INTRODUCTION TO NIS2 & DORA

STEVE PURSER

CSPRO SERVICES

STEVE.PURSER@PROTONMAIL.COM

Agenda

- Trends in EU Cybersecurity Policy
- Directives & Regulations
- Background to NIS2 and DORA
- Similarities
- Specifics of NIS2
- Specifics of DORA
- Implementation Tips

Trends in EU Cybersecurity Policy (I)

- Cybersecurity legislation is on the increase globally.
- EU examples include the NIS Directive, NIS2, the Cybersecurity Act, DORA and the CRA. There is also a proposal for a regulation on Artificial Intelligence.
- Other important EU legislation references cybersecurity (notably the GDPR).
- The US has issued two Executive Orders in the last few years in the area of cybersecurity.
- This will present a challenge to global companies that will need to be compliant with several different legal regimes.
- The private sector will play an important role in advising governments on the consequences of such legislation.

Trends in EU Cybersecurity Policy (II)

- We also start to see legislation that is referencing specific technologies.
  - E.g. “Security of Connected Devices,” Cal. Civil Code §§ 1798.91.04-1798.91.05(b)
- There are several challenges with such an approach:
  - Technology evolves quickly, whereas legal systems tend to develop slowly – technological references might become irrelevant.
  - Definition of terms is important in legal texts, but this is difficult for evolving technologies.
  - Technology specific legislation might have unintended impacts on the market and introduce unintentional bias.
  - In many cases, ‘soft law’ is a good alternative to legislation.

Agenda

- Trends in EU Cybersecurity Policy
- Directives & Regulations
- Background to NIS2 and DORA
- Similarities
- Specifics of NIS2
- Specifics of DORA
- Implementation Tips

Important Terminology

- In this presentation, we will discuss two types of legislative instrument:
- A Regulation is a piece of legislation that applies to all Member States, in the same form, the day it comes into force.
  - DORA is a regulation.
- A Directive is a piece of legislation that must be transposed into national law before it comes into force – the text therefore differs slightly between Member States.
  - NIS2 is a directive.

Agenda

- Trends in EU Cybersecurity Policy
- Directives & Regulations
- Background to NIS2 and DORA
- Common Goals
- Specifics of NIS2
- Specifics of DORA
- Implementation Tips

Commission Communication COM(2009)149

- "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience".
- The origins of all the instruments underlying the current approach to Critical Information Infrastructure Protection (CIIP) can be found in this paper.
- Published shortly after the large-scale cyber-attacks targeting Estonia in 2007 and the breaks of transcontinental cables in 2008.
- Actions designed to execute in parallel to the European Program for Critical Infrastructure Protection (EPCIP)

Evolution of Supporting Mechanisms

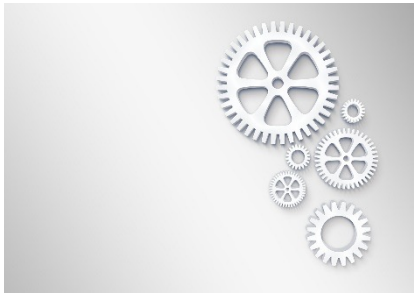
COM(2009)149 NIS Directive

EFMS → NIS Platform → Cooperation Group

N/G CSIRTS Cooperation → CSIRTs Network

EP3R → ?

The NIS Directive



- Scope: to achieve a high common level of security of NIS within the Union
- Provisions:
  - Improved cybersecurity capabilities at national level
  - Increased EU-level cooperation
  - Obligations for Operators of Essential Services (OES)
  - Obligations for Digital Service Providers (DSP)
- Member States decide on penalties and are to take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive

EU Cybersecurity-Related Policy Streams

CIIP	Data Protection	Targeted
The COM communication of 2009	General Data Protection Regulation (GDPR)	eIDAS
The first EU Cybersecurity Strategy (2013)		The CyberSecurity Act
The NIS Directive		The Cyber Resilience Act
NIS2 DORA		The AI Act
The Cyber Solidarity Act		

