Swiss Insurance Association

The Swiss Insurance Association and its members have compiled their feedback to the consultation document on “Achieving Greater Convergence on Cyber Incident Reporting”. Although the deadline was 31 Dec 2022, may I kindly ask you to still consider our response in your final recommendations. Due to unexpected sick leaves and personal leaves, we were unable to submit it on time.

Recommendation 15 addresses the need for data exchange FI to FI.
⇨ The need for a feedback-loop from regulator to FIs is not well described. It is hinted at the description of the FIRE concept, but it’s not concrete enough.

Recommendations 13 and 7 address the data exchange "quality assurance".
⇨ This is good, but it is rather qualitative than quantitative. Further emphasis on the latter would be beneficial.

Recommendation 5 addresses the proper trigger to be used.
⇨ This is clearly important for underwriting/capacity management purposes and should be as homogeneous as possible across reporting requirements (i.e. regulators) to allow comparable statistics.

Recommendation 8 suggests the inclusion of "likely breaches" (near misses).
⇨ This is very difficult to use in a statistical model/analysis and for the underwriting/capacity activities it is of little value EXCEPT for very high triggers where a type of "counter-factual analysis" could be carried out for capacity/capital management.

Recommendation 3 addresses the "reporting format", i.e. "individual data fields within incident reports".
⇨ This is crucial for the underwriting/capacity management purposes and the insurance industry has a lot of experience at defining the needed data (taxonomies).

With regards to the **Cyber Lexicon** and the 5th paragraph of the introduction of Chapter 5 (operational incidents vs cyber incidents), we are agnostic to how it is phrased, but the clear need is to have a reporting of both malicious activities (security failure) and non-malicious system/human failures leading to a "cyber" incident with at least a flag to differentiate them.

FIRE concept:
The granularity of "Incident Details" and "Impact Assessment" (see figure 4) is paramount to a useful implementation. Furthermore, there must be a way to also aggregate individual incidents linked to the same "accumulating event" (e.g. NotPetya) to enable a per event analysis further to the “per corporate” analysis. As mentioned in our comment about recommendation 3 above, the insurance industry has a lot of experience in defining the needed data fields and granularity requirements.

Reporting:
- Reducing the fragmentation of reporting requirements is a clear need. It will improve efficiency and decrease the risk of mistakes/misunderstandings. This is especially true in the stressed days just after discovering a cyber or operational incident.
- Financial authorities should enable "safe harbor" conditions, to make sure that reporting corporates are not penalized by their reporting, especially in cases of conflicting reporting requirements across jurisdictions or across authorities.
- The FSB lexicon should be made clearer to split the mentioned cyber security incidents from the cyber non-malicious (operational) incidents, as mentioned above.

I’d appreciate if you could confirm that our input was received and that it can still be considered for your final recommendations on this topic.

Best regards,

Gabor Jaimes