Table of Contents

Effective Practices for Cyber Incident Response and Recovery
Consultative Document

Executive Summary

Cyber incidents[3] pose a threat to the stability of the global financial system. In recent years, there have been a number of major cyber incidents that have significantly impacted financial institutions and the ecosystems in which they operate.[4] A major cyber incident, if not properly contained, could seriously disrupt financial systems, including critical financial infrastructure, leading to broader financial stability implications.

Efficient and effective response to and recovery from a cyber incident by organisations in the financial ecosystem are essential to limiting any related financial stability risks. Such risks could arise, for example, from interconnected IT systems between multiple financial institutions or between financial institutions and third-party service providers, from loss of confidence in a major financial institution or group of financial institutions, or from impacts on capital arising from losses due to the incident. Organisations that are resilient to cyber incidents will be crucial for a smooth functioning of the financial system and in engendering financial stability.

The Financial Stability Board (FSB) has developed a toolkit of effective practices that aims to assist organisations in their cyber incident response and recovery (CIRR) activities. Organisations' respond function executes the appropriate activities in reaction to a detected cyber event, while the recover function carries out the appropriate activities to restore any capabilities or resume services that were impaired due to a cyber incident.[5] The toolkit draws from survey responses by national authorities, international organisations and external stakeholders;[6] a review of existing standards and case studies of cyber incidents; engagement with external stakeholders at workshops and bilateral meetings; and insights drawn from national authorities based on their supervisory work.

Enhancing cyber incident response and recovery at organisations is an important focus for national authorities. National authorities are in a unique position to gain insights on effective CIRR activities in financial institutions from their supervisory work and their observations across multiple organisations or peer analysis that can help suggest areas that both authorities and organisations can enhance. In addition, authorities have an important role to play in responding to cyber incidents that present potential risks to financial stability. For example, authorities can consider the sector-wide implications of a cyber incident, including any market confidence issues arising through, for example, social media, news media and market reactions. Authorities are also appropriate bodies to, when necessary and appropriate, support

---

[3] 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) Cyber Lexicon, November, page 9.

[4] The twin episodes of the NotPetya and the WannaCry ransomware attack in 2017, for example, showed the potential of cyber incidents to be both widespread and devastating.

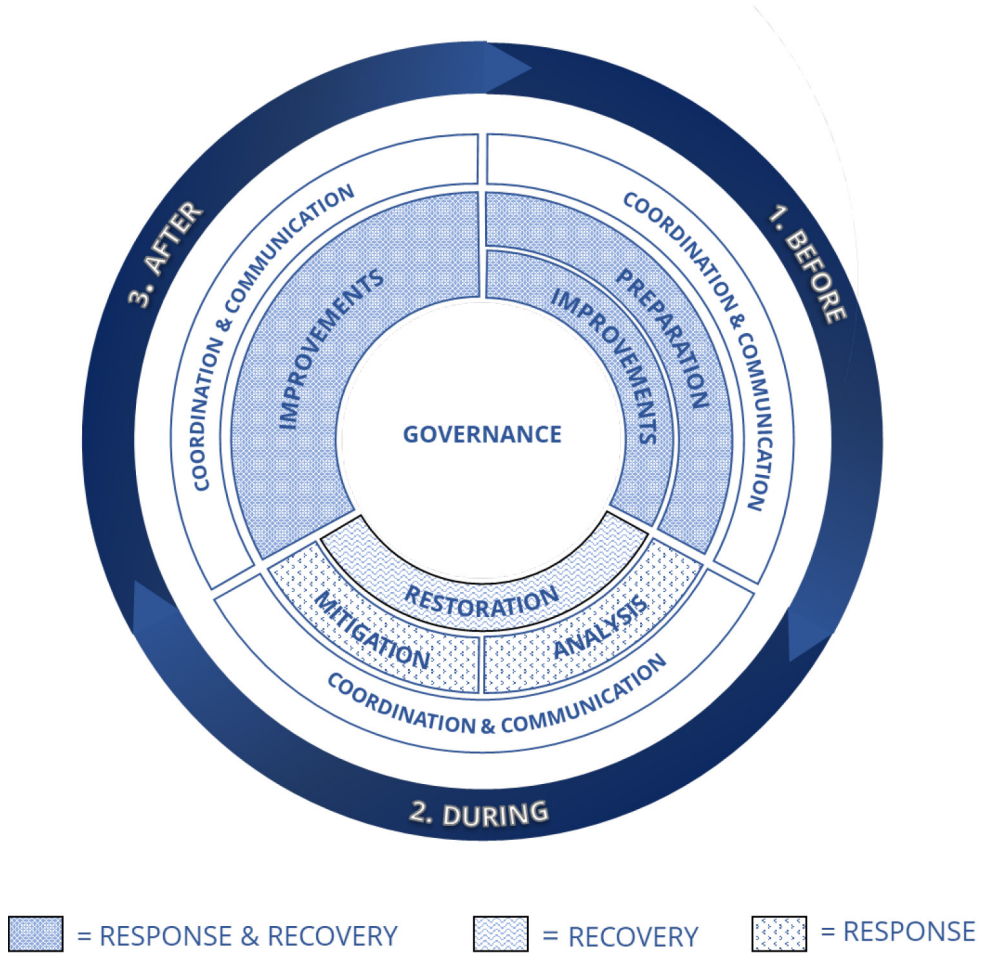
[5] See FSB (2018), Cyber Lexicon, November, page 12 for definitions of the Respond and Recover functions.

