Topic 4

EU Directive 2022/2225
Network Information System v2 (NIS2)

Dr Diarmuid Ó Briain

Version: 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

Illustration Index

1 Introduction

The Network Information Systems 2 (NIS2) Directive [1] seeks to further enhance the work started in the NIS Directive [2] to build a high common level of cybersecurity across the European Union (EU). It places obligations on Member States and individual companies in critical sectors. NIS2 adds more sectors, more entities, New methods of selection and registration, New incident notification deadlines and extra requirements based on the learnings from the implementation of the initial directive.

1.1 Objectives

By the end of this topic, you will be able to:

- Understand the key objectives of the NIS2 directive
- Identify the key pillars of the NIS2 directive
- Understand the categorisation of essential and important entities under the NIS2 directive
- Recognise the incident notification obligations under the NIS2 directive
- Evaluate the requirements of organisation to comply with the NIS2 directive.

2 Introduction

The open market nature of the EU facilitates organisations to operate across EU member states within a single market. In terms of Cybersecurity organisations operated differing requirements and standards from member state to member state. As the cybersecurity requirement increased and lack of a standard approach by member states, particularly in the case of Critical National Infrastructure (CNI), the European Union (EU) responded with the Network and Information Systems (NIS) Directive 2016/1148 [2] which was published in the Official Journal of the EU in July 2016. This was transposed into member states law, in Ireland's case on 18/9/2018 via Statutory Instrument No. 360 of 2018. The directive is a framework that brings all entities to a common level of security no matter which state, or states, within the EU they operate in, therefore protecting CNI, the consumer, companies, states and the market alike. The directive focused on two specific groups; Operators of Essential Services (OES) and Digital Service Providers (DSP). However, this first NIS Directive had certain limitations. The digital transformation of society, intensified by the COVID-19 crisis, has expanded the threat landscape. New challenges appeared, which required adapted and innovative responses.

The introduction of the NIS2 2022/2225 [3] directive broadened the scope of the original directive. It identifies 10 sectors of high criticality and 7 other critical services. Entities in both categories will have to meet the same requirements. However, the distinction will be in the supervisory measures and penalties.

3 The three main pillars of NIS2

Figure 1: The three main pillars of NIS2

The three pillars of NIS2, as illustrated in Figure 1, support the EU collaborative approach to Cybersecurity. The figure depicts the shared responsibilities of Member States, National Authorities (NAI), and Essential entities and Important entities. It highlights the collaborative approach that is essential for achieving the directive's goal of enhancing cybersecurity in the EU.

Member States play a crucial role by implementing the NIS2 directive through designating and establishing individual NAI, such as the National Cyber Security Centre (NCSC) in Ireland and identifying and categorising both Essential and Important Digital Service Providers, as well as developing national cybersecurity strategies. They also monitor the cybersecurity performance of Essential and Important entities and enforce the directive's requirements.

NAIs are the frontline enforcers of the NIS2 directive within their respective jurisdictions. They work closely with Member States to identify and categorise Essential and Important entities, monitor their cybersecurity practices, and investigate any reported incidents.

Essential and Important entities are the private sector entities that are subject to the NIS2 directive's requirements. They must conduct cybersecurity risk assessments, implement appropriate security measures, establish incident response plans, and notify NAIs of significant cybersecurity incidents.

The figure also emphasises that effective cybersecurity requires a collective effort from all stakeholders. Member States, NAIs, and Essential and Important entities must work together to identify, assess, and mitigate cybersecurity risks, and to respond promptly and effectively to any incidents that occur.

By promoting collaboration and accountability in this way the NIS2 Directive aims to create a more resilient cybersecurity landscape that can protect critical infrastructure and safeguard the digital economy.

- Coordinated Vulnerability Disclosure (CVD)
- European Cyber Crises Liaison Organisation Network (EU-CyCLONe)
- European Union Agency for Cybersecurity (ENISA)

4 Essential and important entities

"*Entities may be designated as "Essential" or 'Important" depending on factors such as size, sector and criticality.*"

For the purpose of compliance with cybersecurity risk-management measures and reporting obligations entities are classified into two categories, essential entities and important entities that reflects the extent to which they are critical as regards their sector or the type of service they provide, as well as their size. Essential entities will be required to meet supervisory requirements, while important entities will be subject to ex-post supervision, meaning that in case authorities receive evidence of non-compliance, action is taken.

