UNIPOL GRUPPO S.P.A 30 December 2022

Achieving Greater Convergence in Cyber Incident Reporting

Template for Responding to Public Consultation

Background

In 2021, the Financial Stability Board (FSB) published a report on *Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence*. The report set out three ways the FSB would take work forward to achieve greater convergence in cyber incident reporting (CIR): (i) develop best practices; (ii) create common terminologies for CIR; and (iii) identify common types of information to be shared across jurisdictions and sectors. To inform its work, the FSB conducted a survey of FSB members to: identify the most common reporting objectives and types of reporting performed; understand the practical issues financial authorities and financial institutions (FIs) have in collecting or using incident information; identify the information items authorities collect to meet the common reporting objectives, including a review of existing incident reporting templates; and explore the mechanisms for financial authorities to share incident information across borders and sectors.

Drawing on the survey findings, the FSB has set out recommendations to address impediments to achieving greater convergence in CIR with a view to promote better practices. This work also helped to inform refinements to the *Cyber Lexicon*, which resulted in the addition of four terms and revision of three definitions. The FSB also reviewed financial authorities' incident reporting templates and identified commonalities in the information collected. Leveraging on this work, the FSB presents a concept for a format for incident reporting exchange (FIRE) to promote convergence, address operational challenges arising from reporting to multiple authorities and foster better communication.

The FSB is inviting feedback on this consultative document, in particular on the questions set out below. Responses should be sent to fsb@fsb.org by 31 December 2022 with the subject line 'CIR Convergence'. Responses will be published on the FSB's website unless respondents expressly request otherwise.

Challenges to achieving greater convergence in CIR (Section 2)

1. Is the emphasis on practical issues to collecting and using cyber incident information consistent with your experience? Does your institution want to provide any additional evidence for the FSB to consider from your experience?

   The FSB description of the practical issues to collecting and using cyber incident information is consistent with our experience. In particular, the fragmentation of the relevant regulatory framework and the lack of a consistent methodology for assessing the impact of an incident are significant issues in defining the scope of the incidents that need to be reported and hinder the convergence in CIR.

   Albeit may be out of scope of this consultation, we encourage the FSB to explore in its future works the role that greater convergence in CIR could have on the growth of cyber insurance, which is widely acknowledged for increasing the entities' cyber resilience by encouraging investments in risk reduction and facilitating responses and recovery from cyber-attacks[1]. Indeed, a common framework and template for CIR would allow the development of a reliable and coherent dataset that could be used by insurers to enhance cyber risk measurement, pricing, and management.

   Accessibility to larger and comparable dataset on cyber incidents and losses (even if duly anonymized and aggregated) would likely lead to a reduction of the overall average premiums for cyber insurance, as it would mitigate the adverse selection effect and allow a more accurate and tailored pricing. In this context, limited disclosure of incidents as well as heterogeneity of data capture are two of the main constraints hindering the development of cyber insurance. As to the lack of information, it is worth considering that most of the data on cyber incidents is reported by virtue of contractual or regulatory obligations but even when reporting is mandatory, relevant data is almost never shared with interested parties. As to the heterogeneity of data capture, IAIS noted that: "*The comparability (and ultimate utility) of the incident data that is available is limited by a lack of a shared taxonomy for categorizing the incidents and resulting losses, thereby increasing the uncertainty around loss estimates* […] *These shortcomings undermine the possibility of combining internal and external data* […] *and forming a consistent view of cyber risk when accessing external or public data*" (IAIS – Cyber Risk Underwriting).

   A solution to overcome these obstacles would be developing proper data information sharing between competent authorities and financial institutions. Even EIOPA, in its Strategy on Cyber Underwriting, observed that: "*in order to allow for sound pricing, underwriting and cyber risk management, the availability of data on cyber incidents should be broadened and appropriately standardized, while safeguarding the level playing field and data confidentiality*." Considering the above, it would be important that any future policy initiative on CIR will also take further steps towards the development of information sharing mechanisms between (financial, data protection and cyber security) authorities and financial institutions, possibly at regional or international level.

---

[1] In this respect, OECD (amongst many others) stated that "*while not a substitute for investing in cyber security and risk management, insurance coverage for cyber risk can make a significant contribution to the management of cyber risk by promoting awareness about exposure to cyber losses, sharing expertise on risk management, encouraging investment in risk reduction and facilitating the response to cyber incidents*" (OECD – *Enhancing the role of insurance in Cyber Risk Management*, 8 December 2017).

Recommendations (Section 3)

2. Can you provide examples of how some of the practical issues with collecting and using cyber incident information have been addressed at your institution?

