THE
INVESTMENT
ASSOCIATION

Secretariat to the Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland

The Investment Association
Camomile Court, 23 Camomile Street,
London, EC3A 7LL

T +44 20 7831 0898
E enquiries@theia.org
W theinvestmentassociation.org
Twitter @InvAssoc

Date: 20 August 2018

Dear Sir/Madam,

RE: FSB Cyber Lexicon Consultation

The Investment Association (IA) champions UK investment management, supporting British savers, investors and businesses. Our 250 members range from smaller, specialist UK firms to global investment managers with a UK footprint. Collectively, they manage £6.9 trillion of savers' and investors' money. The UK asset management industry is the largest industry of its kind in Europe and the second largest in the world.

The investment management industry is not immune to cyber risks. Highly professional and highly motivated cyber criminals are continually developing new techniques and seeking new targets. Recent high profile attacks highlight the importance of addressing the risks and mitigating the impact of cyber attacks on overall financial stability.

To address ever-evolving cyber threats, action needs to be taken across financial services. Basic understanding, effective information sharing and appropriate risk monitoring are key initial actions to begin building industry wide cyber resilience.

The IA, therefore, welcomes the creation of a Cyber Lexicon by the FSB to be used across the investment management industry. Following its presentation to the G20 in November 2018, we hope the Cyber Lexicon is widely adopted to create a common understanding and approach to cyber risks across the investment management industry. The current narrow focus and simplicity could undermine firms' willingness to fully adopt the Cyber Lexicon. Our responses to the questions in the Consultation aim to identify actions that could be taken to ensure the Cyber Lexicon more fully achieves its overall objective.

We hope this feedback is useful and would welcome further involvement in future discussions on this topic.

Yours sincerely,

Pauline Hawkes-Bunyan

Director – Risk, Compliance & Tax

Date: 20 August 2018

FSB CYBER LEXICON CONSULTATION RESPONSE

ABOUT THE INVESTMENT ASSOCIATION

The Investment Association (IA) champions UK investment management, supporting British savers, investors and businesses. Our 250 members range from smaller, specialist UK firms to global investment managers with a UK footprint. Collectively, they manage £6.9 trillion of savers' and investors' money. The UK asset management industry is the largest industry of its kind in Europe and the second largest in the world.

EXECUTIVE SUMMARY

The investment management industry is not immune to cyber risks. Highly professional and highly motivated cyber criminals are continually developing new techniques and seeking new targets. Recent high profile attacks highlight the importance of addressing the risks and mitigating the impact of cyber attacks on overall financial stability.

To address ever-evolving cyber threats, action needs to be taken across financial services. Basic understanding, effective information sharing and appropriate risk monitoring are key initial actions to begin building industry wide cyber resilience.

The IA, therefore, welcomes the creation of a Cyber Lexicon to be used across the investment management industry, enhancing a high-level understanding of key cyber security terms.

The draft Cyber Lexicon successfully covers core terms that describe the main components and risks associated with cyber security.

If the Cyber Lexicon is widely adopted and used consistently across the investment management industry, it has the potential to align and improve the effectiveness of information sharing, risk monitoring and future guidance development. It is important to ensure the content is not too narrowly focussed or the definitions too simplistic.

To ensure accuracy and relevance the Cyber Lexicon should be regularly reviewed by the investment management industry, wider financial services and Standards Setting Bodies (SSBs) utilising it and calibrated with technical knowledge of leading expert agencies.

The FSB should consider creating additional layers of the Cyber Lexicon to provide more comprehensive insight into cyber security risks.

The Cyber Lexicon has the potential to go beyond the objectives stated in the Consultation. Having a commonly adopted set of terms could be used to enhance board level understanding and engagement with cyber issues, encourage global cooperation, and increase awareness of cyber security risks and their importance to third party suppliers for the investment management industry.

Responses to the questions asked in the Consultation can be found below. We hope this will provide the FSB with useful feedback and suggestions to address potential issues to help the FSB Cyber Lexicon more fully achieve its overall objectives. We would welcome further involvement in future discussions on this topic.

INTRODUCTION

In May the IA released the report, 'Building Cyber Resilience in Asset Management'[1]. The report states that "cyber crime is a growing global industry now estimated to make criminals over $400 billion a year. Cyber attackers are becoming more determined and more skilled than ever. Highly professional and highly motivated, they are continually developing new techniques and seeking new targets to attack."

