Comments on the Consultative report concerning the Guidance on cyber resilience for financial market infrastructures

23 February 2016
Leon Strous
Chair of a group of business continuity experts of core financial infrastructure institutions in the Netherlands (Platform BC VIF)

Comments are on behalf of a number of members of this group.

We welcome the initiative of the BIS to provide supplemental guidance on cyber resilience to the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI).

This guidance can certainly help to enhance the cyber resilience capabilities of Financial Market Infrastructures (FMI) to cope with the interconnected nature of cyber threats. At the same time we would also like to express some concerns with regard to possible unintended effects.

General comments
Firstly we should be aware that broadly defined principles leave space for National Competent Authorities to translate them into practical baselines. This makes it possible to take into account specific circumstances. The downside of this feature is however that they also give room to too many interpretations of principles thereby creating unlevelled market circumstances for FMIs across the EER. The issued supplemental guidelines can help to prevent this by carefully considering and advising that principles should not be defined too broad and that rules are not too detailed.

Another concern is that member states do have the right to implement specific local legislation (often inspired by the generic principles) intended to get a firmer grip on local FMI's. These local legislations sometimes contain specific rule based quantitative norms which inherently have the tendency of being interpreted in too absolute terms (without sufficient care for probability and magnitude) and regardless of the specific context of the object of scrutiny. This might hinder sound material judgments and result in unnecessary cost for FMI's, creating disproportional unfair market conditions for local players compared with their foreign EU peers.

We would appreciate it if these concerns are taken into account when publishing principles and guidelines.

Specific comments

Expected usage – Target groups (1.3.1)
The scope of the guidance may be too limited (caused by the defined target groups in 1.3.1 and by the exceptions mentioned in footnote 8). Looking from a transaction chain perspective, all parties involved in such a chain can cause risks to other parties when encountering cyber threats. This means that not only FMIs as defined in the PFMI should pay attention to cyber resilience (and follow the guidance) but also FMIs mentioned in footnote 8: "market infrastructures such as trading exchanges ….". The fact that it is left to the discretion of the relevant authorities to decide whether or not to apply the guidance to types of infrastructures not formally covered by the report does not contribute to clarity and a level playing field. While we acknowledge that this is a difficult and sensitive issue given mandates and competencies, we feel that there are options to put this into wording.

Information-sharing groups (8.3.2)
We agree that FMIs should participate actively in information-sharing groups and collectives to gather, distribute and assess information about cyber practices, cyber threats and early warning indicators relating to cyber threats. We also agree that the membership of these groups could be cross-industry, cross-government and/or cross-border.

However there is a risk that recommendation 8.3.2 is overly ambitious as the recommendation advises that a FMI should participate in groups that include at least a cross-industry, a cross-government and a cross-border group. We therefore propose a small amendment to this recommendation to include the words “where appropriate”. The proposed wording becomes “FMIs should…, including *where appropriate*, cross-industry…..”.

Furthermore we like to emphasize that the detail and/or actuality of information that can be shared in these groups may be restricted due to the setup of the FMI (e.g. disclosure of information for listed companies may be restricted due to listing rules).