Non paper – Digital Omnibus - Single Entry point for incident notifications

'Towards simplifying the cybersecurity landscape, instead of adding complexity'

By France, Germany, Italy, the Netherlands, Spain and Sweden

In a world where swift action is needed to effectively counter cyber threats, simplifying the cybersecurity landscape is a necessity. The proposal of the European Commission to develop a Single-Entry Point for incident notifications at EU-level would only add more complexity to incident response and notification, impacting consequently the current processing of incident notifications at national level by Member States. We strongly believe that the Commission should find alternative ways to effectively create clarity within the landscape.

1. **The pivotal role of national CSIRT's within the cyber landscape.**

As cooperation and coordination between Member States are needed to effectively counter cyber threats, the most effective way to realize this is to invest in existing structures. National CSIRT's and competent authorities play a fundamental role within the cyber landscape, as they officiate as deeply entrusted partners for entities. They also dispose of profound knowledge of the sectors within each specific Member State. They are consequently best placed and equipped to help and support entities in times of cyber crises throughout the whole process, from assistance to incident notification and incident response. Indeed, incident reporting can not only be seen as a legal obligation, but should be directly linked to the role of CSIRTs to assist victims facing a cybersecurity incident. The CSIRT role is central in helping entities through assistance but also accompanying the victim in the notification process.

The trust assigned to national CSIRT's and competent authorities did not emerge overnight, but has been built steadily over the years. Their constant and pivotal implication in the landscape should not be underestimated as they helped shape strong national structures. Trust is -as widely understood- a crucial aspect in the cyber domain, as being targeted by cyber-attacks or having to deal with an important incident can be a very sensitive matter. This is especially the case for small and medium enterprises, being also the most vulnerable for cyber-attacks. The organization of incident reporting at the national level is or has been already a significant burden for these entities. Changing and restructuring incident reporting to the EU-level therefore does not only undermine the trust that was built with national CSIRT's, but also increases the administrative burden for entities. Even more, introducing this initiative could even be experienced as an encumbrance for the timely handling of cyber incidents.

2. **An inadequate technical solution that would complexify the existing structures**

The proposal for a Single-Entry Point constitutes a technical feature with which the Commission aims to centralise different reporting regimes at the EU level. However, until this day it remains unclear and unproven as to how this technical solution will lead to simplification and harmonization, since the necessary prerequisites are not elaborated yet.

Introducing a Single-Entry Point at EU level at this stage would lead to more complexity, given the fact that operational and efficient national structures are already in place, that national reporting obligations exist alongside European obligations and that it touches national competences. The processes related to reporting obligations should remain the sole responsibility of the Member States. Also, the majority of entities conduct their operations

within a single or a few Member States, and thus do not have cross-border operations, complexifying the process for a majority of entities without simplifying cross-border notifications.

Finally, centralizing sensitive information on incident notifications of 27 Member States would render the EU more vulnerable for cyber-attacks in the event of inadequate security measures. Bringing together in one single point all vulnerabilities of private, public and civil structures, would pose a very significant risk to the security of information systems and national security. This centralization also creates dependencies with regards to the continuity of services, since potential failure or downfall of this critical (notification) processes may have considerable consequences.

We strongly believe that the alignment and streamlining of incident notifications is part of the needed prerequisites and would directly contribute to the regulatory simplification. Working on harmonisation would support entities in navigating the administrative regulatory obligations, and Member States could integrate these into their national notification processes, enabling secure processing of the reported incident. This is the most effective way to simplify incident notification at EU level, and is a first but prerequisite step towards simplification.

3. Our solution to maximize our simplification efforts:

In addition to harmonising European incident reporting obligations and in order to further support entities navigating EU cybersecurity incident notification landscape, we see strong added value in the development of an EU website on EU-wide incident reporting obligations. This website could be developed and managed by ENISA and should help identify and connect with the most appropriate national responder, enhancing clarity and accessibility, while allowing an anonymous navigation. This European website for guidance would map all obligatory incident reporting in the different Member States and at EU level and provide links to the competent reporting authority. Developing a mapping tool of the regulatory landscape contributes to sharing knowledge and information as part of the current ENISA's mandate.

Considering all the above, we propose the first draft of compromise text should focus on the following:

The EU Single Information Point will consist of a publicly accessible website developed and managed by ENISA. The Single Information Point will reduce administrative burden for entities by providing information on reporting and assistance structures and a clear overview of information on incident reporting of the respective legislation. The Single Information Point will give a clear and centralised overview on when, where and how entities must report security incidents to the recipients defined in respective legislation. This overview may include the redirecting of Website-visitors to the respective Member States' national entry points and/or reporting forms.

There will be no changes to the respective legislation, as Member States remain the sole and direct recipient of all notifications and continue to have the sole responsibility for all processes related to reporting obligations. The Single Information Point-website will not collect any data on reports or notifications and will not store any data related to the reporting obligations following the respective legislation.

We do strongly support the Commission's objective to simplify the cyber landscape and reduce the administrative burdens for entities. This requires effort from both the European institutions and from the Member States, and better alignment of existing legislative frameworks. We believe that a first step is mapping the European and national obligations in terms of incident reporting. Next, deadlines, templates and national end-points for notification should be better aligned to improve user-friendliness. Where feasible, centralisation of national end-points for cyber notifications should be encouraged. Finally, different concepts and definitions should be harmonised and a common set of data to notify should be defined. This way, simplification efforts in the cybersecurity domain can have real added value for entities and governments alike.