Bank of England PRA

FCA FINANCIAL CONDUCT AUTHORITY

Effective practices: Cyber response and recovery capabilities

Introduction

Cyber-attacks continue to represent a significant threat to the financial sector. This document highlights effective practices that the Bank of England (Bank), Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA) have observed in systemic firms' (Other Systemically Important Institutions) and financial market infrastructures' (FMIs) (referred to as 'firms') operational resilience self-assessments. These practices demonstrate how firms are strengthening their ability to respond to, and recover from, severe cyber disruptions – whether they stem from their own systems or material third-party suppliers.

We are sharing this effective practice for firms to consider and apply appropriately and proportionately. Boards may also use this to support conversations about operational resilience, and challenge and discuss elements such as:

- the level of assurance they have that they can deliver their important business services within impact tolerances;
- whether the firm is testing cyber disruption scenarios that are appropriately severe;
- whether the firm has calibrated its impact tolerance appropriately to mitigate potential impacts to the regulators' objectives;
- to what extent the firm's stakeholder communication strategy is resilient and fit for purpose during severely disruptive events; and
- whether the firm has a clear plan for restoring critical data from back-ups following a cyber-attack, including whether it can rebuild critical applications and core infrastructure, or how it will fail over to a separate environment.

Background

Operational resilience remains a high priority for the Bank, the PRA, and the FCA. Since the publication of joint operational resilience policies in 2021 (hereafter, the policies),[1,2,3,4] firms have been working to identify their important business services, set impact tolerances, and take action to remain within impact tolerances in severe but plausible disruption, or in the case of FMIs, extreme but plausible disruption.

Firms have been working to meet the requirements of this policy against the backdrop of a fast-changing risk landscape. In particular, the cyber threat continues to evolve, and third-party dependencies are increasing. High severity scenarios are becoming increasingly plausible. In this environment, firms are finding it necessary to take a strategic and dynamic approach to maintaining resilience, ensuring their capabilities keep up with evolving risks.

The practices and examples shared here are primarily from large, complex firms. However, the underlying principles will, in many cases, be relevant across the wider population of regulated firms. We encourage all firms to consider the messages in this publication in the context of their own size, business model, and role within the wider financial system, as part of their efforts to strengthen operational resilience. Firms should consider where the practices noted in this paper may help them to strengthen their resilience, which in turn can strengthen the resilience of the sector.

Remaining within impact tolerance for some scenarios, such as severe cyber-attacks on a firm or its third parties, presents a complex challenge. A cyber-attack may disrupt multiple sites and disable or even destroy backup data and systems. Cyber-attacks can undermine confidence sharply, increasing the pace of impacts on customers, counterparties, and the wider market. Market participants and clients may act to protect their operations by disconnecting and isolating operations from the disrupted entity, which could potentially amplify impact on the market. In some instances, firms do not yet have full sight of the cyber resilience of their suppliers, and alternatives may be limited. This is additionally complicated by third parties often having their own suppliers, and assurance can diminish further down the supply chain. We are encouraged to see firms taking steps to enhance their detection, response, and recovery capabilities to remain within impact tolerances throughout these scenarios. In many cases, firms have developed, or are developing, response capabilities to mitigate the impact whilst full recovery is ongoing, including where it may take an extended period.

---

[1] www.bankofengland.co.uk/paper/2021/bank-of-england-policy-on-operational-resilience-of-fmis.
[2] www.bankofengland.co.uk/prudential-regulation/publication/2021/march/operational-resilience-impact-tolerances-for-important-business-services-ss.
[3] www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper.
[4] www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience.

Below, we have outlined examples of effective practices we have observed.

Effective practice: Response to a high severity cyber disruption

In the current threat landscape, firms recognise that severe cyber-attacks are becoming increasingly plausible. We have observed that firms are focusing more on simulating destructive scenarios involving highly capable threat actors and expanding the attack surface to include resources supporting multiple important business services.

The most mature firms have considered impact tolerance metrics beyond duration, including value, volume, critical activity, end-users, and types of payments. By doing so, these firms have provided a more accurate articulation of the level of service they need to deliver to mitigate risk to consumer harm, market integrity, their safety & soundness, and financial stability.

Where firms have identified important business services supporting the orderly functioning of financial markets, many have set impact tolerances that reflect the potential for broader systemic impact. This enabled them to develop alternative solutions, prioritising delivery of key elements of an important business service, or a certain volume or value, in line with the additional metrics defined in their impact tolerance. For example, some firms have identified critical payments they must complete as a priority and have developed the capability to deliver these should they have a significant payments outage occur. To achieve this, firms may use workarounds, restore minimum infrastructure, or transition to a segregated alternative solution with lower capacity.

