NIS2 Implementation Workshop: Incident Reporting

Voice of Industry

Context

One year after the official publication of the NIS2 Directive (EU 2022/2555), the efforts towards its implementation are fully underway. Different types of stakeholders are involved: EU institutions are working on the definition of guidance and guidelines; Member States are working on the transposition of the Directive, often through consultations with the national entities in scope; and last, several entities have already invested resources to better understand the scope of the Directive and its operational impact for their implementation.

In this context, by 17 October 2024, the European Commission (EC) is expected to adopt mandatory implementing acts on incident reporting with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms **specifying the cases in which an incident shall be considered significant.**

Main insights

Major debate in the industry revolves around the question of defining **thresholds for significant incidents:**

a) **Fixed thresholds**
b) **Variable thresholds across sub-sectors**
c) **Fully absent thresholds**

Fixed thresholds would simplify and harmonise incident reporting for the digital service and infrastructure providers but could not be equally applied across all other sectors in the scope of the NIS2 given sector-specific regulatory requirements and challenges.

Variable thresholds are the option that would consider specifics of a sub-sector but at the same time make it harder for companies providing several types of digital services to comply to multiple thresholds. Variable thresholds could lead to a situation where the incident reports will not be comparable and hence not being able to maintain the situational awareness and trending of the whole incident landscape, nationally or centrally in the member states.

Having no thresholds at all would give companies autonomy to develop the most effective and efficient approach according to the internal or sectorial best practices. This option would increase risk of excessive or limited reporting.

Industry is looking to have clear definitions on **what constitutes an incident and what defines a significant incident**. Internal incident processes are already in place and each company has varying methodologies for the classification of incidents depending on parameters like:

- Number of affected instances,
- Number of affected customers,
- Financial value,
- Personal data impact,

European Cyber Security Organisation (ECSO) • https://www.ecs-org.eu • EU Transparency registry: 684434822646-91 • Avenue des Arts 46 Kunstlaan, 1000, Brussels, Belgium

- Operational disruption,
- Reputational damage,

However, the **weighting of specific parameters varies across companies, sectors and countries, which makes it difficult to establish a core set of parameters to define the severity of incidents.**

The EC needs to establish clear thresholds for the reporting of significant incidents, either horizontally or specifically for certain types of attacks. **Specifying the type of threat in the Implementing Act (e.g. ransomware) is not seen as effective by the industry**, as impacts can vary, and the same type of attack can be sometimes addressed immediately.

Companies in the scope of the mandatory Implementing Act on incident reporting are digital service and infrastructure providers. A clear distinction should be made between internal incident reporting and incident reporting for service recipients. **Thresholds need to be tied to the requirements of digital service providers and not to the entity benefiting from the service, given that providers lack visibility on key incident information from a customer (e.g., number of users impacted, size and criticality of the company).**

The level of significance **of an incident might change over time** with the continuous assessment so the incident reporting framework needs to be flexible. Additionally, the incident reporting framework should be **simple, user friendly** and focus on **measurable parameters**. **Standardised guidelines** for reporting incidents are needed to **avoid ambiguity and discrepancies in national transposition of the NIS2 Directive**. This will in turn streamline reporting of incidents and lower the amount of non-relevant or duplicated information being reported.

When assessing incidents, determining a figure for the duration of **operational disruption deemed significant poses a challenge**. Considering that incidents are not occurring in a vacuum and have an impact on society, or the ecosystem of the company, **systemic risk and societal impact** need to be taken into account when assessing impact of an incident in an individual company. For DNS providers, managing operational disruptions is crucial because they can pose system risk Furthermore, **estimating financial loss during the initial assessment is difficult with a complexity varying across impacted sub-sectors** and might not impact the severity of the incident significantly.

Requirements set in the implementing act should be **harmonised with the other EU policies tackling incident reporting.** Additionally, a clear link has to be established **between the implementing act on security measures and the one on incident reporting,** as having predefined security measures for incident management procedures supports streamlining of impact assessments across companies.

Conclusion

ECSO applauds efforts by institutional partners to foster dialogue between policymakers and industry stakeholders. Such collaboration is essential for ensuring that cybersecurity policies are not only comprehensive but also practical and implementable. ECSO encourages continued engagement with industry experts to harness their insights and expertise in shaping effective policies.