Cyber Incident Response and Recovery[1]

Survey of Industry Practices

At the October 2018 Plenary meeting, the Financial Stability Board (FSB) agreed to develop effective practices relating to a financial institution's response to, and recovery from, a Cyber Incident.[2] The toolkit is intended to provide financial institutions and authorities with a set of effective practices and will be based on the shared experience and diversity of perspectives gathered by the FSB working group on Cyber Incident Response and Recovery (CIRR) in the course of its work. It is not intended to create an international standard or adopt a prescriptive approach for financial institutions or their supervisors.[3]

Enhancing cyber resilience is often characterised as involving a set of functions, e.g. the Identify, Protect, Detect, Respond and Recover functions.[4] The toolkit of effective practices focuses on the Respond and Recover functions.

The development of effective practices for Cyber Incident response and recovery will be informed by a review of publicly available documents on how firms have responded to and recovered from past Cyber Incidents; a stocktake of relevant publicly released guidance issued by national authorities and international organisations; and responses to this survey on industry practices. This survey is a key element of the FSB's outreach strategy with external stakeholders (e.g. financial institutions, industry groups, academics, Cyber Resilience experts) to gather views on effective practices relating to financial institutions' response to, and recovery from, a Cyber Incident.

---

1 To help promote a common understanding, the survey uses terms defined in the FSB Cyber Lexicon and these are denoted in initial capitals. 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 For details on the CIRR work, see FSB (2019) Cyber Incident Response and Recovery: Progress Report to the G20 Finance Ministers and Central Bank Governors meeting in Fukuoka, 8-9 June 2019, May.

4 US National Institute of Standards and Technology (NIST) (2018), Framework for Improving Critical Infrastructure Cybersecurity, April, Version 1.1.

Table 1 provides definitions for the components used in this survey. The definitions aim to help provide some consistency in the survey responses and may be refined as CIRR work to develop effective practices progresses, based on inputs from various stakeholders.

Table 1: Definitions of Components

Preparation	Establish and maintain capabilities to respond to Cyber Incidents, and to restore critical functions, processes, systems, data and activities affected by Cyber Incidents to normal state through disruption.
Communication	Develop, deploy, manage and coordinate communications with internal and external stakeholders.
Improvements	Establish processes to improve response and recovery capabilities through lessons learnt from past Cyber Incidents, exercises and other relevant sources.
Analysis	Analyse Cyber Incidents to ensure effective response and support recovery activities.
Mitigation	Contain the spread and propagation of Cyber Incidents both internally and externally in a timely manner, and minimise or alleviate the impact.
Interconnectedness	Identify and assess the risk arising directly or indirectly from and to relevant participants in the ecosystem and actively mitigate the risks.

Instructions

The toolkit of effective practices is aimed at assisting financial institutions in their cyber response and recovery activities, which can be conducted as an individual institution or collectively with other firms and/or with authorities. The FSB recognises, however, that lessons can be drawn from experiences outside the financial sector, as cyber risk is a cross-sectoral and cross-border issue. As such, this survey aims to collect information on industry practices from both the financial and non-financial sectors (herewith referred to as 'industry') on response and recovery of critical services, including restoration of data integrity following a Cyber Incident that could have an impact on financial stability.

More specifically, the objective of the survey is to identify the key challenges and effective industry practices related to the Respond and Recover functions.

- The **Respond function** involves the development and implementation of the appropriate activities to take action regarding a detected Cyber Event.[5]
- The **Recover function** involves the development and implementation of the appropriate activities to maintain plans for Cyber Resilience and to restore any capabilities or services that were impaired due to a Cyber Incident.

A set of components have been identified (see Table 1), which are drawn from discussions among CIRR members and existing standards related to cybersecurity.[6] The FSB will identify effective practices for each of these components.

Participation in this online survey is voluntary. Some national authorities may ask their supervised financial institutions to complete the survey and to send their completed response directly to them.