   Click or tap here to enter text.

3. Are there other recommendations that could help promote greater convergence in CIR?

   Click or tap here to enter text.

4. Could the recommendations be revised to more effectively address the identified challenges to achieving greater convergence in CIR?

   Provided that the FSB recommendations seems fully agreeable, it is worth remarking the importance of enhancing the collaboration tools "to proactively share event, vulnerability and incident information" (Recommendation 15). Current CIR requirements often result in one-way communications from the financial institutions to the competent authorities, each of them triggering further requests of information and updates.

   Notwithstanding the fact that the mandate of Financial Authorities does not include the management of cyber-incidents nor the sharing of intelligence information, it is necessary that future policy initiatives will enhance collaboration and information sharing between financial and non-financial authorities (cyber security, data protection) and private sectors firms. To this end, an effective policy choice to enhance cyber resilience and financial stability would be establishing a single hub of notification (on a cross-sectoral basis), fully accessible to all competent authorities. The information thus collected should also be made available to all interested parties, after due anonymisation and aggregation, as it would allow those entities to enhance their understanding of cyber risks (also for cyber underwriting purposes, as argued above) and strengthen their cyber resilience.

   The single hub of notification, if built on effective institutional mechanisms of information sharing and collaboration between all competent authorities and private stakeholders, could serve as the basis to develop **regional cyber-security platforms**[2], aimed sharing intelligence, analysing cyber threats, and providing timely reports. These cyber-security platforms would have the merit of overcoming the current "silos" approach and of allowing the combination of ex-post analysis with ex-ante sharing of threat intelligence.

[2] Similar institutional mechanisms have been described and advocated by institutions and scholars. On this matter see, amongst others, ENISA – *Information Sharing and Analysis Centres (ISACs): Cooperative Models*, 2018, and C. Callies and A. Baumgarten – *Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective*, in German Law Journal, 2020, 21, pp. 11-49-1179.

Common terminologies for CIR (Section 4)

5. Will the proposed revisions to the Cyber Lexicon help to encourage greater adoption of the Cyber Lexicon and promote greater convergence in CIR? Are there any other ways in which work related to CIR could help to encourage greater adoption of the Cyber Lexicon and promote greater convergence in CIR?

Click or tap here to enter text.

6. Do you agree with the definition of 'cyber incident,' which broadly includes all adverse events, whether malicious, negligent or accidental?

We agree that the definition of "cyber incident" should broadly include all adverse events, whether malicious, negligent, or accidental. That being said, a "cyber incident" could be triggered by several kinds of malicious activity, such as a "cyber-attack" or other non-authorised activity.

7. Are there other terms that should be included in the Cyber Lexicon to cover CIR activities?

Based on our experience, we propose four terms that could enrich the framework and ensure its relevance in the current legal and cyber threat landscape.

First suggestion is to define the concept of a major cyber incident, to distinguish between incidents that do not reach a certain materiality threshold (and that should be subject to none or minor requirements) and major ones. This concept would help dismiss the misconception that all cyber incidents are the same and should be subject to similar requirements, coherently with existing legislations (e.g., DORA). As a matter of example, several authorities (e.g., SEC, Banque de France, European Banking Authority and MAS) are imposing mandatory CIR only for serious or major incidents, as shown in Annex 3 of the Consultative Paper. The lack of a uniform definition of major cyber-incident could therefore hamper the standardisation of the reporting processes. Should the FSB consider inappropriate or unfeasible to add this new definition in its Cyber Lexicon, we would at least recommend providing more guidance on the metrics and methodologies for assessing the severity of cyber incidents, possibly relying on existing standard such as those published by ENISA and by further developing the past FSB's work on this matter.

In addition, we propose to the FSB to include the following terms: authentication, authorization, and encryption. The introduction of these new items is justified by the fact that most policymakers rely on these notions, without providing the relevant definitions. Moreover, greater clarity on these terminologies could improve the cross-sectoral comprehensiveness of cyber issues, facilitate information sharing between entities and support the work of the FSB and other standard-setting bodies (also in the context of financial stability monitoring).

8. Are there other definitions that need to be clarified to support CIR?

Click or tap here to enter text.

Format for Incident Reporting Exchange (FIRE) (Section 5)

9. Would the FIRE concept, if developed and sufficiently adapted, usefully contribute towards greater convergence in incident reporting?

In our view, the FSB's Format for Incident Reporting Exchange (FIRE) represents a crucial initiative to achieve greater convergence in CIR. The wide adoption of the FIRE could facilitate information sharing between private and public actors, with significant benefits for the industry.

