Swiss Re

August 2018

Response to Cyber Lexicon Consultative Document

Dear colleagues,

We would like to thank the FSB for providing us with the opportunity to comment on the draft Cyber Lexicon. Swiss Re has provided input to the response of the Geneva Association and supports the feedback provided therein.

In addition, on the issue of whether any additional terms are appropriate, or if existing terms should be modified or deleted, Swiss Re proposes some added terms and modifications to terms already within the Lexicon. We urge the FSB to consider adding these additional terms:

Privacy Violation: The collection or use of data and information of a person or entity without adequate consent or for a different purpose then consented to.

Network Security Liability: The liability encountered by an organization if its IT-systems or networks create a disturbance in a third-party system or enable the transfer or transmission of malicious software and activities to a third-party system.

Communication and Media Liability: The liability encountered in case of any kind of defamation (e.g. slander, libel) and for infringement or misappropriation of copyrights, patents, trademarks and trade secrets.

Crisis Management costs, Incident Management Costs, Event Management Costs: Additional costs incurred to deal with a cyber incident, whether malicious or not, such as Incident Analysis, Forensics, Credit Monitoring Costs, Notification Costs, Public Relation Costs (communication, protection of reputation), Assistance (e.g. psychologic support) for cyber bullying/mobbing, Remediation costs.

Data Restoration / Reinstatement: Costs to reinstate, recreate or restore lost or corrupted data. It often includes cost to replace hardware made unusable by the cyber event.

Cyber Terror: A disruptive or destructive cyber event, targeted at physical or non-physical systems (such as data and IT-systems) committed for political, religious, ideological or similar purpose including or with the intention to influence any government or to put the public, or any section of the public, in fear.

Cyber War, Cyber Warfare: A disruptive or destructive cyber event, targeted at physical or non-physical systems (such as data and IT-systems) considered as act of war (whether declared or not),

hostilities or warlike operation, military operations or by or under the order of any foreign government.

Cyber Crime, Cyber Fraud: Cyber internal or external malicious activity designed to commit fraud, thefts, illicit payments, transfers or claims of money or other financial assets.

Cyber Extortion/Ransomware: Threat(s) directed against a person's computer system or digital assets if this person does not comply with the request of the originator of the threat.

Phishing: Fraudulent attempt to obtain sensitive information such as but not limited to usernames, passwords, credit card details, by disguising as a trustworthy entity in an electronic communication.

We understand that the FSB seeks to maintain a lexicon that is concise and effective. Cyber insurance has the potential to significantly mitigate the impact of global cyber risks, and we believe that a sound definition of these terms is essential to facilitate the further growth of the cyber insurance market.

We urge the FSB to contact us if a further discussion is desired.

Best regards,

Dr. Eric Durand, Head Cyber Center of Competence

Dr. Nina Arquint, Head Group Qualitative Risk Management