[6] For example, see FSB (2019), Cyber Incident Response and Recovery: Survey of Industry Practices, July.

organisations in sharing of information to protect against threats that could have a detrimental impact on financial stability. Thus, authorities may consider this toolkit of effective practices in their interactions with financial sector participants, particularly with those experiencing a cyber incident.

The toolkit, structured across seven components, comprises 46 effective practices that organisations have adopted while taking into account jurisdictions' legislative, judicial and regulatory frameworks, the size of the organisation affected by a cyber incident and the type of organisation that is affected. The toolkit may also be useful for authorities as they consider the approaches they may undertake with respect to regulation or supervision, or in responding to a cyber incident within the sector. The effective practices are meant to serve as a toolkit of options rather than applied in a one-size-fits-all manner, as not all practices are applicable to every organisation or in every cyber incident. The toolkit does not constitute standards for organisations or their supervisors and is not a prescriptive recommendation for any particular approach. An effective practice will evolve over time as the cyber threat landscape changes, particularly as organisations move toward more reliance on third-party service providers (e.g. cloud services), and industry and authorities alike learn from their experiences and additional insights are garnered.

Figure 1: Illustration of CIRR components



1. Governance

Governance frames the way in which CIRR is organised and managed. It aligns CIRR activities with goals set for continuity of business operations, sets the organisational structures and roles required to coordinate response and recovery across internal functions, business lines, firms, jurisdictions or even sectors. Governance involves defining the decision-making framework with clear steps and measures of success, and allocates responsibilities and accountabilities to ensure that the right stakeholders are engaged when a cyber incident occurs. Governance also encapsulates the commitment to supporting CIRR through adequate sponsorship and promoting positive behaviours when dealing with, and following, a cyber incident.

1. **Organisation-wide governance framework.** The CIRR governance structure is part of the broader organisation-wide governance framework. CIRR objectives and priorities are aligned with the organisation's risk management framework and are communicated and understood throughout the organisation. The board is ultimately responsible for overseeing the management of CIRR activities, while senior management oversees the implementation of the policies, procedures and controls that support the CIRR process. Senior management engages with business and technical functions within the organisation to develop, exercise, maintain, manage, support and improve CIRR objectives and plans consistent with organisational needs.

2. **Role and responsibilities of the board.** An organisation's board challenges the planning activity of the organisation, and provides a broader view of the ecosystem in which the organisation operates. The board empowers senior management to take decisions to deploy CIRR activities and works with senior management to enhance the effectiveness of CIRR activities. In particular, the role of the board is to oversee senior management's implementation of the organisation's CIRR objectives, and allocation of certain roles for CIRR activities that are empowered to make decisions and take action. The board with executive authority as well as senior management form the group of decision-makers to steer the organisation out of the crisis. Board and senior management also have the responsibility of implementing the required improvements, including the funding and overseeing the set-up of new solutions within an acceptable timeframe.

3. **Roles, responsibilities and accountabilities for CIRR.** Organisations clearly define the roles, responsibilities and accountabilities for various CIRR activities to one or more named individuals that meet the pre-requisite role requirements.[7] Potential conflicts of interest are minimised by ensuring a separation of implementation and oversight roles where possible. Apart from staff who are responsible for the various CIRR activities, organisations identify key roles (among others) to assist in managing the cyber incident. The roles are part of the multidisciplinary incident coordination team:

    - *Incident Owner*: An individual is responsible for handling the overall CIRR activities according to the incident type and services affected. The Incident Owner is delegated appropriate authority to manage the mitigation of the incident. "Unity of command" is established by ensuring that incident responders report only to the Incident Owner for task assignment. The Incident Owner can minimise the potential

[7] For instance, organisations could use a RACI matrix, which is a tabular format for documenting the allocation of Responsible, Accountable, Consulted and Informed roles.

