FSB FINANCIAL STABILITY BOARD

19 October2020

Cyber Incident Response and Recovery

Overview of Responses to the Public Consultation

On 20 April 2020, the Financial Stability Board (FSB) published a consultative document *Effective Practices for Cyber Incident Response and Recovery*[1] that proposed a toolkit of effective practices to assist organisations in their cyber incident response and recovery activities (CIRR). The toolkit leverages on the FSB Cyber Lexicon, that was developed in 2018 to facilitate more effective communication and support the work of the FSB, standard-setting bodies (SSBs), authorities and private sector participants to address financial sector cyber resilience.[2]

The FSB received 58 responses to the public consultation from banks, insurers, industry associations and public authorities.[3] In addition, the FSB held four virtual outreach meetings in early July, reaching out to over 300 private sector participants, to receive feedback on lessons learnt from the COVID-19 pandemic and on the consultative document. Respondents generally welcomed the consultative document, particularly amid an increase in cyber threats due to remote and split-team working environments in light of the COVID-19 pandemic.

This note summarises the main issues raised in the public consultation, including the virtual outreach meetings, and describes the changes that have been made to the toolkit ('the final toolkit') to address them.

1. General comments

The following describes some of the general comments received on the consultative document and how they were reflected in the final toolkit.

- **Lessons learnt from the COVID-19 pandemic**. Many respondents mentioned that they faced different challenges that arose from remote working in light of the COVID-19 pandemic. Some said that remote working made it more challenging to coordinate cyber incident reporting and take prompt action. One respondent mentioned that certain activities previously conducted onsite, such as documenting digital evidence and forensic analysis, became inaccessible during remote working. Some had to reassess interconnectedness with critical third-party vendors and suppliers, who had their own

---

1 FSB (2020), *Effective Practices for Cyber Incident Response and Recovery: Consultative Document*, April.

2 FSB (2018), *Cyber Lexicon*, November.

3 The consultation responses that could be made publicly available are published on the FSB's website: https://www.fsb.org/2020/08/public-responses-to-consultation-on-effective-practices-for-cyber-incident-response-and-recovery/.

difficulties with remote working. Many respondents mentioned that phishing tactics also evolved to take advantage of the COVID-19 situation. The final toolkit includes the need for organisations to reflect these lessons learnt into their scenario analysis, plans and playbooks as well as in the overall cyber resilience strategy.

- **Application of the toolkit**. Although the consultative document stated that the "toolkit does not constitute standards for organisations or their supervisors and is not a prescriptive recommendation for any particular approach", many respondents expressed the need to emphasise that the toolkit is not a new standard or regulation. To address this, the final toolkit includes an introduction with a subsection on the toolkit, which further clarifies the nature of the toolkit as a resource and reference guide.[4]

- **Proportionality**. Many respondents noted that the toolkit should be implemented flexibly and proportionally, depending on the size and complexity of an organisation. In particular, there are smaller organisations that may not have the resources or necessity to implement all the tools. Organisations are also in different sectors and jurisdictions, and at different maturity levels, so not all tools are relevant for all types of organisations. Further clarifications were included in the final toolkit to emphasise that it provides a range of effective practices and that organisations can choose to adopt some or all of the effective practices that are suitable for their respective business model, taking into account their size, complexity and risks to the financial ecosystem in which they operate.

- **Cyber Lexicon and incident reporting**. Several respondents highlighted the need for updating the FSB Cyber Lexicon, noting that some of the terms used in the Lexicon and the toolkit (e.g. "incident") could go further in encouraging authorities to adopt more harmonised practices based on existing frameworks or may need further elaboration. In relation to this, these respondents also highlighted the need for enhanced coordination among authorities on cyber incident reporting. The FSB will consider whether to review the Cyber Lexicon and ways to enhance coordination as part of its forward work programme.

- **Benefits for authorities**. Several respondents sought clarity on how authorities would use the toolkit. The final toolkit states that the toolkit aims to promote a common range of effective practices that SSBs and authorities can incorporate into their guidance around cybersecurity.

2. Comments on the CIRR components

Most respondents' cybersecurity frameworks include the seven components of the FSB toolkit to some extent, with some including additional components, such as 'Identification' and 'Prevention'. The final toolkit does not include these components as the toolkit focuses on the

[4] Specifically, the final toolkit states that it is composed as a resource and reference guide for effective practices, using common cyber-taxonomies in a manner aligned to industry standards accessible to senior management, board of directors or other compliance, risk, and legal professionals that interface with cybersecurity technical experts within the organisation, the SSBs or the authorities.

Respond and Recover functions at organisations, and hence, assumes that the incident has already been identified and not prevented.

Some respondents suggested that the tools for a few of the components were broader than implied by the component's name, and that the list of components could be better sequenced. For instance, a few respondents noted that 'Preparation' reflects steps taken before a cyber incident is identified and involves steps for how to mitigate the impact of an incident. Also, some suggested that 'Restoration' is not only about restoring systems 'back to normal' but also recovering data. The final toolkit has renamed 'Preparation" to "Planning and preparation" to better reflect that these tools should be in place before a cyber incident happens. The component "Restoration" is now called "Restoration and recovery" to better reflect that the tools are also helpful for recovering data.

3. Enhancements to specific tools

Across the seven components, a number of effective practices were added to reflect feedback from respondents, including additional examples provided in the boxes. Out of the 46 tools listed in the consultative document, all but nine tools were substantively modified to include additional examples of effective practices and to provide clarity on what the tool aims to achieve. In light of the feedback from the public consultation, three new tools were added, which resulted in a total of 49 tools.

The most substantive comments received were related to the Governance component. Many respondents considered the tools related to roles and responsibilities as being too prescriptive and conflicted with organisations' established governance and control practices. More specifically, many respondents expressed concerns that Tool 2 in the consultative document, on roles and responsibilities of the board, placed too many operational responsibilities on the board that are better suited for senior management. The final toolkit delineates more clearly between the roles and responsibilities of the board and of senior management.

In addition, respondents generally considered Tool 3 in the consultative document, related to roles, responsibilities and accountabilities for CIRR, as too focused on assigning key responsibilities to individuals: incident owner; scribe/independent observer; and media spokesperson. In the final toolkit, these roles are no longer prescribed and have been converted to tools that an organisation can draw upon depending on its size, complexity and risk.