All responses to the online survey are automatically anonymised before being shared with the CIRR unless a respondent indicates otherwise. Responses, whether anonymised or non-anonymised, will only be reviewed by CIRR members and members of the FSB Secretariat supporting this project. The individual responses will not be made public. Further, the FSB will not associate any given practice with a particular entity or respondent in the toolkit. Responses to the survey should focus on observed practices in responding to and recovering from cyber incidents, with a particular focus on mitigating and addressing financial stability risks. Responses should avoid addressing matters related to national security. Respondents also should avoid providing any firm-specific information that could reveal the firm's identity, particularly for those respondents that want to remain anonymous. To the extent possible, responses should use terms as defined in the Cyber Lexicon.

Section 1 collects general information to help provide some insight on whether industry practices differ by sector or international presence and whether respondents rely on a set of national or international standards for their cyber Response and Recovery activities.

Sections 2 and 3 collect information on industry practices related to Cyber Incident response and recovery. Respondents are also asked to share information for (i) activities as an individual organisation and (ii) activities carried out collectively with other parties (e.g. other financial institution(s), authorities) especially if the responses differ. The FSB aims to develop effective practices for each of these components. Section 4 seeks input on whether there are other categories that should be considered in the development of the toolkit.

The information collected from the survey will be used solely for this FSB project to develop a toolkit of effective practices for Cyber Incident Response and Recovery.

Please submit your completed survey by Wednesday, 28 August.

---

[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] This includes the US National Institute of Standards and Technology (NIST), ISO 27001, ISACA COBIT, CPMI-IOSCO Guidance on cyber resilience for FMIs, and G7 Fundamental Elements of Cybersecurity for the Financial Sector. See Annex for further examples of standards.

1. Baseline questions

1. How would you characterise your organisation?

- ☐ Bank
- ☐ Insurer
- ☐ Financial Market Infrastructure
- ☐ Trading Venue or Exchange
- ☐ Broker-Dealer
- ☐ Asset Manager
- ☐ Pension Fund
- ☐ Corporate
- ☐ Other (Please specify)

2. In how many jurisdictions do you have operations and infrastructure within your control that may be affected by a Cyber Incident?

- ☐ < 5
- ☐ 6-10
- ☐ 11-25
- ☐ 26-40
- ☐ 41-50
- ☐ More than 50
- ☐ Other (Please specify)

3. Which jurisdiction is your principal country of operation?

4. Which of the following frameworks or standards, if any, do you look to approach for Response and Recovery? Please check all the relevant boxes.

- ☐ NIST Framework for Improving Critical Infrastructure Cybersecurity
- ☐ ISO 27001/ISO 27002
- ☐ ISO/IEC 27031
- ☐ ISO/IEC 27035
- ☐ ITIL
- ☐ ISACA COBIT
- ☐ CPMI-IOSCO Guidance on cyber resilience for FMIs
- ☐ G7 Fundamental Elements of Cybersecurity for the Financial Sector
- ☐ FSSCC The Financial Services Sector Cybersecurity Profile

☐ Other (Please specify)

5. Would you like your response to be anonymous? (yes/no)

   If no:
   a. Name of your firm:
   b. Can the FSB Secretariat contact you to follow-up on your responses? (yes/no)
   c. If yes: Email address.

2. Component questions

2.1 Preparation

6. How are risks stemming from third-party dependencies addressed as part of Cyber Incident response and recovery preparation?

   Please elaborate on both **response preparation** and **recovery preparation** (if applicable).

7. What are the key challenges and effective practices associated with implementing governance arrangements for evaluating, directing or monitoring responses to and recovery from Cyber Incidents?

   Please elaborate on both **key challenges** and **effective practices**.

8. What are the key challenges and effective practices associated with acquiring and maintaining people resources with appropriate skills and knowledge to satisfy the roles, responsibilities and accountabilities needed to respond to and recover from Cyber Incidents?

   Please elaborate on both **key challenges** and **effective practices**.

