FSB Consultative Document on Achieving Greater Convergence in Cyber Incident Reporting - Comments from Swift

1 Introduction

Swift appreciates the opportunity to provide comments to the FSB's Consultative Document on Achieving Greater Convergence in Cyber Incident Reporting. Overall, we strongly welcome greater global convergence in this area and fully support the FSB's work to this end.

Like many global operators, we are faced with inconsistent requirements from different authorities around cyber incident reporting. The landscape is becoming increasingly complex, and it is challenging to monitor the new and changing requirements in different jurisdictions. We also see that different jurisdictions apply different timelines for reporting and also use different terminology. Greater convergence in this field would thus be very helpful and would in our view not only reduce compliance burdens, but also contribute to enhanced cybersecurity.

2 Questions & Answers

(Swift's comments in bold)

2.1 Challenges to achieving greater convergence in CIR (Section 2)

1. Is the emphasis on practical issues to collecting and using cyber incident information consistent with your experience? Does your institution want to provide any additional evidence for the FSB to consider from your experience?

The plethora of requirements and lack of standardisation is seen as major risk to complying with regulation regarding CIRs. Taking a pragmatic approach in this matter – and therefore a focus on removing/preventing practical issues related to CIR - is key for organisations operating under multiple authorities to make reasonable efforts to be in compliance. We encourage the focus on a pragmatic approach by the FSB.

2.2 Recommendations (Section 3)

2. Can you provide examples of how some of the practical issues with collecting and using cyber incident information have been addressed at your institution?

As part of upcoming changes in CIR regulation, we are analysing several CIR requirements. We conclude that significant operational efforts will have to be made to comply with the differences in requirements between authorities. We attempt to address the practicalities by designing templates, handling guidelines and playbooks.

3. Are there other recommendations that could help promote greater convergence in CIR?

Increased standardisation of reporting and reporting templates would be helpful in promoting greater convergence in CIR. To this end, we would encourage the FSB to explore existing standards for re-use in a cybersecurity setting. For example, the ISO 20022 standard includes a Legal Entity Identifier (LEI) which could be used to identify parties involved or affected by an incident.

4. Could the recommendations be revised to more effectively address the identified challenges to achieving greater convergence in CIR?

No answer.

2.3 Common terminologies for CIR (Section 4)

5. Will the proposed revisions to the Cyber Lexicon help to encourage greater adoption of the Cyber Lexicon and promote greater convergence in CIR? Are there any other ways in which work related to CIR could help to encourage greater adoption of the Cyber Lexicon and promote greater convergence in CIR?

We appreciate the FSB's proposal to update its Cyber Lexicon, which since its publication has promoted a much-needed cross-sectoral, common understanding of relevant cybersecurity terminology across the financial sector industry and relevant stakeholders. It has helped in reducing fragmentation and promoting shared cyber security terminology understanding. However, as cyber security is a discipline that is continually evolving, continuous updates should be envisaged in addition to the forthcoming update.

6. Do you agree with the definition of 'cyber incident,' which broadly includes all adverse events, whether malicious, negligent or accidental?

We agree with the definition of a cyber incident. It should be free of intent and based on impact. We further recommend clarity on what the criteria for reporting should be.

An example would be an unsuccessful exploitation attempt. If the activity was not successful, it does not create any impact, but shows intent for targeting. Is this reportable?

7. Are there other terms that should be included in the Cyber Lexicon to cover CIR activities?

No answer.

8. Are there other definitions that need to be clarified to support CIR?

A Cyber Alert is an indication that a Cyber Event has occurred. A cyber event can then indicate that a cyber incident has occurred. The current definition in the lexicon is that a cyber alert is an indication that a cyber incident has occurred, this leaves out a cyber event, which the presence of a singular event, or correlation of multiple events is the indicator that an incident has occurred in the past or is presently occurring.

For clarity, the definition of "indicators of compromise" should include examples such as "File names / hashes, process names, registry entries, etc."

2.4 Format for Incident Reporting Exchange (FIRE) (Section 5)

9. Would the FIRE concept, if developed and sufficiently adapted, usefully contribute towards greater convergence in incident reporting?

A successful Format for Incident reporting Exchange (FIRE) framework should allow for flexibility of incident reporting. For instance, the initial (urgent) incident notification should be simple, consist of only high-level information and be actionable, so that the receiver understands the content and its use.

10. Is FIRE readily understood? If not, what additional information would be helpful?

No answer.

11. If FIRE is pursued, what types of organisations (other than FIs) do you think would need to be involved?

No answer.

12. What preconditions would be necessary to commence the development of FIRE?

No answer.

*****END OF DOCUMENT*****