GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

July 2020

Response to FSB consultation report on effective practices for cyber incident response and recovery

The Global Federation of Insurance Associations (GFIA) is a non-profit association established to represent national and regional insurance associations that serve the general interests of life, health, general insurance and reinsurance companies in 60 countries. These companies account for approximately 89% of total insurance premiums worldwide. As GFIA is a representative body and the Consultation Report is aimed largely at the practices of individual financial institutions, GFIA is unable to provide detailed responses to the questions on the toolkit. However, GFIA appreciates the opportunity to provide comments of a general nature on the Consultation Report, Effective Practices for Cyber Incident Response and Recovery (Consultation Report).

The insurance industry places great importance on securing its own information systems and welcomes the international community's efforts to enhance cross-border cooperation in addressing this global risk. Overall, the Consultation Report offers helpful observations to enhance cyber incident response and recovery. Nevertheless, GFIA is of the view that the Consultation Report should: i) recognise and provide tools for scaling the identified practices, ii) take into account existing regulation to which financial institutions have to abide by, iii) reflect a more appropriate role for the Board, and iv) strengthen the emphasis on cross-border coordination and incident sharing.

Scalability

Financial institutions vary greatly in their size and in the nature of their activities, both across the financial sector as a whole (e.g. insurers vs. banks) and within different financial services sectors such as insurance (e.g. global insurers vs. captive insurers). As currently written, the Consultation Report takes the form of an extensive inventory of existing practices by large, internationally active financial institutions. As such it reads more as a guide on existing practices for large financial institutions rather than a toolkit for financial institutions of all sizes. Less resource-rich and less sophisticated firms could benefit from a toolkit that is proportionate not only to their type, size or financial profile, but also to the risks they are exposed to and the systems and services to be protected and maintained, thereby raising the overall level of cyber resilience in the financial sector. Therefore, GFIA respectfully encourages the drafters to consider how proportionality can be applied in this document so that smaller institutions can utilise the toolkit as appropriate.

Governance

Cybersecurity is no longer just an IT problem and is in fact a Board of Directors (Board) level discussion. In this regard, it is important that there is awareness of cyber risks across all levels of an organisation. Nevertheless, the requirements in paragraphs 1 ("Organisation-wide governance framework") and 2 ("Role and responsibilities of the board") are too onerous and place obligations on the board that are beyond corporate governance expectations and corporate law requirements. Direct oversight and responsibility of a firm's approach to cyber incident and response should reside with senior management while the Board's role should be to review, challenge, and give strategic guidance. Incorporating acknowledgement of the importance of appropriate liability protections for Senior Management and the Board could also be a useful reference point in the toolkit.

Global Federation of Insurance Associations (GFIA)
Secretariat: rue Montoyer 51, 1000 Brussels, Belgium
Tel: +32 2 894 30 81 E-mail: secretariat@GFIAinsurance.org
www.GFIAinsurance.org

GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

Cross-border coordination and information sharing

GFIA supports the cross-border coordination and trust information sharing concepts discussed in paragraphs 43 ("Cross-border coordination") and 44 ("Trusted information sharing"). To improve an organisation's preparations for and responding to cyber incidents, there is a need for greater sharing of data between agencies and jurisdictions. These efforts are important mitigation tools that prevent the spread of the same or similar cyber-attacks and allow companies to learn from and assess their own approach to cybersecurity in a risk-based manner. Similarly, sharing should involve reciprocal public/private arrangements.

The ex-ante analysis of a large number of aggregated past cyber incidents would allow for the threat landscape to be better understood. The establishment of a voluntary two-way reporting mechanism for the exchange of cyber incident reports (above a certain materiality threshold) between participating financial institutions and National Competent Authorities (NCAs) would allow NCAs to gather data on incidents and operate a feedback mechanism with financial institutions, who could draw upon incident data from across the financial sector to improve their own information and communication technologies (ICT) security. As an added layer, an incident exchange mechanism between the different NCAs would widen the pool of incident data, strengthening the added value of such a mechanism.

However, in response to Question 6.2, one the major impediments to cross-sectoral and cross-border testing exercises, and information sharing generally, are the reputational repercussions, whether between organisations in different jurisdictions or within the same jurisdiction. Reputational risks can affect an organisation's relationship with the public, its supervisor, and its peers. In this regard, any information-sharing framework, as well as participation in any exercise, must be on an anonymous and aggregated basis to ensure confidentiality. A liability safe harbor provision for companies that share information should also be considered.

There is also a great degree of fragmentation in the way that organisations collect and share information on cyber threats and incidents, due in particular to the fact that there is no one commonly used taxonomy. We appreciate the FSB's efforts to create a cyber lexicon to develop a consistent reference point for consistency across FSB's identified work streams for information sharing and cross-border guidance. That work with the appropriate legal precautions for its impact on any international arrangement or agreement or private contract may be a useful starting point, if any cross-border information-sharing initiatives were to be undertaken. Please refer to GFIA's August 20, 2018 comment letter for additional feedback specific to the Lexicon.

Cyber risk insurance

Finally, as with any emerging and complex risk, insurance is a valuable tool in crafting a risk management program. Cyber risk insurance offers customers many benefits. First and foremost, it is a valuable risk transfer mechanism, but it can also serve as a useful evaluation tool to accompany and assist in each individual business's risk calculations. Cyber insurance products also offer an increasing range of associated pre-event and post-event services that can play an important role in cyber incident response and recovery.

Unquestionably, though, cyber insurance is but one aspect of a far broader solution to increasing resiliency and cannot be a guarantor of security. It is a valuable risk transfer mechanism that organisations may want to consider in consultation with their insurer and/or broker. Taking time to evaluate insurance coverage and understanding

potential exposure due to insurance gaps is a useful and meaningful exercise for cyber-related loss recovery, therefore, FSB may consider an insurance gap analysis as part of the outlined response and recovery practices.

GFIA would like to thank the FSB for the opportunity to comment, and stands ready to answer any questions that you may have. GFIA's global reach promotes a broad awareness of the cyber landscape and its implications for standard setters. As such, the GFIA Cyber Risks Working Group welcomes the opportunity to have a thorough, ongoing dialogue with the FSB on cybersecurity issues.

GFIA Contact

Steve Simchak, Chair of the GFIA Cyber Risks working group (steve.simchak@apci.org)

James Padgett, GFIA secretariat (secretariat@gfiainsurance.org)

About GFIA

Through its 41 member associations and 1 observer association, the Global Federation of Insurance Associations (GFIA) represents the interests of insurers and reinsurers in 64 countries. These companies account for around 89% of total insurance premiums worldwide. GFIA is incorporated in Switzerland and its secretariat is based in Brussels.