Box 3: Examples of CIRR taxonomies

- Information to be used when describing cyber incidents
  - Describe the payload (e.g. malware, virus, worm, hyperlink)
  - Describe the delivery channel used (e.g. email, web browser, removable storage media)
  - Describe the impact (e.g. service degradation/disruption, data leakage, data destruction/corruption, tarnishing of reputation)
  - Describe the intent (e.g. malicious, theft, monetary gain, fraud, political, espionage, opportunistic)
  - Describe the threat actor (e.g. script kiddies, amateur, criminal syndicate, hacktivist, nation state)
- Classification of the severity of cyber incidents
  - Severity 1 incident has or will cause a serious disruption or degradation of critical service(s) and there is potentially high impact on public confidence in the organisation.
  - Severity 2 incident has or will cause some degradation of critical services and there is medium impact on public confidence in the organisation.
  - Severity 3 incident little or no impact to critical services and there is no visible impact on public confidence in the organisation.

20. **System and transaction logs.** Organisations identify and collect the types of logs required for timely analysis and forensic investigation, including their location and owners (e.g. database administrator, server administrator). Analysing logs and configurations enables the response team to determine the extent of a cyber incident. The logs are stored and preserved in a secure and legally admissible manner.

21. **Trusted information sources.** Organisations correlate a variety of internal and external information sources for quick threat and root cause analysis of the cyber incident.[8] For example, organisations join or subscribe to cyber threat intelligence sharing sources (e.g. national/international computer emergency response team (CERT) and sector information sharing platforms) to gather intelligence or recommendations on threats and on analysis of tactics, techniques, procedures (TTPs) and risk mitigation. Organisations also collect data from all computing resources for analysing the cyber incident and possible actions. The integrity of these data is continuously monitored. This includes lists of network-connected devices, running processes, users' sessions, open files, relevant configurations (e.g. network, firewalls) and the contents of memory.

[8] Examples of trusted sources are the multi-lateral information platforms.

4. Mitigation

Mitigation activities are performed to prevent the aggravation of the situation and eradicate cyber threats in a timely manner to alleviate their impact on business operations and services.

22. **Containment.** Organisations activate their containment measures, processes and technologies best suited to each type of cyber incident to prevent a cyber incident from inflicting further damage. Having knowledge about what is the specific threat and an understanding of its possible behaviours would also aid in the decision-making.

23. **Business continuity measures.** Organisations invoke business continuity plans during a cyber incident and resume critical operations based on pre-defined prioritisation process in the event restoration is expected to be protracted. Examples of business continuity measures include activating contingency measures not necessarily fully automated to facilitate the processing of critical transactions while system restoration efforts continue, or activating an alternative service provider if the primary service provider will not be able to recover from an incident within a certain period of time, as agreed in the respective SLA.

24. **Isolation.** Organisations consider the costs, business impact and operational risks when deciding whether to shut down or isolate all or substantial parts of their systems and networks, as opposed to maintaining their business services operations. Options for isolation include disconnecting the compromised systems from the network, adding network traffic blocking rules and obstructing threat actors' physical access to affected systems and networks.

25. **Eradication.** After evidence is collected and preserved, organisations remove all materials and artefacts (i.e. malicious code and data) introduced by the attacker. The process may involve patching and closing all system and network vulnerabilities that had been exploited by the attacker. Organisations utilise antivirus and specialised tools and software to remove malware from the affected assets. Organisations also assess whether such standard measures are sufficient to address the particular cyber incident and level of spread, or whether it is necessary to reinstall or rebuild all compromised assets.

5. Restoration

Organisations repair and restore systems or assets affected by a cyber incident to safely resume business-as-usual delivery of impacted services.

26. **Prioritisation.** Organisations prioritise restoration activities based on business, security and technical requirements. All internal and external stakeholders are updated regularly and made aware of the conditions to be met, or restrictions, before resuming critical operations.

27. **Key milestones.** Organisations define in CIRR plans key milestones to redesign, reinstall and reconfigure systems. Where it is not possible to achieve restoration of all systems, organisations consider defining interim restoration goals or interim measures, such as continuing operations in a diminished capacity instead of full capacity.

28. **Monitoring.** Organisations monitor third-party service providers, the network and systems for abnormal activities during the restoration process for compromised IT assets. Cyber incident escalations and resolutions are tracked and monitored, and updates are provided to the management regularly.

