EBF responses to FSB consultative document on Achieving Greater Convergence in Cyber Incident Reporting

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 EBF agrees with the content of Section 2 and particularly highlights the need for convergence of cyber incident reporting (CIR) definitions, templates, and thresholds. Between the proliferation of fragmented CIR requirements and the increasing complexity of the current threat environment, CIR and broader information sharing efforts have been challenging. Monitoring and thwarting cyber threats and vulnerabilities and remediating cyber incidents could benefit from convergence of CIR requirements, as financial institutions could focus more on protecting the firm from future cyber incidents and remediating confirmed cyber incidents, rather than complying with disparate CIR requirements. Voluntary information sharing has been challenging as financial institutions struggle to provide quality cyber incident information to financial authorities because the public and private sectors do not maintain a trusted relationship. For example, firms find it difficult to report incidents, threats and vulnerabilities to the authorities without knowing the policy objectives and how the data will be used (e.g. could there be a negative impact on the firm if the financial authority shares the firm's data publicly?).

The EBF supports the FSB's overall efforts to harmonize incident reporting requirements globally, however, the following aspects of the consultative document cause concern:

- The materiality-based triggers (2.2) in incident reporting frameworks are particularly hard to use, given that it is difficult to fully describe or measure the impact of an incident as it emerges. For this reason it is important that firms are allowed to determine materiality based on their greater understanding of the risk of the cyber incident to which they have unique insights.
- There are not clear and defined reporting mechanisms for cyber incidents, triage and support and industry awareness, which is a separate reporting mechanism outside the numerous regulatory and legal requirements.
- Regarding 2.3, it should be considered what would happen in case an incident is reported using FIRE to different authorities and any of them decides to issue a media statement. Coordination between the authorities that received the report would be required. The FSB should encourage financial authorities to protect data and keep it confidential, unless otherwise stated by the financial institution.

Examples:

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

i) Within the UK, there are multiple mechanisms to report a cyber incident or seek support to triage or discuss an incident with FI peers. For instance, there is the Financial Emergency Cyber Call (FinEcc) run by the Financial Services Cyber Coordination Centre (FSCCC).. Financial Services Information Sharing and Analysis Centre, (FS-ISAC), is active in the UK with a large proportion of the industry as participants. FS-ISAC also operates broadly throughout the EU.

The UK National Crime Agency and UK National Cyber Security Center (NCSC) can invoke a FinECC, when they have information they wish to share with FSCCC Firms. In addition, there may be instances where non-member financial firms might invoke a FinECC by contacting the FSCCC, NCSC, NCA, CDA or FS-ISAC directly. UK financial institutions may use this mechanism for sharing of threat intelligence, but reporting of material cyber incidents also takes place directly between the compromised firm and their regulators There are other similar information sharing initiatives, for instance the Financial Services Cyber Security Centre (FS-CSC) in Switzerland[1] and the Cyber Information and Intelligence Sharing Initiative (CIISI-IE) in Ireland[2]. It is noted that in both the UK and Swiss models, FS-ISAC is a partner organization which allows for leveraging of their global network.

ii) For a given large Swedish bank with additional operations in another EU Member States, one (1) large enough incident would trigger the following incident reporting schemes:

1. Reporting of a significant event to the S-FSA
2. PSD2 incident reporting to the S-FSA
3. GDPR incident report to the Swedish Authority for Privacy Protection
4. NIS incident reporting to the Swedish Civil Contingencies Agency
5. Informal incident reporting to the Swedish Central Bank
6. ECB cyber incident reporting
7. 2nd EU MS FSA incident reporting
8. 2nd EU MS NIS incident reporting

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?

Financial institutions are facing the same issues that are identified in the consultative document, mainly disparate timeline, materiality threshold and template requirements across financial authorities.

