FSB FINANCIAL STABILITY BOARD

Cyber Incident Response and Recovery

Progress Report to the G20 Finance Ministers and Central Bank Governors meeting in Fukuoka, 8-9 June 2019

28 May 2019

The Financial Stability Board (FSB) is established to coordinate at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations under the FSB's Articles of Association.

Contacting the Financial Stability Board
Sign up for e-mail alerts: www.fsb.org/emailalert
Follow the FSB on Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Cyber Incident Response and Recovery[1]

Progress Report to the G20 Finance Ministers and Central Bank Governors meeting in Fukuoka, 8-9 June 2019

Introduction

Cyber incidents[2] pose a threat to the stability of the global financial system. The twin episodes of the NotPetya and the WannaCry ransomware attack in 2017 demonstrated the potential of cyber incidents to be both widespread and devastating. Financial institutions not only have to guard against cyber threats but must also be ready to respond to and recover from an incident safely and swiftly. Ensuring that financial institutions are resilient to cyber incidents is crucial for a smooth functioning of the financial system and in engendering financial stability.

The Financial Stability Board (FSB) has been working on enhancing cyber resilience of financial institutions to promote financial stability. Following a stocktake of publicly available regulations, guidance and supervisory practices on cyber security in the financial sector in 2017,[3] the FSB published the Cyber Lexicon in November 2018.[4] This comprises a set of approximately 50 core terms related to cyber security and cyber resilience in the financial sector.

Building on these efforts, at the October 2018 Plenary meeting, the FSB agreed on the importance of having in place effective practices relating to a financial institution's response to, and recovery from, a cyber incident. In this regard, the FSB established a working group on Cyber Incident Response and Recovery (CIRR). The mandate of the CIRR is to develop a toolkit of effective practices to assist financial institutions, as well as for supervisors and other relevant authorities, in supporting financial institutions, before, during and after a cyber incident. The toolkit is not intended to be an international standard nor a prescriptive approach for financial institutions or their supervisors.

This project seeks to mitigate the implications of cyber incidents on financial stability, by taking into account their cross-border and cross-sectoral nature. It will also leverage on the shared experience and diversity of perspectives gathered in the course of this work. As part of the process, the development of effective practices will incorporate a stocktake of publicly released

---

1 To help promote a common understanding, this report uses terms defined in the FSB Cyber Lexicon. See FSB (2018) Cyber Lexicon, November.

2 A cyber incident is a cyber event that:

(i) jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or

(ii) violates the security policies, security procedures or acceptable use policies,

whether resulting from malicious activity or not. See FSB (2018), page 9.

3 FSB (2017), Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices, October.

4 FSB (2018).

guidance from national authorities and international bodies, a review of case studies on past cyber incidents and various engagements with external stakeholders.

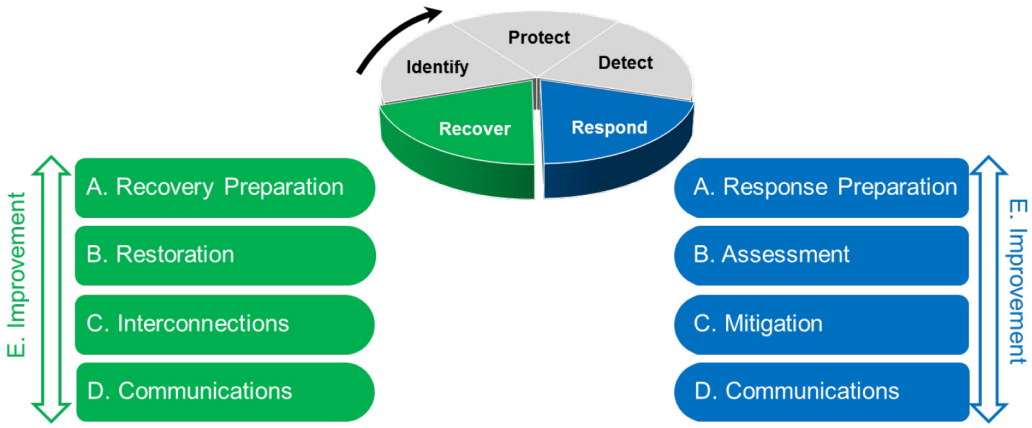
This progress report summarises the CIRR's work to date and its workplan for developing effective practices for cyber incident response and recovery.