The IA has established a senior level Cyber Security Committee to address policy and legislation issues regarding cyber risks and cyber-enabled financial crime in addition to the impact of cyber security risk and compliance issues on business operations and performance.

Further action needs to be taken across the investment management industry and wider financial services to protect financial stability from cyber risks. Basic understanding, effective information sharing and appropriate risk monitoring are key initial actions to begin building industry-wide cyber resilience.

The IA welcomes the creation of a Cyber Lexicon by the FSB to be used across the investment management industry. Following its presentation to the G20 in November 2018, we hope the Cyber Lexicon is widely adopted to create a common understanding and approach to cyber risks across the investment management industry. The current narrow focus and simplicity could undermine firms' willingness to fully adopt the Cyber Lexicon. Our responses to the questions in the Consultation aim to identify actions that could be taken to ensure the Cyber Lexicon more fully achieves its overall objective.

[1] IA Report: Building Cyber Resilience in Asset Management https://www.theinvestmentassociation.org/media-centre/press-releases/2018/ia-helps-asset-managers-tackle-cyber-security-threats.html

RESPONSES TO QUESTIONS

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?

Overall, the proposed scope and reasoning for selecting the terms in the draft Cyber Lexicon appear to meet the objectives stated in the Consultation.

The majority of terms describe cyber security terminology in a high-level manner that is digestible for non-technical professionals.

Using this Cyber Lexicon will improve basic common understanding across the investment management industry and wider financial services. This shared knowledge will contribute to more effective information sharing and will help to align future guidance created by the SSBs. It will be important to ensure that, in a rapidly changing technological landscape, this does not result in a limited monitoring of cyber risks.

The Cyber Lexicon should not be treated as a definitive list of the only terms necessary to understand cyber risks. The FSB should consider recommending additional information sources or expand upon the existing Cyber Lexicon. This would improve understanding of more niche concepts associated with core terms currently defined in the Cyber 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? SHOULD ANY ADDITIONAL CRITERIA BE USED?

The criteria used to define terms in the Cyber Lexicon have facilitated the development of simple, comprehensive definitions based on pre-existing expert material that appear to meet the objectives stated in the Consultation.

The plain language used should help to create a common high-level understanding of core terms across the investment management industry and wider financial services. This will aid the translation process and, therefore, international alignment.

We welcome the use of plain language and the creation of internationally accepted terminology. This will allow discussion of the issues by boards and other non-technical specialists. However, it is important to remember that the Cyber Lexicon will also provide an opportunity for specialists to discuss the risks and required actions and it therefore needs to be sufficiently detailed and kept up to date.

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 SOURCE MATERIAL FOR THE DEFINITION AND REASONS IN SUPPORT OF INCLUSION OF THE TERM AND ITS DEFINITION.

Traffic Light Protocol (TLP)

> "Traffic Light Protocol (TLP) - A set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colours to indicate expected sharing boundaries to be applied by the recipients"
> Source: FIRST

The FSB should consider deleting the term 'Traffic Light Protocol (TLP)' from the Cyber Lexicon as the definition does not appear to support the objectives stated in the Consultation. For example, many other areas of cyber security could be measured using traffic light labelling, such as prioritising when a cyber event should be investigated following detection, or labelling of the severity of a cyber incident.

Including the current definition of 'Traffic Light Protocol' could suggest that firms should change their internal cyber security processes to facilitate this term and ensure its accuracy across all those using the Cyber Lexicon. This in turn could undermine firms' willingness to engage with the Cyber Lexicon.

Phishing

> "The misleading of individuals into disclosing sensitive information by claiming to be a trustworthy entity in an electronic communication."
> Source: Adapted from NIST SP 800-82 Rev.2

The FSB should consider including the above term for 'Phishing' in the Cyber Lexicon as the current draft includes a definition for 'Distributed Denial of Service', which is a common method of cyber attack. 'Phishing', is another extremely common cyber risk and should be included. Covering such terms will improve the range of cyber risks covered and therefore support the Cyber Lexicon achieve its overall objectives and improve its usefulness.