9. What are the key challenges and effective practices associated with identifying, delivering and maintaining facilities, equipment, technical solutions, information sources, or external services required to support Cyber Incident response and recovery?

   Please elaborate on both **key challenges** and **effective practices**.

10. What are the key challenges and effective practices associated with validating with sufficient confidence that Cyber Incident response and recovery capabilities are present and meet stakeholder expectations?

    Please elaborate on both **key challenges** and **effective practices**.

11. What are the key challenges and effective practices associated with restoration of critical business services after a Cyber Incident?

    Please elaborate on both **key challenges** and **effective practices**.

12. What are the key challenges and effective practices associated with restoring data integrity and addressing data leakage following a Cyber Incident?

    Please elaborate on both **key challenges** and **effective practices**.

2.2 Communications

13. What are the key challenges associated with sharing information about response and recovery activities with internal stakeholders (e.g. the board)?

    Please elaborate on both **response activities** and **recovery activities** (if applicable).

14. Which internal stakeholders should be considered in response or recovery communication planning?

    Please elaborate on both **response communication planning** and **recovery communication planning** (if applicable).

15. What types of information should be communicated to internal stakeholders with respect to Cyber Incident response and recovery?

    Please elaborate on both **Cyber Incident response** and **Cyber Incident recovery** (if applicable).

16. What are the key challenges associated with sharing information about response and recovery activities with external stakeholders (e.g. customers, relevant authorities, third-party service providers)?

    Please elaborate on both **response activities** and **recovery activities** (if applicable).

17. Which external stakeholders (e.g. customers, relevant authorities, third-party service providers) should be considered in response and recovery communication planning?

    Please elaborate on both **response communication planning** and **recovery communication planning** (if applicable).

18. What types of information should be communicated to external stakeholders (e.g. customers, relevant authorities, third-party service providers) with respect to Cyber Incident response and recovery?

    Please elaborate on both **Cyber Incident response** and **Cyber Incident recovery** (if applicable).

19. What are the most effective practices for ensuring accurate, timely and actionable communication to internal stakeholder (e.g. the board) and external stakeholders (e.g. customers, relevant authorities, third-party service providers)?

    Please elaborate on both **Internal stakeholders** (e.g. the board) and **External stakeholders** (e.g. customers, relevant authorities, third-party service providers) (if applicable).

2.3 Improvements

20. What are the *key challenges* and *effective practices* associated with incorporating lessons learnt from Cyber Incidents?

    Please elaborate on both **key challenges** and **effective practices**.

21. What are the most effective practices for improving entity-wide response to, and recovery from, and a Cyber Incident (including criteria or metrics used)?

    Please elaborate on both **Cyber Incident response** and **Cyber Incident recovery** (if applicable).

2.4 Analysis

22. What are the key challenges and effective practices associated with analysing the cause and assessing the impact of a Cyber Incident (including criteria or metrics used)?

    Please elaborate on both **key challenges** and **effective practices**.

2.5 Mitigation

23. What are the key challenges and effective practices for mitigating and containing the effects and expansion of a Cyber Incident (including criteria or metrics used)?

    Please elaborate on both **key challenges** and **effective practices**.

2.6 Interconnectedness

24. How are interconnections between participants in the ecosystem taken into account in Cyber Incident response and recovery activities (including criteria or metrics used)?

    Please elaborate on both **Cyber Incident response** and **Cyber Incident recovery** (if applicable).

25. What are the key challenges and effective practices for responding to Cyber Incidents where services or operations in multiple jurisdictions are affected?

    Please elaborate on both **key challenges** and **effective practices**.

26. What are the key challenges and effective practices for recovering from Cyber Incidents where services or operations in multiple jurisdictions are affected?

    Please elaborate on both **key challenges** and **effective practices**.

3. Other

27. Has your organisation established mechanisms or a strategy for the coordination of Cyber Incident response and recovery activities? If so, please describe your organisation's plan or process for such coordination.