1. Defining the components of respond and recover functions

Enhancing cyber resilience is often characterised by a set of functions. The toolkit of effective practices will focus on the *Respond* and *Recover* functions. The *Respond* function involves the development and implementation of the appropriate activities following a detected cyber event.[5] The *Recover* function involves the development and implementation of the appropriate activities to restore and maintain any capabilities or services that were impaired due to a cyber incident.[6]

To take this project forward, the CIRR has preliminarily identified five components for the respective functions, which are broadly in line with existing standards on cyber security.[7] These components (labelled A to E for each function) are illustrated below.

Components of the Respond and Recover functions[8]



[5] Any observable occurrence in an information system. Cyber Events sometimes provide indication that a Cyber Incident is occurring. See FSB (2018), page 8.

[6] FSB (2018), page 12.

[7] For example, the US National Institute of Standards and Technology (NIST) describes the components of the Respond function as (i) response planning, (ii) communications, (iii) analysis, (iv) mitigation and (v) improvements and the components of the Recover function as (i) recovery planning, (ii) improvements, and (iii) communications. For further details, see NIST (2018), Framework for Improving Critical Infrastructure Cybersecurity, April, page 23.

[8] These components and their definitions will be further refined in light of CIRR work going forward.

Each component will set out a desired outcome and be broadly mapped to existing national and international standards that are most relevant for the financial sector. This will form the foundation for the development of effective practices. The components of the *Respond* and *Recover* functions and their stated outcome will be further developed according to the findings from the stocktake, the literature review and outreach to external stakeholders. Each of these streams of work are elaborated below.

2. Development of the toolkit of effective practices

The development of the toolkit of effective practices relating to a financial institution's response to, and recovery from, a cyber incident will be taken forward in two phases. The first phase of work will continue until October 2019 and focuses on identifying and developing effective practices. The second phase of work will likely commence during the last quarter of this year and will focus on drafting of the toolkit. It will subsequently involve a public consultation to be conducted in early 2020.

Phase 1: Identification and development of effective practices (March – October 2019)

This first phase of work was launched in January 2019 and will continue through October 2019. It will include:

- *Literature review*: CIRR noted that there is already an extensive amount of publicly available studies on how firms have responded to, and recovered from, a cyber incident. This literature review will hence cover cyber incident experiences in both financial and non-financial sectors given that threats are cross-border and cross-sectoral in nature. Further, as many financial institutions rely on other third-party service providers, it will be important to review the broader linkages across an economic ecosystem, not just at the individual firm level.
- *Stocktake of international bodies*:[9] The CIRR will launch a survey in June 2019 to take stock of the work since 2017 by other international bodies on cyber-related incident response and recovery. This survey will update the FSB's cyber security stocktake conducted in 2017 but with specific focus on cyber incident response and recovery.
- *Stocktake of national authorities*: In June, the CIRR will initiate a stocktake of publicly released guidance issued by national authorities, which will also leverage on the FSB's 2017 stocktake, but delve more deeply into the components of the *Respond* and *Recover* functions. The survey will also seek authorities' views on observed key challenges and effective practices at financial institutions in their jurisdiction.
- *Engagement with external stakeholders*: The CIRR will launch in July an online survey from the FSB website for completion by interested parties within six weeks.

[9] International bodies include the Basel Committee on Banking Supervision (BCBS), Committee on the Global Financial System (CGFS), Committee on Payments and Market Infrastructures (CPMI), G7 Cyber Experts Group, International Association of Insurance Supervisors (IAIS), International Accountings Standard Board (IASB), International Monetary Fund (IMF), International Organization of Securities Commissions (IOSCO), Organisation for Economic Cooperation and Development (OECD) and the World Bank.

National authorities may also choose to interact directly with external stakeholders in their jurisdiction. The survey aims to collect a diverse range of perspectives on industry practices relating to cyber incident *Respond* and *Recover* functions, as well as some of the key challenges. Once the online survey is launched, there will be further engagement with external stakeholders through bilateral meetings and workshops.

The findings from these various streams of work will be consolidated, assessed and discussed at the CIRR's meeting in Singapore on 2-3 October 2019.

Phase 2: Drafting and consultation of the toolkit (November 2019 – September 2020)

After the first phase of work is completed, the CIRR will focus on drafting a toolkit of effective practices for cyber incident response and recovery. This second phase of work also includes issuing a public consultation document in early 2020, with additional engagement with external stakeholders.

The final toolkit will incorporate the feedback from the public consultation and be published following FSB Plenary approval in September 2020.