Intesa Sanpaolo comments on "Cyber Lexicon Consultative Document"

Financial Stability Board

July, 2018

Contents

Introduction

The Financial Stability Board (FSB) is working since to protect financial stability against the maliciuous use of ICT, considering that a damage to a single bank or institution can have consequences on the whole financial ecosystem. In March 2017, following the Communiqué issued at the meeting of the G20 Finance Ministers and Central Bank Governors, the FSB was asked to perform a stocktake of existing relevant released regulations and supervisory practices in G20 jurisdictions and to identify effective practices. Such stocktake was provided in October 2017 based on survey responses among the FSB members and a public-private sector workshop in September 2017; Intesa Sanpaolo also participated in last September workshop.

The latest initiative by the FSB about cooperation and common efforts to guarantee financial stability against the malicious use of ICT is the production of a non-mandatory common lexicon with the following objectives:

- Cross-sector common understanding of relevat cyber security and cyber resilience;
- Work to assess and monitor financial stability risks of cyber risk scenarios;
- Information sharing as appropriate;
- Work by th FSB and/or standard-setting bodies (SSBs) to provide guidance related to cyber security and cyber resilience, including identifying effective practices.

The FSB is asking members the following five questions about the common lexicon draft to be answered by 20 August 2018:

Q1. Are the criteria used by the FSB in selecting terms to include in the draft lexicon appropriate in light of the objective of the lexicon?

Q2. Are the criteria used by the FSB in defining the terms in the draft lexicon appropriate in light of the objective of the lexicon?

Q3. In light of the objective of the lexicon, should any particular terms be deleted from, or added to, the draft lexicon?

Q4. Should any of the proposed definitions for terms in the draft lexicon be modified?

Q5. Going forward and following the publication of the final lexicon, how should the lexicon be maintained to ensure it remains up to date and a helpful tool?

Intesa Sanpaolo comments

Q1 - Are the criteria used by the FSB in selecting terms to include in the draft lexicon appropriate in light of the objective of the lexicon?

We find the criteria used by the FSB in selecting terms to include in the draft lexicon to be appropriate in light of the objective.
The only suggestion we believe can be helpful for a better understanding of the criteria for selection of terms is to better clarify the third one: "*Exclusion of technical terms*".

Reasoning: it is not completely clear what the FSB means for *technical*, considering the presence of terms such as "Access Control", "Authentication" or "Configuration Management".

Q2 - Are the criteria used by the FSB in defining the terms in the draft lexicon appropriate in light of the objective of the lexicon?

We find the criteria used by the FSB in defining the terms in the draft lexicon to be appropriate in light of the objective of the lexicon.

Q3 - In light of the objective of the lexicon, should any particular terms be deleted from, or added to, the draft lexicon?

We propose to add the following terms:

Term	Definition
Likelihood of occurrence of a threat	Probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities Source: adapted from NIST
Likelihood of success of a threat	Probability that a given threat, once initiated, will result in adverse impact Source: adapted from NIST
Social Engineering	Psychological manipulation of individuals (customers or employees) to induce certain actions or to disclose confidential information Source: adapted from ECB
Insider/Third Party Provider Event Misuses of access rights	An event that is made by employees or former employees, as well as third party suppliers, which involves the accidental or intentional failure to respect the security policies and the right of access to the systems Source: adapted from ECB
Unauthorised access (intentional)	A wide range of incidents through which a hacker intentionally accesses networks, data or systems in an unlawful manner Source: adapted from ECB

Term	Definition
Sabotage (physical attack)	Sabotage/destruction of equipment and/or assets through physical access Source: adapted from ECB
Accidental events	Accidental events, such as human errors Source: adapted from ECB
External events	Events caused by external factors Source: adapted from ECB
Software problem/ system failure	Malfunctions of applications or basic software programs/ Performance degradation of services Source: adapted from ECB
Hardware problem	Incidents due to malfunctions of hardware systems and components Source: adapted from ECB
Infrastructural issue	Incidents due to infrastructure malfunctioning, communication networks or shared platforms. Such events may arise due to external factors or internal Source: adapted from ECB
Key Persons/Skills Unavailability	Events due to the unavailability of key persons or specific skills during the process activity Source: adapted from ECB
External Provider Issues	Events due to technical and/or operational issues of Third Party Providers Source: adapted from ECB

Reasoning: considering the presence of terms such as "Malware", "DoS" and "DDos", we propose to add the terms defined in the previous table in order to provide exhaustive coverage for cyber security events taxonomy.

Sources

ECB	European Central Bank, Annex B – Reporting Significant Cyber Incidents (2017)
NIST	NIST Special Publication 800-30, Appendix B – Glossary

Q4 - Should any of the proposed definitions for terms in the draft lexicon be modified?

We propose the following modifications:

Term	Current Definition	Proposed Definition
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities or processes.	Property that information is not made available or disclosed to unauthorized individuals, entities, process *or system.*
Reasoning: we suggest to add also "system" for completeness.		
Cyber Risk	The combination of the probability of cyber events occurring and their consequences.	*Any type of risk emanating from the use of electronic data and its transmission, including technology tools such as the internet 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.* *Source: IAIS (2016) Issues Paper on Cyber Risk to the Insurance Sector*
Reasoning: we suggest to modify the definition in order to better specify what cyber risk is.		
Identify	Develop the organizational understanding to manage cyber risk to systems, assets, data and capabilities.	Develop the organizational understanding to manage cyber risk to *assets.*
Reasoning: we suggest this simplification, given the definition of "Asset" that already includes people, information, infrastructure, finances and reputation.		
Protect	Develop and implement the appropriate safeguards to ensure delivery of services.	Develop and implement the appropriate safeguards to ensure delivery of services *and to guarantee confidentiality, availability and integrity of data*.
Reasoning: we suggest this change in order to make the definition more complete than only referring to "delivery of services".		

Q5 - Going forward and following the publication of the final lexicon, how should the lexicon be maintained to ensure it remains up to date and a helpful tool?

We suggest reviewing the Cyber Lexicon at least twice a year, every six month, in order for it to be updated with the latest threats that can be found.

We also want to point out some issuet to be taken into account in developing a maintenance process for the lexicon:

- a public consultation for every review could protract the period needed for a new release of the lexicon to be published;
- beyond the bi-annual regular review, in order for the lexicon to be updated, it could be useful to define changes / events that can trigger extra-reviews;
- it can be useful to define a procedure also for keeping into consideration adivces and recommendations by members for adding / modifying / deliting / correcting terms or definitions outside public consultation periods.