - EU member states must include it within their national legislation
- January 17th 2025 – Establishment of of the Cooperation group and CSIRT peer reviews
- April 17th 2025 – Establishment of essential and important entity list within Member states
- October 17th 2027 – NIS2 Directive review

NIS2 – Relationship to other legislation

- **Digital Operational Resilience Act (DORA)** – specific to the Financial sector. More specific measure around ICT protection. Enforced from January 2025. Compotent authority is the Central Bank of Ireland
- **Cyber Resilience Act** – Manufacturing industry. Supply chain focused. Aim addressing specific risk areas. Providers of national digital infrastructure. Cyber Resilience Act applies to radio equipment in scope of the Delegated Regulation adopted under the Radio Equipment Directive 2014/53/EU
- **GDPR** – works in parrellel to NIS2. GDPR safeguards the rights of peoples data. NIS2 works to enhance the security on which this data is stored

Legislation hiearchy

Overarching Principles	NIS 1 & 2
Sector specific	DORA, CRA
National Implementations	SI 360/2018

NIS2 – Summary

- NIS 1 replaced NIS 2 in December 2023
- National transposition on October 17th 2024
- Aims at building on work done by NIS in terms of enhancing national cyber security measures
- Clarifies areas of ambiguity around business thresholds
- Removes the language around OES and DSP, replaced by Essential and important identities
- Introduces larger fines and stricter regulatory penalties in line with GDPR
- Aims to further enhance the cyber resilience of the EU

Questions