29. **Approved restoration procedures.** Organisations carry out systems restoration based on documented and tested procedures. Where required, deviation from approved and tested restoration procedures are risk assessed, tested and management approved before implementation. This reduces risk of human error that may arise in the manual, multistage recovery of systems and data. To restore affected systems, organisations use uncompromised system images and snapshots that are regularly updated, tested and securely stored to prevent malicious corruption or destruction

30. **Validation.** Organisations validate that restored assets are free of compromise, fully functional and meet the security requirements before returning the systems to normal business operations.

31. **Record activities.** Organisations document and timestamp restoration actions taken from the time the incident was detected to its final resolution. Tools and artefacts (e.g. scripts, configuration changes) used for restoration are recorded for future use or for the improvement of current processes and/or systems. This record facilitates the tracing back of actions taken, reversing actions to reinstate to pre-incident conditions or troubleshooting should the recovery actions be unsuccessful.

32. **Data recovery.** Organisations recover and restore data, including data maintained at third-party service providers, to meet business requirements. To provide assurance on data integrity (i.e. not been tampered or corrupted before restoration), organisations perform checks such as validating checksums and reconciliation to ensure data is consistent between systems when recovering from a cyber incident. In worst-case scenario, organisations plan for the reconstruction of data from external stakeholders such as business partners and customers.

33. **"Golden source" data.** Where appropriate, organisations restore backup data kept in another system with a significantly different operating environment to the main system and ensure that both systems are not directly connected. The "golden source" backup data are securely protected from unauthorised access or corruption.

6. Improvement

Organisations establish processes to improve response and recovery capabilities through lessons learnt from past cyber incidents and from proactive tools such as CIRR exercises. Necessary changes are made to CIRR policies, plans and playbooks to improve the overall process as well as any necessary training and testing. Lessons learnt are used in the selection and implementation of additional controls and mitigation measures.

34. **Exercises, tests and drills.** Organisations conduct tests, such as tabletop exercises and live simulations, to validate the capability of resources and the robustness of their CIRR plans and procedures. Organisations design their tests to incorporate interactions within the organisation as well as with external stakeholders and executive level decision-makers

under simulated conditions. The sophistication of these tests increases with the organisation's cyber security maturity. Organisations set clear and appropriate objectives for tests and exercises (e.g. for developing skills, testing the effectiveness of plans, for "muscle memory") to measure the effectiveness of the tests.

Box 4: Examples of scope and types of test

- Tests could take different forms such as:
  - Modular or playbook exercises involving incident responders and incident management teams to build muscle memory.
  - Live simulations including cyber range, adversarial attack or red/blue teaming exercises, and bug bounty to enhance the actual technical response and recovery capabilities.
  - Executive-level crisis management scenarios to stress decision-making under simulated conditions. This could include developing challenging scenarios, such as dealing with "lose-lose" choices, uncertainty and imperfect information, or requiring the prioritisation of the timing of recovery of competing systems and business lines.

35. **Cross-sectoral and cross-border exercises.** Organisations participate in cross-sectoral and cross-border crisis management and contingency exercises to prepare and enhance coordination among multiple stakeholders in the event of a cyber incident with systemic impact on the financial ecosystems. These exercises include different scenarios to validate the effectiveness of coordination on the response and recovery processes. Organisations are committed to share effective practices and lessons learnt with other participants, which include government and organisations. National authorities may participate in these exercises in the spirit of enhancing cyber resilience.

36. **Technological aids.** Organisations invest in the testing of the capabilities of CIRR systems. Computing sandboxes are one tool that enables organisations to test the CIRR systems' effectiveness against the latest malware by allowing potentially malicious files to be executed in an isolated environment.

37. **External events and sources.** Organisations identify opportunities for improvements to their CIRR activities from various sources: cyber publications; reports on the cyber incidents; information sharing and discussions between peers; trend and threat analysis; regulatory and supervisory initiatives; changes to the environment, such as technological developments; and cyber risk management best practices.

38. **Industry-wide initiatives**. Organisations collaborate with peers, such as in established forums, on sharing industry-wide knowledge, discussing cyber events, skill-sets regarding cyber threats, as well as mitigation strategies against existing and potential cyber security vulnerabilities. Organisations also collaborate with authorities to promote information sharing and effective practices for the overall benefit of the industry. Their active engagement in trusted information sharing arrangements contributes to better

mutual understanding of their key interdependencies in the financial system and enhances the organisation's capabilities to respond to and recover from cyber incidents.