According to the ENISA, cyber incident information sharing is the most effective approach to detect and counter modern complex cyber threats that cross national borders. Broader information allows to identify patterns and anticipate new threats, as well as support the digital resilience of the financial system. Also, from the perspective of an insurance company, the development of FIRE could have positive spillovers related to the creation of larger, reliable, and comparable datasets that are needed to insure and price cyber risk. Therefore, we strongly support the principles and core elements of the proposed framework.

To date, the scope of the information required for CIR activities is broadly fragmented, making the institution-initiated reporting cumbersome and hindering the benefits of reporting, as also acknowledged by the FSB. In Italy, for example, there is no single template for the notification of cyber incidents and, thus, each insurance undertaking has developed its own. However, the legislative gap will be filled in the next future by the DORA, which provides that European Supervisory Authorities shall develop a single template for cyber incident reporting. In this respect, we believe that FIRE should serve a baseline for developing the upcoming DORA's template, to allow greater comparability of the data reported across regions, even outside Europe.

10. Is FIRE readily understood? If not, what additional information would be helpful?

On general note, Unipol finds the proposal readily understandable, owing in part to the flexible approach taken by the FSB. Having said that, we would like to highlight some relevant aspects to consider in the development of the FIRE.

The first relates to the importance of secure communication channels. The content of a cyber incident notification may reveal sensitive details about the reporting entity; hence it is crucial to preserve the integrity of such information and prevent vulnerable entities from being exposed to additional risks. Even data related to contact persons – if compromised – could trigger further targeted attacks as they reveal the identity and the contacts of the persons likely to have a central cybersecurity role in the organisation. In this respect, it is concerning that – according to the FSB – unencrypted emails represent the most used communication channel for reporting cyber-incidents. For this reason, we encourage the FSB to further explore the international best practices aimed at sharing cyber-incident information securely.

Secondly, the FIRE should ideally be developed in conjunction with common methodologies for assessing the severity and the economic impact of cyber incidents. We acknowledge that financial institutions and authorities may have different views on this matter, especially concerning the thresholds triggering the notification requirements. Nonetheless, we believe that some common ground should be found in view of the potential upsides. Indeed, information on the economic costs of cyber incidents could help financial entities to accurately assess their risks and raise awareness of having adequate ICT security standards. Moreover, closing data gaps would allow policymakers to improve their supervisory activities and expand their macro-prudential toolkit to safeguard the resilience of the financial system[3]. In this respect, the work already done by the FSB on the "Effective Practices for Cyber Incident Response and Recovery" represents a particularly good starting point for further developing common methodologies to assess cyber incidents.

11. If FIRE is pursued, what types of organisations (other than FIs) do you think would need to be involved?

Critical third-party providers (TPPs) should be included within the scope of organisation using FIRE by virtue of their key role within the value chain of financial services. Admittedly, TPPs have offered flexible, cost-effective, and robust solutions to support the digitalisation of the financial sector. However, the extent of this reliance has heightened the operational dependence and risks related to TTPs.

A recent survey by the Ponemon Institute[4] revealed that 59% of respondent companies experienced a data breach caused by one of their TPPs, whereas 38% say the breach was triggered by one of the sub-contractors ("Nth party") due to flaws in third parties' securities controls. The same report highlighted the increasing trend in cyber incidents involving third parties, as well as the limited transparency among the third-and-Nth party relationships.

The risks for financial stability stemming from cyber-incidents involving TTPs is further exacerbated by the market concentration for the provision of certain ICT services[5].

In this context, a major cyber incident affecting TPPs (or even a subcontractor) could represent a threat for the financial entities. In the case such disruption involves a major ITC TPP provider, this could simultaneously affect numerous financial institutions, undermining the overall financial stability.

In light of the above, including critical TPPs within the scope of the entities using FIRE for CIR purposes seems appropriate and would also be coherent with the policy approach adopted by DORA.

---

[3] See, ECB - *Towards a framework for assessing systemic cyber risk*, Financial Stability Review, November 2022.

[4] Ponemon Institute - *The 2022 Data Risk in the Third-Party Ecosystem Study*, September 2022.

[5] According to ESMA, three major ICT providers hold 60% of the market share for cloud services to financial firms. See ESMA - *Financial stability risks from cloud outsourcing*, 2022.

12. What preconditions would be necessary to commence the development of FIRE?

Click or tap here to enter text.

* * *

Unipol Gruppo S.p.A.

Head of Regulatory Affairs

Luca Giordano