The most effective firm self-assessments include a pre-defined crisis communication plan that is transparent and timely during and after an attack, covering all customers, counterparties, regulators, and any broader stakeholders. Firms are also testing to ensure the resilience of their communication capabilities during and after an attack. For example, some firms are replicating their critical services, such as authentication and security capabilities, in tertiary or cloud-based environments. While others have alternative communication channels to ensure continuity should on-premises communication infrastructure be compromised.

Effective practice: Recovery from a high severity cyber disruption

Firms have implemented a range of solutions to strengthen their resilience capabilities and have reported an acceleration in their ability to recover from a severe cyber-attack. These solutions include:

1. Restoring critical data from immutable back-ups and rebuilding critical applications and core infrastructure which support important business services. For example, the firms we reviewed are:

a) Investing in immutable back-up capabilities for data and applications. Once the firm's data is backed up and marked as immutable, it cannot be changed, modified, or deleted. Firms subsequently test their ability to restore data to its original usable state and reconstruct it into a complete and accurate data set.

b) Testing their ability to conduct a bare metal recovery in a clean environment. This process ensures that all aspects of the system, including operating system, applications, and data, can be rebuilt from scratch without relying on potentially compromised backups or infrastructure.

c) Recognising that restoring significant volumes of data takes considerable time, some firms are prioritising the most critical data required to deliver their important business services within impact tolerances, making sure this can be restored and recovered quickly.

d) Setting clear priorities for rebuilding core infrastructure, services, and applications, restoring and reconciling data, restoring end-user computing services and onboarding users. They also design their recovery considering the inter-dependencies between these elements.

2. Using a separate, segregated, tertiary facility designed to make it highly unlikely for an external actor to be able to gain unauthorised access to the firms' production environments. Many firms are testing their ability to switchover to either a tertiary site, or to a stand-in service or application.

Effective practice: response to a high severity cyber disruption at a firm's material third party

Where third parties support delivery of important business services, the most mature firms actively ensure the third party's resilience capabilities are equivalent to those they would expect from their own infrastructure.

Where firms cannot currently achieve this level of assurance, they are considering alternative ways to remain within impact tolerances. For example:

- requiring the third-party provider to build its own capability;
- developing the ability to fail over to an alternative third-party provider or to the firm's own systems;
- establishing sustainable manual workarounds for third-party provider capabilities; and
- building the capability to restore the service after data loss or destruction at a third-party provider.

The resilience capabilities firms have, and continue to build, do not sit in a vacuum. Effective resilience capabilities fit within a broader incident response framework that includes clearly defined roles and responsibilities, decision-making set at the

appropriate level within the organisation, and a resilient communications strategy that has tailored, clear messaging to the public, consumers, clients, markets, regulators, and counterparties.

Use of collective action to build resilience

In addition to the work that firms are undertaking individually to strengthen their own resilience, they are also working collectively, by sharing knowledge and expertise, and working on collective solutions.

For example, the Cross Market Operational Resilience Group (CMORG) has produced guidance for firms working to meet the **operational resilience requirements**. CMORG regularly update this guidance as firms learn and share lessons from their own implementation of the policy, and it is made publicly available enabling all firms to benefit. CMORG is currently developing guidance to inform the design and delivery of firm-level cyber recovery capabilities, supporting firms and the wider sector to prepare for and respond to severe cyber scenarios.

Similarly in July 2025, **CMORG** published a reconnection framework to support firms in reducing the time needed to restore access following a disconnection. This included defined pre-requisites and the process of reconnection and full recovery. This will be tested alongside the sector's response structures via two CMORG-led exercises in H2 2025. CMORG also monitors and shares intelligence about the evolving cyber threat landscape, enabling the sector to remain abreast of changes and ensure their resilience posture is appropriately calibrated. Firms have also come together and shared information about their most important third parties and worked to understand the risks and solutions to mitigate such concentration risks.

While the use of CMORG outputs is voluntary, we would encourage firms to stay informed of, and where appropriate, to engage with these work strands as they help to enhance both individual and sector-wide collective operational resilience.

The effective practices shared in this publication complements the findings of the **2024 Cyber Stress Test** (CST24). CST24 focused on systemic impacts and collective response capabilities to a suspected cyber-attack affecting transaction settlement. As well as emphasising the importance of firm level resilience, CST24 reinforced the value of cross-firm collaboration and coordinated exercises in strengthening sector-wide resilience.

Conclusion

While firms have made good progress, there is still more to be done as the threat landscape continues to rapidly evolve. We encourage firms to consider their investments in resilience capability within the context of the end-to-end response and recovery process. Firms must continue to keep their boards apprised of their

operational resilience work through regular updating of their self-assessments. The regulators will continue to request these periodically.

Operational resilience is not a one-off compliance activity. The value of individual technical capabilities is realised not when they are considered as an end in themselves, but when they are designed to meet the needs of, and are understood by, the business. Firms will need to take a dynamic approach, adapting their resilience capabilities in response to the continually evolving risk environment.