Financial Stability Board consultation on a Cyber Lexicon, 20 August 2018

Dear Sir/Madam,

Please find below replies to questions set out in the public consultation by the Financial Stability Board on a draft Cyber Lexicon to support the FSB in its work to protect financial stability against the malicious use of ICT. The replies are made in a personal capacity.

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?... Should additional criteria be used?

The criteria (of meeting the objective and scope of the lexicon and excluding technical, general business and regulatory terms) in selecting terms seems fine. As an observation, overall, the terms are generic that could apply to almost all sectors; it is appreciated that cyber incidents are global and there is a need to address cross-sector understanding. Given the Lexicon's intent to focus only on the financial sector, however, there seems lacking a sense or 'feel' that the terms relate to the sector *per se*; it seems therefore there might be a challenge for consideration to meet needs of both the generic and the specific. Perhaps some user examples relating to the financial sector could be added as appropriate (eg, suggestion in Q4 below regarding TLP).

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? ... Should any additional criteria be used?

The criteria of reliance on existing sources and having sufficiently comprehensive and plain language definitions are fine to define terms. A challenge is to monitor changes in the cyber security environment for additional and updated sources of information, not necessarily in glossary form, eg, https://www.cybok.org.uk.

Q3. In light of the objective of the lexicon, should any particular terms be deleted from, or added to, the draft lexicon? If any particular terms should be added, please suggest a definition, along with any source material for the definition and reasons in support of inclusion of the term and its definition.

The term 'Attribution' might be added: the cause of cyber incidents is often tied to configuration mis-management, human error, or internal non-malicious events, compared to targeted external 'attacks'. The latter is where the term attribution is applied traditionally to refer to external 'Threat Actors', another term in the draft Lexicon (source, eg, https://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks).

The term 'Encryption' might be added; it has also become more topical. Many existing sources will have definitions.

The term 'Vulnerability Assessment' perhaps can be renamed as 'Threat and Vulnerability Assessment', or 'Risk Assessment', and then the definition can be adjusted to include threat as well as vulnerability assessment.

Q4. Should any of the proposed definitions for terms in the draft lexicon be modified? If so, please suggest specific modifications, along with any source material for the suggested modifications and reasons in support thereof.

With reference mainly to the criteria of plain language, the following are suggested modifications to some terms:

Cyber risk: to substitute the word '*probability*' with the word '*likelihood*'. This is a common misinterpretation and while it may seem a nuance it is an important distinction. (source: other bodies of knowledge, including from health and safety executives (eg, https://www.hsa.ie/eng/Topics/Hazards, www.hse.gov.uk/risk/theory/alarpglance.htm) and from 'Official (ISC)2 Guide to the CISSP CBK pp 103-105.

Confidentiality: suggest reordering of words to read: "Property that information is not *disclosed or made available* to unauthorised individuals, entities or processes." (placing 'disclosed' first is suggested to de-emphasise 'not made available' which might be confused with 'denial of service')

Cyber Incident: suggest appending text: "*An incident is 'neutral' until such time cause and/or attribution is established*." (source: lessons learned from information security incident investigation reports many available online, and from Y2K mitigation)

Denial of Service: suggested rewording to read: "*The deliberate disruption to the availability of information systems to authorised users that results in the loss or delay of access to information*."

Penetration Testing: suggest appending text: "…*usually with a view to improve enterprise-wide cyber security controls*. *This is not to be confused with vulnerability testing which tests simply for the presence of a vulnerability and not, as in penetration testing, also exploiting it."*

Traffic Light Protocol: suggest rewording to read: "*A method of labelling the communication of sensitive information with a choice of four colours to indicate the access and sharing level of the intended audience.*"

Additionally, perhaps a way to meet the challenge of Q1, is to incorporate a phrase by way of a financial user/ compliance example. The following might be considered to append to TLP definition:

"For example, communication of reports of suspicious financial transactions to be shared with a small trusted audience might use red or amber coloured labels; such information would not likely be placed on the public Internet which would likely be a communication using a white label."

(source: Suspicious transaction reporting aligns with requirements for all States to implement various mandatory UN Security Council Resolutions, through national legislative and regulatory processes.)

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?

This challenge of 'future proofing' applies to other glossaries and bodies of knowledge whether or not addressing the financial sector. As also with reviews of international treaties, options might include designating an existing committee to include a role that addresses issues of the Cyber Lexicon and/or appointing a group of persons with mixed expertise that meets periodically.

Thank you.

Olivia Bosch PhD (encryption export controls)
Director, International Security and Communications Ltd, UK
former UK Member to a NATO ICT advisory panel
former UK Expert to a UN Security Council subsidiary body