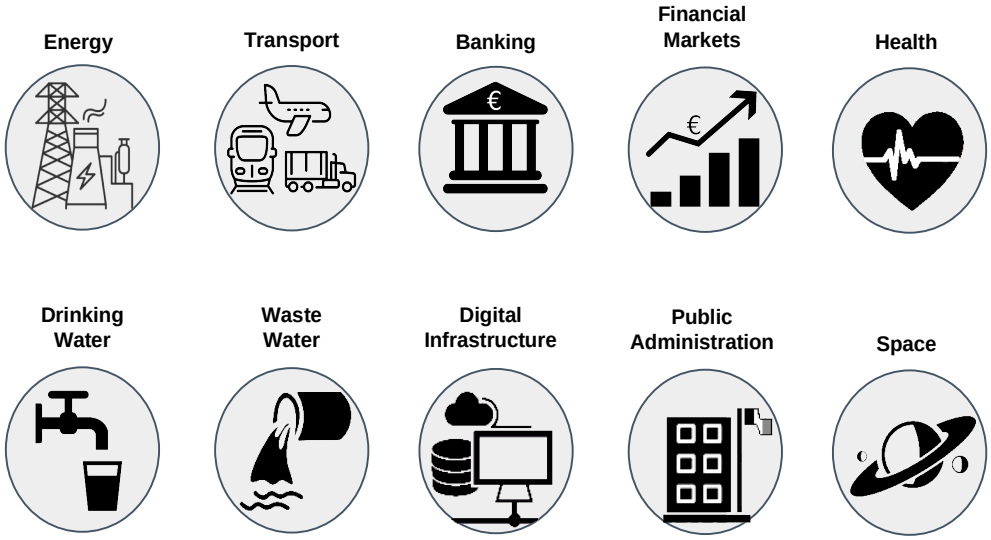

Figure 2: Sectors of High Criticality

4.1 Sectors of high criticality

As illustrated in Figure 2, energy, transportation, banking, and financial market infrastructure are among the sectors of high criticality identified by the NIS2 directive. These sectors are considered essential for the smooth functioning of the EU economy and society, and they are therefore subject to more stringent cybersecurity requirements under the NIS2 directive. These are detailed below:

1. **Energy**
   - Electricity
   - District heating and cooling
   - Oil
   - Gas and hydrogen

2. **Transport**
   - Air
   - Rail
   - Water
   - Road
3. **Banking**
4. **Financial market infrastructures**
5. **Health**
   - Manufacturers of pharmaceutical products including vaccines
6. **Drinking water**
7. **Waste water**
8. **Digital infrastructure**
   - Internet eXchange Points (IXP)
   - Domain Name System (DNS) service providers
   - Top Level Domain (TLD) name registries
   - Cloud computing service providers
   - Data centre service providers
   - Content delivery networks
   - Trust service providers
   - Providers of public electronic communications networks and publicly available electronic communications services
   - Information Communications Technology (ICT) service management (managed service providers and managed security service providers)
9. **Public administration**
10. **Space**.

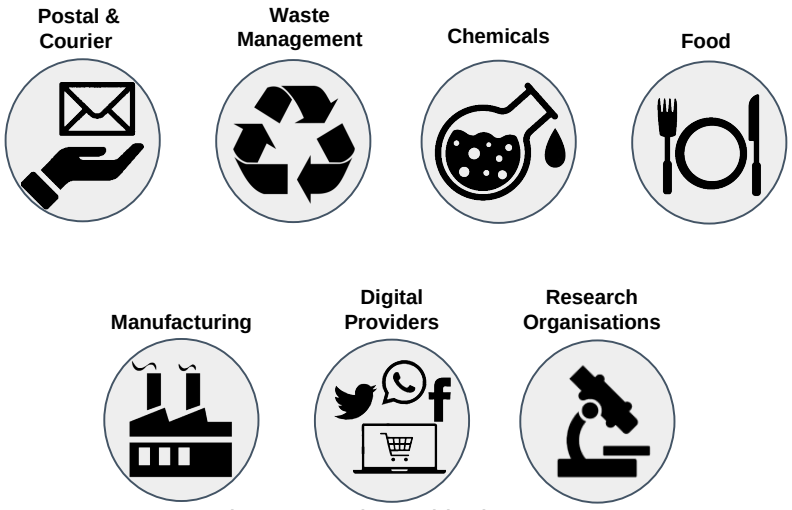

Figure 3: Other critical sectors

4.2 Other critical sectors

As illustrated in Figure 3, postal and courier services, waste management, manufacturing, production, and distribution of chemicals are among the Other critical sectors identified by the NIS2 directive. These sectors are considered to have a significant impact on the EU's security, public health, or economic and social well-being, and they are therefore subject to cybersecurity requirements under the NIS2 directive.

Apart from Digital providers, all of these sectors are newly incorporated into the NIS2 scope. These are detailed below:

1. **Postal and courier services**
2. **Waste management**
3. **Chemicals**
4. **Food**
5. **Manufacturing**
    - Medical devices
    - Computers and electronics
    - Machinery and equipment
    - Motor vehicles
    - Trailers and semi-trailers
    - Other transport equipment
6. **Digital providers**
    - Online market places
    - Online search engines
    - Social networking service platforms)
7. **Research organisations**.

5 Incident Notification

NIS2 imposes notification obligations in phases, for incidents which have a 'significant impact' on the provision of their services. These notifications must be made to the relevant NAI or Computer Security Incident Response Team (CSIRT).

5.1 Incident reporting obligations

Every Member State has a central point of contact for compliance with the Directive and a coordinating CSIRT for incident reporting or an NAI. In Ireland, this is the role of the CSIRT Ireland (CSIRT-IE) within the NCSC, the NAI.

