

Mr Dietrich Domanski
Secretary General
Financial Stability Board
Centralbahnplatz 2
CH-4002 Basel

Zurich, 20 August 2018

Re: FSB consultation on Cyber Lexicon

Dear Mr Domanski,

We would like to thank the FSB for providing us with the opportunity to comment on the draft Cyber Lexicon.

The Geneva Association recognizes the potential of the Lexicon as a means to, over time, achieve a higher degree of cyber resiliency and cyber security in the financial sector. A robust take-up and acceptance of this lexicon may serve to drive a greater common understanding and cooperation in the financial sector (asset management, banking, CCPs and insurance) and relevant authorities on issues related to cyber resiliency and security. Indeed, widespread use of the lexicon in the financial sector, directly or as a foundation for other geography/ industry specific taxonomies, may also spur other industries to adopt the Lexicon. Preferably, the Lexicon would be adopted by standard-setting bodies (e.g., BCBS, IAIS, and IOSCO-CPMI) and jurisdictional regulators to produce a more consistent approach to cyber regulation across jurisdictions and bring about a clearer understanding of what constitute effective cyber security practices.

Cyber incidents are multidimensional and thus the Lexicon may encompass terms, which directly relate to impact, minimization, restoration and recovery. Insurance promotes resilience against cyber incidents and intends to encourage risk reduction behaviors and can provide compensation in case of cyber related incidents. Therefore, the insurance sector is a critical stakeholder in discussions on cyber risk and on how to assess, manage and mitigate that risk.

Specific to insurance, we believe a common cyber lexicon can help foster a shared language that can be applied consistently across jurisdictions and help promote disciplined growth in the cyber insurance market (i.e. clarifying coverage, expanding product offerings). It is generally acknowledged that a robust and healthy cyber insurance marketplace has a role to play in building cyber risk resiliency.

As to the specific questions raised in the Consultation Document, we have no comments on the criteria used (Questions 1 and 2). However, we would like to point to the need for some amendments, clarifications and modifications (Questions 3 and 4). Finally, we would like to comment on the further work on the Lexicon (Question 5).

Modifications to terms in the Lexicon

The Geneva Association proposes the following modifications to terms and their definitions in the draft Lexicon:

- Availability - Enabling timely and reliable access to authorized users (people, processes or devices) whenever it is needed (Adapted from ISO and NIST)
- Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information (adapted from NIST)
- Cyber - Relating to, within, or through the medium of the information technology.
- Cyber Resilience - The ability of an organization to continue to carry out its mission in the presence of actual or threatened stress or disruption to its information systems (adapted from CERT Glossary)
- Cyber Risk - Any type of risk emanating from the use of electronic data and its transmission, including technology tools such as the internet, information systems and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – being related to individuals, companies, or governments (adapted from IAIS (2016) Issues Paper on Cyber Risk to the Insurance Sector)
- Data Breach - Compromise of security that leads to the unauthorized disclosure of or access to protected personally identifiable data transmitted, stored or otherwise processed (DAB/TS)
- Integrity - Guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity (adapted from NIST)

In addition to the above suggested modifications, it would enhance clarity to replace some common and well-understood terms. For example, rather than having the generic term **Information Sharing** it would be optimal to use the term **Threat Intelligence** or **Threat Intelligence Sharing**.

Terms suggested to be removed from the draft Lexicon

We propose that two terms, **Campaign** and **Cause of Action** be deleted from the proposed Lexicon. The focus of the Lexicon is, amongst others, to promote cyber resilience, and we think that these terms do not align with this objective.

New terms suggested

We take note that the Lexicon is designed to be limited in scope and focused on the core terms necessary to support its objectives. Moreover, the Lexicon is supposed to be delivered to the G20 summit in Buenos Aires in November this year. Hence – except for so-called Affirmative Cyber and Non-Affirmative Cyber, see below - we shall refrain from suggesting terms to be added which do not directly relate to terms which are included in the draft Lexicon.

However, going forward we would be keen to discuss how to develop the Lexicon (reference to question 5). We have work undergoing in order to develop a number of suggested definitions for terms that could eventually be added at a later date. We are interested to take this work further and to engage in a dialogue with the FSB on this at a later stage.

Reference to Affirmative Cyber and Non-Affirmative Cyber

In light of the objective to develop a common language that promotes resilience, The Geneva Association proposes to differentiate between affirmative and non-affirmative cyber. The insurance industry uses the terms affirmative and non-affirmative cyber in their policies, marketing and general parlance. The definitions below provide illustrative definitions.

- **Affirmative cyber risk** are those risks contained within insurance policies that explicitly include coverage for cyber risk.
- **Non-affirmative cyber risk** are those risks within insurance policies that do not explicitly include or exclude coverage for cyber risk.

The Geneva Association proposes the explicit inclusion of these terms to drive commonality and universal understanding of the terms. Moreover, explicit recognition of Affirmative and Non-affirmative cyber risk help better monitor cyber risk and cyber risk mitigation efforts. It could help foster a robust cyber insurance market because it would be made clear that cyber risk is a risk in its own right.

Reference to other sources where the Cyber Lexicon is not exhaustive

Given the Lexicon's objective is not to provide definitions where they already exist and are commonly employed it might be useful to develop a plan of gradual expansion of the terminology. For example, as the Lexicon gains traction among authorities, the financial sector and beyond, there is the potential for the Lexicon to incorporate commonly used terminology or to provide a preference regarding which alternative definition is optimal.

The Geneva Association is strongly committed to continue the constructive dialogue and cooperation with the FSB and we will be happy to work further with the FSB on the Lexicon. Should you have any questions on the issues raised in this letter, please contact Rachel Anne Carter (rachel_carter@genevaassociation.org) or Peter Skjoedt (peter_skjoedt@genevaassociation.org).

Yours sincerely,



Anna Maria D'Hulster
Secretary General

The Geneva Association

The Geneva Association is the leading international insurance think tank for strategically important insurance and risk management issues. The Geneva Association identifies fundamental trends and strategic issues where insurance plays a substantial role or which influence the insurance sector. Through the development of research programmes, regular publications and the organisation of international meetings, The Geneva Association serves as a catalyst for progress in the understanding of risk and insurance matters and acts as an information creator and disseminator. It is the leading voice of the largest insurance groups worldwide in the dialogue with international institutions. In parallel, it advances— in economic and cultural terms—the development and application of risk management and the understanding of uncertainty in the modern economy.

The Geneva Association membership comprises a statutory maximum of 90 chief executive officers (CEOs) from the world's top insurance and reinsurance companies. It organises international expert networks and manages discussion platforms for senior insurance executives and specialists as well as policymakers, regulators and multilateral organisations.

Established in 1973, The Geneva Association, officially the 'International Association for the Study of Insurance Economics', is based in Zurich, Switzerland and is a non-profit organisation funded by its Members.