As an incident first emerges and then develops, banks need to constantly analyse the incident and compare it to multiple incident reporting frameworks at the same time to determine what should and what should not be reported under what incident reporting framework; -"what services are in scope of the incident, how many users are affected, how many transactions are affected, how long has the incident lasted" etc-. Some of the

[1] https://fscsc.ch/en/

[2] https://www.centralbank.ie/financial-system/operational-resilience-and-cyber/cyber-resilience/cyber-information-intelligence-sharing-initiative

larger institutions have been considering to establish dedicated and centralised incident reporting teams on a Group level to be able to manage incident reporting to a large number of authorities in a correct and timely manner.

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

Supervisors should engage in bi-directional information sharing with the private sector. Once cyber incident information is reported to financial authorities, they should strive to provide comprehensive, timely and actionable feedback to the industry, particularly around potential sector wide issues. However, we note that threat intelligence for events which do not meet the threshold for reporting or which do not have an impact are best shared through voluntary information groups such as those listed above. Ensuring there is an effective feedback loop will build a trusted relationship between financial authorities and financial institutions. The creation of centralized reporting hubs to simplify incident reporting should be considered, with a view to build a global network of intelligence reporting hubs. A good example is the Danish incident reporting portal[3], as presented also in the EBF position on Cyber incident reporting.

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

All recommendations appear to be relevant and identifying a particular pinch-point within cyber incident reporting and where agreement is required for convergence.

However, regarding recommendation 8, the terms "materiality" and "likely" are conflicting. This is also not aligned with the new Cyber Lexicon definition of cyber incident, as they are excluding the "potential impact" factor. Financial institutions need to be able to focus on confirmed, significant incidents as an influx of likely incidents could overwhelm financial authorities and drive financial institutions' focus away from threat monitoring. Therefore, the FSB should not require the inclusion of "likely breaches" as it has done in Recommendation 8 (Extend materiality-based triggers to include likely breaches).

Also, reporting deadlines should be harmonized, and an initial assessment must also be possible before the first report. The type of reporting should depend on the policy objective and materiality of the incident. First, if the policy objective is early warning, then an incident notification (or an initial assessment in the referenced text) should be done prior to submitting any detailed report. Second, materiality could determine whether incident data is shared with the regulator or through an information sharing mechanism.

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?

The proposed revisions to the Cyber Lexicon are agreeable, as definitions are using recognized cyber industry standards (i.e. NIST) to enhance definitions and help encourage greater adoption of the Cyber Lexicon. We welcome the use of Cyber Lexicon as standardized definition for all FI & FA across all geographies, including the EU. For this to

[3] https://virk.dk/myndigheder/stat/ERST/selvbetjening/Indberetning_af_brud_paa_sikkerhed/

materialize, local supervisors need to adopt and implement the lexicon, which to a great extent has not happened so far.

We would recommend further awareness raising campaigns or other mechanisms to encourage adoption and use of the Cyber Lexicon to achieve greater convergence in CIR. This would support commonality across CIR reporting no matter where the report originates from. In addition, this will ensure that FIs, Authorities and supporting agencies have a single authoritative document for cyber definitions.

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 FSB's decision to remove "jeopardizes" from the definition of cyber incident to limit the scope to incidents that cause "actual" harm. Financial institutions need to be able to focus on confirmed, significant incidents as an influx of likely incidents could overwhelm financial authorities and drive financial institutions' focus away from threat monitoring. However, while the definition specifically eliminates "potential impact" from the equation, there is a recent recommendation from ECB (OSI) to include it in the definition. There is the concern on how these two requests will be aligned, as the same definition must be used by Financial Institutions and Financial Authorities.

It should also be noted that, outside the industry, with the general public, the understanding of a "cyber incident" would most likely be that it is malicious and not non-malicious, or operational.

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

The EBF proposes the inclusion of the following terms:

"*Materiality thresholds*": This would clarify and complement the definition of cyber incident.

"*Supply Chain Risk*": We believe it is important to include this new term, as the EBA Guidelines do not define it and we do not deem adequate the current definitions in NIST.

