WORLD FEDERATION OF EXCHANGES

August 2018

WFE Response to the Financial Stability Board (FSB):
Cyber Lexicon

Visit us at:
www.world-exchanges.org

Background

The World Federation of Exchanges (WFE) is the global trade association for exchanges and clearing houses, representing more than 200 Market Infrastructure Providers. Our members include exchange groups and standalone CCPs.[1]

Our members are both local and global, operating the full continuum of market infrastructures in both developed and emerging markets. Of our members, 36.8% are in Asia-Pacific, 42.6% in EMEA and 20.6% in the Americas. WFE exchanges are home to nearly 45,000 listed companies, and the market capitalisation of these entities is over $82.5 trillion; around $81.8 trillion (EOB) in trading annually passes through the infrastructures WFE members safeguard.[2]

The WFE works with standard setters, policy makers, regulators and government organizations around the world to support and promote the development of fair, transparent, stable and efficient markets. The WFE shares regulatory authorities' goals of ensuring the safety and soundness of the global financial system, which is critical to enhancing investor and consumer confidence, and promoting economic growth.

Cyber security matters have been – and continue to be – a matter of great priority for our membership, and one in which significant time, effort and money has been invested. We therefore welcome the opportunity to offer our perspectives and further contribute to the dialogue in order to secure the shared objectives of fair and orderly markets that promote the safety and resilience of the global financial system.

Executive Summary

The WFE applauds the FSB's objective of setting cyber lexicon as it is very helpful as an industry to have a consistent set of terms. We believe that most of the definitions work, as a general proposition and as between themselves. However, we believe the lexicon would be more effective if the definitions were anchored exclusively in two sources: the definitions provided by 1) the International Organization for Standardization (ISO) and 2) the National Institute of Standards and Technology (NIST) – These two are the distinguished sources for Technical, Risk Management, Cyber Security and Information Security standards. Both (ISO and NIST) glossaries of key terms are more comprehensive than other sources. Our concern stems from the fact that when incorporating definitions from a number of different sources – and due to varying definitions across sources more generally – the terms used can result in some inconsistency throughout the lexicon. The terms are also at varying levels of detail, so we stress that either the FSB align the definitions with those of ISO/NIST or care should be taken when selecting terms from different sources in order to maintain consistency.

Ideally, the WFE believes that it would be most helpful to provide feedback into the relevant organisations (i.e. ISO/NIST) on where the terms should be unified and provide guidance, so they can agree a common lexicon between them which can be at a consistent level with referential integrity between definitions.

1 The WFE membership list can be found here
2 As at end 2017

WFE Comments

Question 1. *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? (See Section 2 for the objective, Section 3.2 for the criteria and the Annex for the lexicon.) Should additional criteria be used?*

No major comments. Meeting the objectives, limiting the scope on "core" (high-level) terms, excluding detailed technical description seems like a good fit relative to the objectives of the lexicon.

Question 2. *Are the criteria used by the FSB in defining the terms in the draft lexicon appropriate in light of the objective of the lexicon? (See Section 3.3 for the criteria.) Should any additional criteria be used?*

No major comments. Reliance on existing sources works on a broad level. Terms should be selected from established sources, i.e., ISO and NIST. If other sources are used, care must be taken to ensure that selecting terms from separate sources doesn't create a disjointed list.

Question 3. *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.*

Threat

The lexicon defines Vulnerability and Vulnerability Assessment but jumps straight to Threat Actor without defining Threat. As such, we propose the following definitions:

- **Threat** – *Any circumstance or event with the potential to adversely impact organisational operations (including mission, functions, image, or reputation), organisational assets, individuals, other organisations, or the Nation through an information system via unauthorised access, destruction, disclosures, modification of information, and/or denial of service. Source: https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf*
- **Threat Objective** – *The end goal or action pursued by any combination of threat actors, vectors, and methods.*
- **Threat Objective Lifecycle** – *A high-level risk assessment and cybersecurity strategy prioritisation approach that focuses on adversary objectives rather that identities, actors, tools, techniques, or vectors. The threat objective lifecycle methodology defines a small number of specific actions such as sabotage, extortion, or fraud and is useful for Board-level discussion on the areas of focus for a cybersecurity strategy.*

Indicators of Compromise (IOCs)

We understand IOCs to be the specific characteristics that can be used to identify a compromised system with a level of confidence (e.g. a file hash). That may or may be as the result of an "intrusion" [this term is not defined in the lexicon] and due to variance in confidence may or may not be considered evidence.

Other terms to include:

- **Authorisation** – *Access privileges granted to a user, program, or process or the act of granting those privileges. Source: https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf*
- **Flaw Remediation** – *An organisation identifies, reports, and corrects information system flaws; tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; installs security-relevant software and firmware updates within [Assignment: organisation-defined time period] of the release if the updates; and incorporates flaw remediation into the organisational configuration management process. Source: https://nvd.nist.gov/800-53/Rev4/control/SI-2*
- **Intrusion** – *Unauthorized act of bypassing the security mechanisms of a system. Source: https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf*
- **Resilience** – *The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning. Source: https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf*

Question 4. *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.*

Penetration Testing

The definition of Vulnerability Assessment is at a different level of detail from a Penetration Test (which enumerates and attempts to actively exploit vulnerabilities). The definitions do not lead to a clear understanding of the differences. As such we provide an alternative definition for Penetration Testing:

- **Penetration Testing** – *A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system. Source: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf*

Situational Awareness

Regarding the definition of Situational Awareness it is not very clear as to why it has been defined in this manner. Given it is a military term that has been co-opted for Security Operations, it is suspected that non-experts will not be much wiser from the definition supplied. As such, we propose an alternative definition:

- **Situational Awareness** – *Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future. Source: https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf*

Threat

Our proposed definitions for Threat Objective and Threat Objective Lifecycle do in fact overlap with the existing FSB's definitions, respectively, for Campaign (which focuses on behaviors and goals over identification of threat actors) and Course of Action (as an approach to taking response and combating risks). In the interest of keeping the lexicon concise, we would suggest replacing the definitions for Campaign and Course of Action with our proposed definitions:

- **Threat Objective (as an alternative to Campaign)** – *The end goal or action pursued by any combination of threat actors, vectors, and methods.*
- **Threat Objective Lifecycle (as an alternative to Course of Action)** – *A high-level risk assessment and cybersecurity strategy prioritisation approach that focuses on adversary objectives rather that identities, actors, tools, techniques, or vectors. The threat objective lifecycle methodology defines a small number of specific actions such as sabotage, extortion, or fraud and is useful for Board-level discussion on the areas of focus for a cybersecurity strategy.*

Question 5. *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 too?*

Maintaining the lexicon has its apparent challenges as the criteria for inclusion relies on existing sources, which may change independently. The fact that the scope of the terms to be included in the lexicon is limited to "core" terms should make the need for updates less frequent. **One option would be for FSB to engage participants through a consultative process on a regular basis, for example every 3 years.**