NIS 2: Revision of the Networks and Information Systems Directive

Briefing to Euro-IX
8th February 2022

Malcolm Hutty

23/02/2021

Executive Summary

- The European Commission has proposed a revision to the NIS Directive
- The key features for IXPs are:
  - To subsume the parallel regime in the European Electronic Communications Code under NIS
  - To broaden the scope of covered OES' slightly further
  - To provide more detail on security requirements imposed on OES' under the directive
  - To abolish assessment of whether OES-category organisations qualify as 'essential'
- NIS2 also changes duties for Member States; this is wholly outside the scope of this briefing.
- NIS2 includes changes affecting adjacent sectors (e.g. datacentres, CDNs)
  - This briefing mentions these in passing, but the focus will be on the impact on IXPs

Existing regime: Electronic Communications Code

- Network operators have duties to maintain security imposed on them under Articles 40-41 of the European Electronic Communications Code
  - (formerly, Article 13A-14A Telecoms Framework Directive)
  - These comprise obligations to notify regulators etc of security incidents, and general duties to manage security risks

Existing regime: NIS

- NIS applies broadly similar duties to "Operators of Essential Services"
  - NIS specifies a range of categories of OES including water, power generation and distribution etc.
  - NIS specifies IXPs as one of the categories

- NIS is a "minimum harmonisation" directive
  - Which means Member States must do *at least as much* as in the Directive, but are free to do more/regulate more stringently
  - This isn't changing in NIS2

Relationship of EECC and NIS

- NIS and Article 40 EECC are explicitly mutually exclusive:
  - NIS expressly excludes from its scope entities that are already regulated under Article 40 EECC
- Some IXPs are classified as 'Public Electronic Communications Networks' (and so regulated under Article 40 EECC), others are not
  - This is partly a result of differences of legal interpretation in different Member States
- The intent of the current regime is that IXPs will be regulated under NIS unless they are already regulated under the EECC: it's one of the other.

Avoiding regulation under the current regime

- Article 40 of the European Electronic Communications Code applies to *all* providers of Public Electronic Communications Networks
  - If your Member State deems an IXP to be a PECN, there is no avoiding it

Avoiding regulation under the current regime

- Article 5 NIS requires Member States to "identify" Operators of Essential Services
  - This is an assessment process
  - Firstly, a service must be in one of the categories listed in the Annex. One of those categories is 'Internet Exchange Points'.
  - Then, the Member State is supposed to conduct an assessment of each to determine whether a security incident at an operator would have 'significant disruptive effect' on the service
- In theory, this would allow small IXPs to escape regulation as being too small to have a 'significant disruptive effect'
- In practice, it's not an easy argument
  - Politically hard too say that the largest/only IXP is too small to qualify when the purpose of the Directive is to regulate IXPs
  - Poor definition of what "service" is being referred to.

Consequences of regulation under existing NIS

- NIS imposes two main sets of obligations (to be imposed on OES by MS)
  - A duty to notify the regulator of security incidents
    - This is well specified
  - A duty to "take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems"
    - There is very little detail in NIS on what that means in practice
- Accordingly, the actual expectations set by national regulators for discharging the security duty vary considerable amongst Member States.

NIS2: a unified regime

- Articles 40-41 of the European Electronic Communications Code is to be repealed. Providers of Public Electronic Communications Networks and Services) will be included in NIS2 instead.

- The requirement for Member States to "identify" (assess) Operators of Essential Services is being removed. Instead, as under the EECC, every operator of a service in a category in scope will be subject to the regulation
  - There remains a limited exception for *some* small and micro enterprises, but this exception is being narrowed compared with NIS

NIS2: small/micro exception (Article 2)

- NIS2 provides that small/micro entities may escape the scope, unless one of several exclusions to the exception applies
  - 'Small' means <50 staff and <€10m annual turnover and balance sheet
- Particularly noteworthy for European IXPs
  - No small/micro exception for providers of Public Electronic Communications Networks and Services (or TLD DNS registries)
    - So if you were previously regulated under the EECC, you're not getting a new small/micro exception
  - No small/micro exception where the provider is the only provider of the service in the Member State (ie. if your nation only has one IXP it will be regulated under NIS2 regardless of size)
  - There are also other, more qualitative exclusions to the exception

NIS2 duties: incident notification (Article 20)

- Mostly similar to existing
- Additional duty to notify '*threats*' as well as '*incidents*'
  - *Incidents* must have significant impact; *threats* must have potential to cause an incident with significant impact.
- Definition of '*significant*' improved
  - Now focuses on disruption or losses causes, instead of number of people affected and geographical area
- New deadlines: 24 hours for first notification, one month for final report
- Content of final report now specified, to include:
  - "a detailed description of the incident, its severity and impact;
  - the type of threat or root cause that likely triggered the incident;
  - applied and ongoing mitigation measures."
- Regulator can inform public, or require the regulated entity to do so

Elaboration of security risk management requirements

- NIS is extremely vague about what OES are actually required to do to manage security risks
  - All it says is
    - Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.
  - What this means in practice is left to national regulators to define
    - NIS also provides national regulators with extensive powers for this purpose
  - As a result, some national regulators developed detailed frameworks, while in other Member States this was simply copy-pasted in law, but in practice it was left to operators to decide how to implement it.

NIS2 duties: cybersecurity risk management

- New duties for Boards and Board members:
  - **Accountability**. "The management body [Board etc], [shall] approve the cybersecurity risk management measures […] supervise its implementation and be accountable for the non-compliance"
  - **Board member training**: "[M]embers of the management body follow specific trainings, on a regular basis, to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risks and management practices…"

NIS2 duties: cybersecurity risk management

- The general requirement for security risk management from NIS is retained, but supplemented by specifying a list of minimum measures required to discharge it:
  - risk analysis and information system security policies;
  - incident handling (prevention, detection, and response to incidents);
  - business continuity and crisis management;
  - supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services;
  - security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
  - policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;
  - the use of cryptography and encryption.

NIS2 duties: cybersecurity risk management

- The general requirement for security risk managemen
  but supplemented by specifying a list of minimum me
  discharge it:
  - risk analysis and information system security policies;
  - incident handling (prevention, detection, and response to incidents);
  - business continuity and crisis management;
  - supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services;
  - security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
  - policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures;
  - the use of cryptography and encryption.

Do you have comprehensive written policies and procedures covering each of these areas?

NIS2: Beyond the IXP

- This briefing is scoped around the impact on IXPs.
- That said, note that NIS2 will also impact:
  - TLD Registry operators (and registrars?), who are being given substantial new obligations beyond those mentioned in this briefing
  - Newly added and categorised as essential:
    - Datacentre operators
    - CDNs
    - Trust service providers
  - Moved from lighter 'digital services' category to be classified as essential
    - Cloud computing providers
  - Newly added and categorised as 'important'
    - Social media platforms (joining online marketplaces and online search engines)
    - Obligations for this category are changing, with most of the obligations mentioned in this briefing also being applied to this category for the first time.

Conclusion

- IXP operators that were previously regulated under the EECC, will now be under NIS2 and will want to check its requirements
- IXP operators that previously escaped both NIS and ECC, may now be caught under NIS2
  - Very small operators: beware of the exclusions to the micro entities exception!
- IXP operators that were previously covered by NIS, will want to assess their current level of achievement of the new requirements
  - Those who have a mature, well-documented security compliance regime (e.g. ISO27001 certified) may not find NIS2 daunting
  - Those whose experience of NIS was that there was little practical impact, may find NIS2 requirements significantly more demanding

linx

Thank you

 malcolm@linx.net