"*Third party service provider*": We believe that it is important to include this new term in alignment with the definitions in the EBA Guidelines. We would propose to join the two existing ones:

"Third Party: An organization that has entered into business relationships or contracts with an entity to provide a product or service"

"Service Provider: means a third-party entity that is undertaking an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement".

"*Cloud Services*"

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

- Trusted entity: Insider Threat definition mentions "trusted entity" without defining it.
- Compromise
- Denial of Service

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?

International authorities should **promote** and **disseminate** the FIRE concept and create a culture of cyber incident convergence. To this aim, **connections** with other definitions and concepts already included in other cybersecurity frameworks or cyber incidents reporting systems should be exploited (i.e., EBA Guidelines, NIS2 Directive, NIST Cyber Security Framework). Particularly on the EU level and the adopted DORA Regulation, it seems likely that the relevant level-2 requirements on incident reporting will already be prepared when the FIRE-framework would be introduced, so these efforts would require coordination. Ideally, FIRE could also be used by authorities outside of financial services, for instances for reporting under the EU's NISD2 framework or to national CERTs.

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

We would like to clarify whether FIRE is a template or a tool, as it does not become clear throughout the document. Should it be a template, it could have benefits, but a tool or platform (complying with all legal and security requirements) could be better for standardization and automation.

If the format could be used as a taxonomy, more information could be added as definitions from the Cyber Lexicon. Further, it could include examples of categorization in order to be more useful. Also, interim solutions and/or procedures to contain an incident might be useful for authorities to understand.

Lastly, supporting documentation would be needed alongside the report to ensure that data reporting (especially within impact assessment section) is normalized, consistent with clear definitions. We would suggest considering expanding the Supplemental Section (1.5.3) so that detailed Indicators of Compromise can be entered, and that the data can be extracted in formats suitable for 1st Line Cyber Security analysts to upload into security tooling to check for matches or to update for alerting.

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

Since cyber incidents may affect not only the financial sector but also others (as for example energy, transport and health sector), we consider very useful to **coordinate with international authorities and organizations** to define cross-sector needs and respond to them effectively. Also, it would be particularly helpful should third party providers (TPPs) -such as Cloud Service Providers (CSPs)- use FIRE to report to FIs or Fas.

Indicatively, the following authorities should be involved: European Commission, ENISA, National CERTs, National Cyber Security Centres, FS-ISAC, MDR / SIEM Vendors (for those FI's who supplement internal security operations centre or utilise these for cyber security incident triage and handling), and any other authority regulating cyber security incidents and impact.

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

Starting from the FIRE concept and its dissemination, a **reconciliation path** can be defined, which allows **comparisons** on an international level and the definitions of

historical trends. There should be a commitment by regulatory Authorities to adopt FIRE for their national CIR.

Due to the sensitivity of FIRE reporting within the FI sector, we would recommend the following preconditions:

- Defined secure communications method and process
- Automation Enablement
- Defined recipients of FIRE reporting within each organisational entity (e.g., FI, Regulatory, National, Cyber)
- Addressing identified sources of operational challenges
- Ensure that there is sufficient adoption levels and commitment within the FI community and wider G20 including a central design position across member countries.

Also, as noted above (question 9), the timing vis-à-vis the EU-level may be concerning, with DORA level-2 requirements to be devised in the next 18 months.

About EBF

The European Banking Federation is the voice of the European banking sector, uniting 32 national banking associations in Europe that together represent some 4,500 banks - large and small, wholesale and retail, local and international - employing about 2.1 million people. EBF members represent banks that make available loans to the European economy in excess of €20 trillion and that securely handle more than 300 million payment transactions per day. Launched in 1960, the EBF is committed to creating a single market for financial services in the European Union and to supporting policies that foster economic growth.

www.ebf.eu @EBFeu

For more information contact:

Dimos Karalis
Policy Adviser, Cybersecurity & Innovation
d.karalis@ebf.eu
+32 485 52 39 16