Agenda

- Trends in EU Cybersecurity Policy
- Directives & Regulations
- Background to NIS2 and DORA
- Similarities
- Specifics of NIS2
- Specifics of DORA
- Implementation Tips

Timelines & Penalties

- NIS2
  - Transposition period ends 17 October, 2024.
  - Administrative fines of up to €7,000,000 or at least 1.4% of the total annual global turnover for Important entities.
  - Administrative fines of up to €10,000,000 or at least 2% of the total annual global turnover for Essential entities.
- DORA
  - Entered into force on 17.01.23, applicable as from 17.01.25.
  - Member States establish appropriate administrative penalties and ensure their effective implementation.
  - Member States can choose to define criminal penalties.

Making Boards Responsible

- Article 20 of NIS2:

Article 20

Governance

1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.

2. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

- Article 5 of DORA:

Article 5

Governance and organisation

1. Financial entities shall have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk, in accordance with Article 6(4), in order to achieve a high level of digital operational resilience.

2. The management body of the financial entity shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1).

Risk Management vs. Compliance

- In general, EU Cybersecurity legislation is proposing a risk management approach as opposed to a compliance approach.
- Both NIS2 and DORA ask organisations to know the risks they are facing and to define suitable mitigating actions.
- To a large extent, ensuring good risk management is the core objective of both instruments.
- Both instruments put the emphasis on fundamentals and are concerned with improving resilience.

Notions of Criticality

- Both NIS2 and DORA provide guidelines on criticality as it applies to the respective target audiences.
- NIS2 distinguishes between Essential and Important organisations based on the type and size of the entity.
- DORA achieves this through Article 4 – the Proportionality Principle:

Article 4

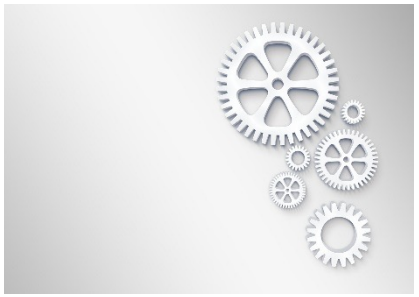
Proportionality principle

1. Financial entities shall implement the rules laid down in Chapter II in accordance with the principle of proportionality, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations.

Agenda

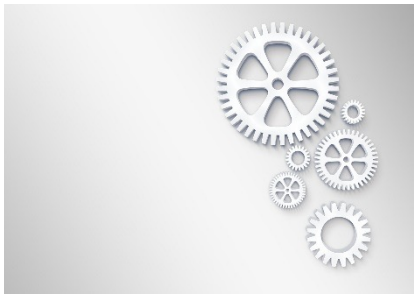
- Trends in EU Cybersecurity Policy
- Directives & Regulations
- Background to NIS2 and DORA
- Similarities
- Specifics of NIS2
- Specifics of DORA
- Implementation Tips

NIS2 – Scope Enlargement



- Sectorial scope is significantly enlarged.
- Establishes a two-layer approach:
  - Focus on big and key entities.
  - Differentiation of supervisory regime that allows only ex post supervision (i.e. reactive and without a general obligation to systematically document compliance) for those considered ‘important’ yet not ‘essential’.

Focus



- Article 1 explicitly identifies the four areas of focus of the Directive:
  - Member State (MS) obligations – national cybersecurity strategies, governance, CSIRTs.
  - Cybersecurity risk management measures and reporting obligations.
  - Rules and obligations on information sharing.
  - MS obligations on supervision and reporting.

NIS2: Supply Chain Requirements

- The key provisions are in articles 21(2)(d) and article 22 (1,2).
- Article 21(2)(d) states that key and important entities will have to put in place appropriate and proportionate technical, operational and organizational measures to ensure supply chain security.
- Article 22 describes an EU-level supply chain risk assessment process, known as coordinated security risk assessment.

