Nasdaq

Nikolaj Plads 6, 1007 Copenhagen K, Denmark | Nasdaq.com

31 December 2022

Financial Stability Board
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Nasdaq's response to the consultation on Achieving greater convergence in Cyber Incident Reporting

Nasdaq Copenhagen A/S, Nasdaq Helsinki Ltd, Nasdaq Iceland hf., Nasdaq Stockholm AB, Nasdaq Oslo ASA and their affiliates (collectively referred to as "Nasdaq") welcome the opportunity to respond to the FSB's consultation on achieving greater convergence in Cyber Incident Reporting.

Nasdaq operates several regulated markets and MTFs across the Nordics and the Baltics, which are home to more than 1,200 listed companies. The Nasdaq trading venues drive the European and global economy and provide investment opportunities for both institutional and retail investors. Additionally, Nasdaq operates a CCP, a CSD, and in the Baltics Nasdaq holds a Pensionikeskus license. Thus, Nasdaq has experience with Cyber Incident Reporting ("CIR") towards multiple supervisory authorities around the globe and brings a unique, global perspective to the issues raised in the FSB consultation.

Nasdaq would like to put emphasis on certain topics for FSB to take into account when continuing its work on increasing convergence in the CIR area.

CIR Convergence

Nasdaq recognizes that cybersecurity threats post an ongoing and escalating risk to companies, investors and market participants and commends the FSB's efforts to increase comparability and convergence in the field of CIR.

Nasdaq welcomes focus on convergence, because different thresholds and differences in reporting requirements, including content of required reporting, can create operational challenges and inefficiencies, which can ultimately undermine the achievement of the objectives for reporting regimes. This is particularly apparent across organisations, which operate distinct regulated entities that rely on common core technology or platforms in multiple jurisdictions. This means facing various national regulatory cyber incident reporting obligations and multiple authorities to which to report.

Nasdaq is therefore positive towards FSB's recommendation for financial authorities to continue to explore ways to align their Cyber Incident Reporting. (Recommendation 2). We believe that a common approach from authorities would also be beneficial for the authorities in their supervisory work.

In this regard, we believe that any additional guidance to be developed by financial authorities in the area of CIR (as proposed in FSB's Recommendation 13) should be aligned internationally in order to achieve convergence across borders. Additionally, common guidance should not be too complex to apply during an incident.

Furthermore, it is our conviction that engagement and ongoing communication between financial authorities and the sector/ financial institutions is of great value for achieving a common understanding of the incident reporting framework, including reporting criteria. Hence, we support FSB's Recommendation 12.

Thresholds and reporting triggers (materiality assessment)

Nasdaq stresses the importance of guidance from financial authorities to financial institutions on reporting thresholds and triggers, i.e. what aspects are to be considered, when carrying out impact assessments for materiality thresholds, which trigger reporting obligations.

Nasdaq welcomes continued efforts to bring more clarity with regard to the reporting thresholds, e.g., through supplementing CIR guidance with examples (Recommendation 7). Additionally, Nasdaq believes that more engagement between financial authorities and financial institutions would promote consistent understanding of cyber incident reporting requirements and minimize the risk of misalignment between authority expectations and financial institution reporting.

At the same time, Nasdaq recognizes certain challenges with qualitative reporting and materiality thresholds triggering reporting, to which FSB points. Assessing the extent of a cyber incident and determining its materiality can be a challenge within tight reporting deadlines. Also, in the initial stages after discovering the cybersecurity incident, facts and circumstances are not fully uncovered or determined. This challenge is amplified by the fact that the main focus for a financial institution in a cyber incident situation should be resolving the incident. Thus, Nasdaq agrees with FSB's considerations in Recommendation 4, pointing out the need for balancing the financial authorities' requirement for timely reporting with the financial authority's main objective.

Reporting timelines and channels

Any reporting windows and timelines for CIR set by financial authorities need to be carefully calibrated in order not to put additional strain on the main objective for financial institutions in case of a cyber incident.

Nasdaq reiterates that once a breach of a company's information systems has been discovered, it is paramount for a company to understand the scope and nature of the cybersecurity incident and immediately commence remediation efforts to limit the amount of damage that such an incident may cause. Time is of the essence for a company dealing with a cybersecurity incident.

As an example of currently differing timelines, NIS directive's incident reporting in some European jurisdictions[1] requires initial reporting within 6 hours of the incident discovery with subsequent follow-up(s), whereas Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) will - when enacted via regulation - require cyber incident reporting within 72 hours in the US. Nasdaq sees merit in working towards transparent and aligned incident reporting timelines across jurisdictions.

[1] This is the case for Iceland and Sweden.

Additionally, Nasdaq stresses the importance of having secure information channels to financial authorities, when submitting information about CIR. Such information would include sensitive information, which needs to be protected. Therefore, Nasdaq supports FSB's Recommendation 16, encouraging financial authorities to implement secure channels to collect CIR information. CIR reporting channels should preferably be encrypted, and multinational corporations would undoubtedly benefit from a possibility of utilizing the same channel for reporting to multiple authorities.

CIR content

Overall Nasdaq agrees with the view expressed in FSB's consultation that common understanding of cyber incidents is needed to avoid over-reporting of cyber incidents and events, which are not significant. Therefore, Nasdaq would welcome continued efforts from financial authorities to explore ways to align and achieve a common definition of a cyber incident. Such efforts should take "lessons learned" from other mandatory reporting regimes to anticipate how requirements may incentivize organisations to over-report out of an abundance of caution in the face of potential regulatory consequences for not reporting a covered incident, i.e. an incident, which occurrence organisations have a regulatory obligation to report.

Moreover, Nasdaq supports endeavors to identify common types of information to be reported for cyber incidents across different jurisdictions, and Nasdaq is positive towards the recommendation for financial authorities to identify common data requirements for CIR (FSB's Recommendation 3).

At the same time, Nasdaq appreciates the challenges with a one-size-fits-all approach, and thus encourages to build in flexibility in such common data requirements. As an examples, it could be overly burdensome for smaller companies if both large and small companies were to be required to provide the very same level of detail in CIR. The size of the company could be factored in, when setting out CIR content requirements.

Against this background it is important to stress that multinational corporations already face challenges with reporting under multiple rulesets and towards multiple authorities. This is for example the case with the NIS directive, which is implemented nationally in the EU / EEA area with certain national differences, resulting in potentially multiple reporting content requirements for a single cyber incident. Thus, FSB's guidance with regard to the content of CIR should derive from and be aligned with existing regulatory requirements. This is to avoid possible duplicative disclosures.

Common, global incident reporting format "FIRE"

Although Nasdaq is not against the idea of developing a common, global incident reporting format ("FIRE") proposed by the FSB in order to work towards further convergence of CIR information requirements, such a common format should not add complexity to the already existing incident reporting requirements.

Thus, a proposal for a common reporting format for all types of incidents and not only those related to cyber incidents raises some concerns due to potential challenges in encompassing a comprehensive set of incident reporting against the background of potential vast differences in national incident reporting requirements. This in turn would add complexity to existing incident reporting. Hence, Nasdaq would suggest to focus on the more narrow area of cyber incidents.

Additionally, the content of such common reporting should be based on a thorough analysis of existing regulatory incident reporting requirements and should not create entirely new definitions, which are not currently used in the legislation/ regulation.

Lastly, Nasdaq applauds the idea of streamlining incident information to enable a certain level of automation in incident reporting. However, if such a common reporting tool was to add value, it would require a broad support and adoption from supervisory authorities around the globe.