39. **Post-incident analysis.** After the closure of a cyber incident, organisations analyse whether established procedures were followed and whether the actions taken were effective. This analysis may include: promptness in responding to security alerts; timeliness in determining the impact of incidents and incident severity; quality and speed in performing forensic analysis; effectiveness of incident escalation within the organisation; and effectiveness of communication (both internal and external).

40. **Lessons learnt.** Lessons learnt are verified with internal and external stakeholders, including business lines affected by the cyber incident, individuals with CIRR responsibilities and senior management. Organisations translate lessons learnt into remedial actions such as controls and procedures to improve future CIRR activities, and track these actions to closure. Closure includes revised metrics and incorporated procedures in playbooks and training.

7. Coordination and communication

Organisations coordinate with their trusted external stakeholders to maintain good cyber situational awareness and enhance the cyber resilience of the ecosystem. During a cyber incident, organisations communicate on an agreed frequency, as well as in a level of detail, and language appropriate to each stakeholder group, in order to improve their engagement in CIRR activities. Progress and outcomes from the cyber incident analysis are shared with internal and external stakeholders so that actions to contain, mitigate, recover or prevent a cyber incident can be taken and to ensure there are no misunderstandings or rumours that could possibly arise from lack of information. A common, secured and trusted communication channel enhances the efficiency and security of information sharing.

41. **Timely escalation.** Organisations escalate cyber incidents to relevant stakeholders within the organisation to avoid delays in addressing the incident. Timely escalation to the organisations' decision-makers based on the agreed framework is essential for the acceleration of CIRR actions, which include seeking approval and authorisation to implement response and recovery plans. Organisations maintain the accuracy and integrity of information during this process, and avoid hierarchical smoothing of risk as it traverses levels of seniority and functional or organisation boundaries.

42. **Regular updates with actionable messages.** Organisations inform relevant stakeholders about potential business disruptions caused by the cyber incident, response and recovery activities taken and the plans to restore operations**.** The information shared is actionable, accurate, timely and concrete.[9] Each message states the actions that are expected to be taken by each audience. The frequency and intervals of such updates are set in advance

[9] *Actionable* refers to information that leads to implementation of concrete controls or configurations. *Accurate* refers to information that has, to the extent possible, been confirmed to be related to the cyber incident. Information is *timely* when it is distributed at a time when the recipient can take actions that minimise the impact of the incident. *Concrete* information goes to the point of the problem, making it easy to read and share among the stakeholders that need to take actions based on that information.

to manage expectations. Whenever possible, organisations communicate on an expected timeframe and conditions under which critical operations are planned to resume.

43. **Cross-border coordination.** Organisations develop and maintain bilateral or multilateral protocols with relevant authorities according to national legislation. Whenever it is legally feasible and relevant for their operations organisations together with the national authorities develop or engage in cross-border coordination and communications.

44. **Trusted information sharing.** Organisations share information on cyber incidents, effective cyber security strategies and risk management practices through malware information sharing platforms (MISP).[10] Technical information, such as Indicators of Compromise (IoCs) or vulnerabilities exploited, are shared as soon as it is available.

Box 5: Examples of information that could be shared

- A brief summary of the cyber incident
- Classification of information e.g. Traffic Light Protocol
- Key contact of the information provider
- Attack pattern
- Vulnerabilities
- Campaign
- Threat actors
- Course of action

45. **Trusted communication channels.** Organisations use trusted and secure communication channels to facilitate communication with relevant internal and external stakeholders, including authorities.

46. **Cyber incident reporting.** Organisations provide without undue delay useful information to the relevant authorities on (significant) cyber incidents, articulating the type or nature of the cyber incident, the impact of the incident and implications on its business continuity, and explaining the rationale of the response and recovery actions taken to restore critical operations in a timeframe.

[10] MISP is an open source software solution for collecting, storing, distributing and sharing cyber security IoCs and threats about cyber security incidents.

Box 6: Type of information that could be included in the cyber incident reporting to provide useful details

- Date and time of discovery of the incident
- Time elapsed from detection to restoration of critical services
- Who discovered the incident (e.g. third-party service provider, customer, employee)
- Type of cyber incident (e.g. DDoS, malware, intrusion/unauthorised access, hardware/firmware failure, system software bugs)
- Impact of the incident (e.g. impact to availability of services, loss of confidential information) and to which group of stakeholders (e.g. retail and corporate customers, settlement institutions, service providers)
- Affected systems and technical details of the incident (e.g. source IP address and post, IOCs, TTPs)
- Action(s) taken at this time
  - Escalation steps taken
  - Stakeholders informed
  - Response and recovery activities commenced