Every incident with significant impact should be notified by the essential and important entities without undue delay. In that regard, the Directive encourages Member States to simplify the incident reporting process by implementing a single entry point for incidents to reduce the administrative burden, including for cross-Member State incidents.

The NAI or its CSIRT, is required to report to the European Union Agency for Cybersecurity (ENISA) on incidents in their jurisdiction every three months, using anonymised information. ENISA will consolidate the information in the form of a report to be published every six months on the EU incidents [4]. This reporting will help organisations and the Member States to learn from other incidents and is a crucial change in the new NIS2 Directive.

Time	Incident reporting
Within 24 hours	**Early Warning** should be communicated, as well as some first presumptions regarding the kind of incident
After 72 hours	**Official Incident Notification** A full notification report must be communicated, containing the assessment of the incident, severity and impact and indicators of compromise.
Upon Request	**Intermediate Status Report** At the request of CSIRT or relevant competent authority.
After 1 month	**Final report** must be communicated.
Every 3 months	Member states CSIRT reports incidents to ENISA.
Every 6 months	ENISA reports on all incidents EU wide.

Figure 4: NIS2 Incident reporting deadlines

6 Cyber Security Risk Management Measures

"*Essential and Important entities must take appropriate and proportional technical, operational and organisational measures to manage the risks posed to the systems*."

Essential and Important entities must take appropriate and proportional technical, operational and organisational measures to manage the risks posed to the systems which underpin their services, and prevent or minimise the impact of incidents on their and other services.

Such measures shall be based on an all-hazards approach that aims to protect the network and information systems and the physical environment of those systems from incidents, and must include at least the following:

1. Risk analysis & information system security
2. Incident handling
3. Business continuity measures (back-ups, disaster recovery, crisis management)
4. Supply Chain Security
5. Security in system acquisition, development and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk management measures
7. Basic computer hygiene and training
8. Policies on appropriate use of cryptography and encryption
9. Human resources security, access control policies and asset management
10. Use of multi-factor, secured voice/video/text comm & secured emergency vulnerability handling and disclosure measures communication.

All measures must be:

- Proportionate to risk, size, cost, and impact & severity of incidents
- Take into account the state-of-the-art, and where applicable relevant European and international standards.

To ensure appropriate risk management measures are in place the EU can:

- Carry out risk assessments of critical ICT services, systems or supply chains
- Impose certification obligations (delegated acts)
- Adopt implementing acts laying down technical requirements.

7 Infringement Penalties

NIS2 introduces stricter penalties for non-compliance by entities. NAIs are granted a minimum list of enforcement powers for non-compliance through the directive, including:

- Issue warnings for non-compliance
- Issue binding instructions
- Order to cease conduct that is non-compliant
- Order to bring risk management measures or reporting obligations in compliance to a specific manner and within a specified period
- Order to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat
- Order to implement the recommendations provided as a result of a security audit within a reasonable deadline
- Designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance
- Order to make public aspects of non-compliance
- Impose administrative fines
- An essential entities certification or authorisation concerning the service can be suspended, if deadline for taking action is not met
- Those responsible for discharging managerial responsibilities at chief executive officer or legal representative level can be temporarily prohibited from exercising managerial functions (applicable to essential entities only, not important entities).

There are particularly high penalties for infringements of:

- Article 21 Cybersecurity risk-management measures
- Article 23 Reporting obligations

In these cases essential entities can be fined up to €10,000,000 or at least 2% of the total annual worldwide turnover in the previous fiscal year, whichever amount is higher while important entities can be penalised by fines of up to €7,000,000 or at least 1.4% of the total annual worldwide turnover, whichever amount is higher.

8 Management Responsibilities

"*Senior management have ultimate responsibility for cybersecurity risk management in essential and important entities*"

Senior management have ultimate responsibility for cybersecurity risk management in essential and important entities. Failure by management to comply with NIS2 requirements could result in serious consequences, including liability, temporary bans and administrative fines as provided for in the implementing national legislation.

Management bodies of essential and important entities must:

- Approve the adequacy of the cybersecurity risk management measures taken by the entity.
- Supervise the implementation of the risk management measures.
- Follow training in order to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the entity.
- Offer similar training to their employees on a regular basis.
- Be accountable for the non-compliance.

9 Bibliography

[1] Directive (EU) 2022/2555, *EU Measures to ensure a high common level of cybersecurity in the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing the Directive (EU) 2016/1148 (NIS 2 Directive)*. 2022, p. 73. Accessed: Aug. 08, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[2] Directive (EU) 2016/1148, *EU Measures for a high common level of security of network and information systems across the Union*. 2016, p. 30. Accessed: Jun. 09, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[3] Directive (EU) 2022/2555, *Measures for a high common level of security of network and information systems across the Union*. 2016, p. 30. Accessed: Aug. 08, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148

[4] ENISA, 'ENISA Incident Reporting', NIS Incident Reporting. Accessed: Aug. 12, 2023. [Online]. Available: https://www.enisa.europa.eu/topics/incident-reporting/