Supply Chain Risk

> "Risks that arise from the loss of confidentiality, integrity, or availability of information systems due to a failure or breach of a third party supplier."
> Source: Adapted from NIST SP 800-161

The FSB should consider including the above term for 'Supply Chain Risk' in the Cyber Lexicon. The investment management industry is becoming increasingly interconnected and more reliant on services provided by third parties. Attacks on, or failures of, third party suppliers could prove to be a significant cyber risk to the investment management industry and overall financial stability. Considering the potential implications of supply chain breaches, 'Supply Chain Risk' should be considered as a core term to be included in the Cyber Lexicon.

Removable Media

> "Portable data storage medium, such as a USB memory stick, that can be added to or removed from a computing device or network."
> Source: Adapted from CNSSI 4009-2015

The FSB should consider including the above term for 'Removable Media' in the Cyber Lexicon. Portable storage mediums are a common part of information system use. Such devices are commonly utilised to facilitate cyber attacks by installing malware. As a significant part of information system use and a potential significant cyber threat, 'Removable Media' should be considered as a core term to be included in the Cyber Lexicon.

Mobile Device

> "A portable computing device that: (i) is small enough to easily be carried by a single individual; (ii) is designed to operate without a physical connection; (iii) possesses local, non-removable data storage; and (iv) is powered for extended periods of time with a self-contained power source. Examples include laptops, smart phones, tablets, and E-readers."
> Source: Adapted from CNSSI 4009-2015

The FSB should consider including the above term for 'Mobile Device' in the Cyber Lexicon. All sectors, including the investment management industry, are becoming increasingly accommodating of flexible and mobile working. This shift in working culture means that firms' information systems are vulnerable to additional threats via mobile devices and how

the workforce uses them. This could be the source of significant cyber threat and overall risk to financial stability.

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.

Definitions that are seen as too general to fulfil the remit of the Cyber Lexicon have been noted, with more detailed definitions provided below.

Authentication

> "Provision of assurance that a claimed characteristic of an entity is correct."
> Source: ISO 27000:2018

This current definition, noted above, could be considered overly vague when addressing the purpose and process of authentication in relation to the usage of information systems.

To address this concern, the FSB should consider modifying the term 'Authentication' to:

> "Verifying the identity of a user, process or device as a prerequisite to allowing access to resources in a system."
> Source: NIST SP 800-33

Threat Actor

> "An individual, a group or an organisation believed to be operating with malicious intent."
> Source: Adapted from STIX

This current definition, noted above, does not address the fact that not all cyber attacks are carried out with malicious intent. Some threat actors can unwittingly be the cause of a significant cyber breach that could threaten customers, the firm and financial stability as a whole.

To address this concern the FSB should consider modifying the term 'Threat Actor' to:

> "Either (i) intent and method targeted at the intentional exploitation of a vulnerability; or (ii) a situation and method that may accidentally trigger a vulnerability"
> Source: NIST SP 800-18 Rev. 1

Cyber Resilience

> "The ability to anticipate and adapt to changes in the environment and withstand, contain and rapidly recover from a cyber incident."
> Source: Adapted from CPMI-IOSCO and NIST (definition of 'Resilience')

This current definition, noted above, appears to be more tailored towards resilience too generally rather than cyber resilience of information systems and what that entails.

The FSB should consider modifying the term 'Cyber Resilience' to the following to address this concern:

> "The ability of an information system to continue to operate while under attack even if in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack."
> Source: NIST SP 800-30

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?

It is important to ensure that this Cyber Lexicon remains relevant in order to achieve the objectives stated in the Consultation.

The FSB should consider forming a committee or series of interlinked groups to collaborate with the FSB. The group(s) should be representative of the whole financial services sector and SSBs. Participation could include individuals from the FSB, SSBs, trade body representatives as well as those who are responsible for risk, operations and information security teams in investment management firms at board or senior level. This gives a broad spectrum of those who would be utilising the Cyber Lexicon and be able to provide different experiences of its usefulness.

The group(s) should meet regularly to discuss how useful the Cyber Lexicon has proven to be, anywhere it may be lacking and ideas for improvement based on the practicality of guidance produced and information sharing.

It may also be useful to liaise with law enforcement and other national and international cyber security bodies. Such bodies outside the investment management industry and the wider financial services industry may have additional expertise in cyber security. Utilising such expertise will allow the Cyber Lexicon to be calibrated from a more in-depth technical perspective to address cyber risks that could impact the investment management industry and overall financial stability.

FURTHER INFORMATION

For further information, please contact:
[Lorna Sharpe, lorna.sharpe@theia.org, +44 20 7269 4690]