    Please elaborate on both **Cyber Incident response** and **Cyber Incident recovery** (if applicable).

28. Please briefly describe any criteria or metrics used to assess the effectiveness of Cyber Incident response and recovery, including any scenario analysis.

    Please elaborate on both **Cyber Incident response** and **Cyber Incident recovery** (if applicable).

29. Are there any aspects of Cyber Incident response and recovery that make use of third-party service providers (i.e. outsourcing arrangements or purchasing of particular service provisions)? If yes, please explain for what areas or functions such third-party service providers are used.

30. Are there other components relating to Cyber Incident response and recovery that are not covered above that should be included? If yes, please describe.

    Please elaborate on both **Cyber Incident response** and **Cyber Incident recovery** (if applicable).

31. Are there other effective industry practices related to Cyber Incident response and recovery that you would like to highlight? If so please specify.

    Please elaborate on both **Cyber Incident response** and **Cyber Incident recovery** (if applicable).

Annex: Reference standards on cyber security

BSI-Standard 100-4 (2009), Business Continuity Management, Version 1.0.

BCBS (2018), *Cyber-resilience: Range of practices*, December.

Carnegie Mellon University Software Engineering Institute (2018), *Incident Management Capability Assessment*.

CERT-RMM (2016), *CERT Resilience Management Model Version 1.2*, February.

CIS Controls.

COBIT 5 APO 12.06.

CPMI-IOSCO (2016), *Guidance on Cyber Resilience for Financial Market Infrastructures*, June.

CREST Cyber Security Incident Response Guide (2013).

Cyber Security Book of Knowledge (CyBoK) (2019), *Security Operations and Incident Management*, Hervé Debar, January.

ECB (2018), *Cyber Resilience oversight expectations for financial market infrastructures*, December.

ENISA (2010), *Good Practice for Guide for Incident Management*, December.

ENISA (2016), *Strategies for incident response and cyber crisis cooperation*, August.

FFIEC (2016), *Information Security*, September.

FFIEC CAT (2017), May.

G7 (2016), *Fundamental Elements of Cybersecurity for the Financial Sector*, October.

IAIS (2018), *Application Paper on Supervision of Insurer Cybersecurity*, November.

ISA 62443 2 1 (2009), *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program.*

ISACA COBIT 5 (2019).

ISF Standard of Good Practice for Information Security 2018 (TM2 – Security Incident Management) (2018).

ISO/IEC 27001:2013 (2013), *Information Technology – Security Techniques – Information Security Management Systems – Requirements*, October.

ISO/IEC 27002:2013 (2013), *Information Technology – Security Techniques – Code of practice for information security controls*, October.

ISO/IEC 27035-1:2016 (2016), *Information Technology – Security Techniques – Information Security Incident Management – Part 1: Principles of incident management*, November.

ISO/IEC 27035-2:2016 (2016), *Information Technology – Security Techniques – Information Security Incident Management – Part 2: Guidelines to plan and prepare for incident response*, November.

ISO/IEC 38500:2015 (2015), *Information technology – Governance of IT for the organization*, February.

ITIL V3 Service Operation

NIST (2014), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, February.

NIST (2018), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April.

NIST SP 800-53 Revision 4 (2013), *Security and Privacy Controls for Federal Information Systems and Organizations,* April 2013.

NIST SP 800-61 Revision 1 (2012), *Corporate Security Incident Handling Guide*, August.

NIST SP 800-61 Revision 2 (2012), *Computer Security Incident Handling Guide,* August.

NIST SP 800-86 (2006), *Guide to Integrating Forensic Techniques into Incident Response*, August.

NIST SP 800-150 (2016), *Guide to Cyber Threat Information Sharing*, October.

NIST SP 800-184 (2016), *Guide for Cybersecurity Event Recovery*, December.

Payment Card Industry (PCI) Data Security Standard v3.2.1 (2018), June.

PwC (2011), *Cyber Investigation*s.