NIS2: Supply Chain Requirements

- Article 21(2)(d) does not describe how the proposed coordinated security risk assessment should be carried out. However:
  - Recital 90 states ‘the aim [of the coordinated risk assessment is] identifying, per sector, the critical ICT services, ICT systems or ICT products, relevant threats and vulnerabilities.
  - Recital 91 states that this assessment ‘should take into account both technical and, where relevant, non-technical factors’. This recital also provides explicit criteria, which the risk assessment must satisfy.

Agenda

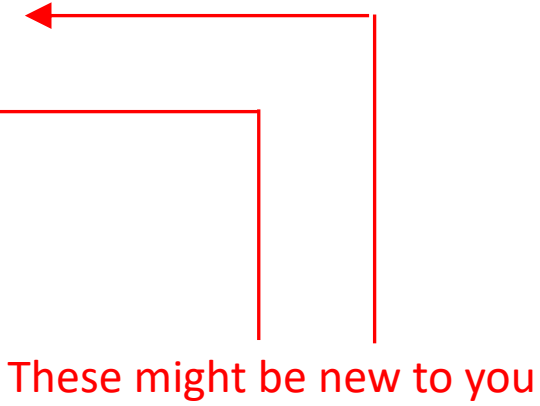
- Trends in EU Cybersecurity Policy
- Directives & Regulations
- Background to NIS2 and DORA
- Similarities
- Specifics of NIS2
- Specifics of DORA
- Implementation Tips

DORA

- The Digital Operational Resilience Act (DORA) will harmonize Information and Communications Technology (ICT) risk requirements in the Financial Services & Banking sector across the EU.
  - This is sector-specific legislation (Regulation NOT Directive).
  - Aims to replace the proliferation of national regulatory initiatives and supervisory approaches by a cross-border approach.
  - Applicable to critical ICT third party providers' (CTPPs), including cloud service providers (CSPs)
  - NIS2 and DORA have been aligned as part of the NIS2 development initiative, but overlaps are still possible….
  - Deadline for publication is 2022.

Focus

- DORA focuses on the following areas:
- ICT Risk Management.
- ICT-related incident management, classification and reporting.
- Digital operational resilience testing.
- Managing of ICT third-party risk.
- Information-sharing arrangements.



DOR Testing Programme

- Financial entities are required to set up a Digital Operational Resilience Testing Programme.
  - Does not apply to microenterprises.
- Must be based on Threat Lead Penetration Testing (TLPT).
- EU Supervisory Authorities are asked to develop draft regulatory technical standards in accordance with the TIBER-EU framework.
- Includes requirements on the testers.

ICT Third Party Risk

- ICT third-party risk must be managed as an integral component of ICT risk.
- Identifies minimal contractual provisions.
- Identifies the important elements of an Oversight Framework.
- EU Supervisory Authorities:
  - Designate critical ICT third-party service providers.
  - Appoint a Lead Overseer.
- Defines powers, tasks and cooperation methods of Lead Overseers.

Agenda

- Trends in EU Cybersecurity Policy
- Directives & Regulations
- Background to NIS2 and DORA
- Similarities
- Specifics of NIS2
- Specifics of DORA
- Implementation Tips

Implementation Tips

- Adopt a risk management approach as opposed to a compliance approach.
- NIS2 and DORA both concentrate on fundamentals. Don't reinvent the wheel – look for synergies.
- Use simple techniques, a simple table-driven method for following progress will suffice.
- Remember the people-process-technology rule. You need to sensibly balance all three components.
- Assign a responsible coordinator for the implementation and ensure that there is a plan.

Implementation Tips

- Look at governance first – there are a lot of people to be educated.
  - Board level participation is key. You need to get their commitment as soon as possible.
  - Remember that key positions should have named backups.
  - Plan awareness-raising activities to accompany the implementation project.
  - Establish a dialogue between technical and non-technical staff.
  - Make sure that the left hand knows what the right hand is doing.

Implementation Tips

- Keep documentation short and sharp.
  - Staff should know where to find it!!
  - It should be kept up to date.
- Test your processes
  - Documents are fine, tests are better.
  - Consider both planned and unplanned tests.
  - Learn from what went wrong and implement improvements.

Questions?