How FCA Guidance Aligns With Global Cyberattack Measures

By **Alix Prentice and Grace Ncube** (June 25, 2024)

Alix Prentice

Grace Ncube

By March 31, 2025, U.K. firms regulated by the Financial Conduct Authority will be required to have conducted mapping and testing to ensure they remain within their impact tolerances for identified operational risks of cyberattacks for each important business service.

Ahead of this deadline, the FCA published a web page last month updating its guidance on operational resilience and providing further insights and expectations for firms to meet.

This article examines the guidance from the FCA and other global regulators on how firms can prepare for cyberattacks. It highlights the recurring themes presented by some of the most prominent regulatory authorities as well as areas that continue to be identified as under-provisioned.

Background

The FCA has long been at the forefront of establishing comprehensive guidelines for operational resilience among financial institutions.

Recent initiatives include 2019's consultation paper on operational resilience and impact tolerances for important business services, which called on regulated firms to enhance their ability to withstand, respond to, and recover from disruptions.[1]

The consultation underscored themes that continue to resonate today, including the importance of identifying critical business services, setting impact tolerances, and conducting scenario testing to prepare for potential operational failures.

The goal was then, and is now, to ensure that firms could continue to deliver critical services even under adverse conditions, and thereby maintain the stability and integrity of the financial system.

Following that consultation, the FCA published a policy statement on building operational resilience in March 2021, outlining the rules that will apply to banks, building societies, Prudential Regulation Authority-designated investment firms, insurers and recognized investment exchanges.[2]

FCA Expectations

The FCA's updated web page provides detailed guidance based on firms' preparations for complying with the policy statement. The guidance sets out key priorities for firms to focus on.

- Identifying critical services: Regularly assess and justify the importance of business services;
- Impact tolerance: Establish clear boundaries for acceptable disruption levels;

- Mapping and third parties: Document and manage third-party relationships required for a firm to deliver each of its important business services;
- Scenario testing: Conduct rigorous testing to handle severe disruptions;
- Vulnerabilities and remediation: A firm's mapping and scenario testing must identify and address weak points that may put impact tolerances at risk;
- Response and recovery plans: Develop, test and refine disruption response plans;
- Governance and self-assessment: Ensure comprehensive board-approved assessments; and
- Embedding operational resilience: Embed resilience into corporate culture and risk management;
- Horizon scanning: Continuously monitor and update resilience strategies against emerging risks.[3]

The FCA's requirements highlight the importance of firms being able to anticipate, prevent, recover from and adapt to a wide range of operational disruptions.

This proactive stance is essential for maintaining the stability of the financial system and protecting consumers. Importantly, the guidance also sets out observations that the FCA has made on poor or incomplete practices — a form of a what-not-to-do guide.

For example, the FCA web page notes that some impact tolerances lack sufficient rationale for a firm's board to understand what parameters have been set and why.

Additionally, impact tolerances have been predominantly set as time-bound tolerances, and firms should consider using additional metrics such as customer types, transaction values and transaction criticality, as well as estimated losses, in order to truly anticipate how a significant disruption might play out.

International Perspectives

Globally, financial regulators are increasingly prioritizing operational resilience as essential to the health and continuity of financial systems. Notable international frameworks include those from the International Organization of Securities Commissions, or IOSCO, and the Swiss Financial Market Supervisory Authority, or FINMA.

IOSCO

On June 5, IOSCO published its final report on market outages, which addresses the critical need for improved preparedness and management of market outages.[4]

The report outlines five good practices aimed at enhancing resilience:

- Detailed outage plans: Establishing and publishing detailed outage plans to ensure that all stakeholders are aware of the procedures to follow in the event of a disruption;

- Comprehensive communication plans: Developing comprehensive communication plans to keep market participants informed during outages. This is essential for maintaining transparency and trust;

- Reopening protocols: Implementing protocols for the reopening of trading post-outage;

- Operating closing auctions: Operating closing auctions and establishing alternative closing prices to maintain market integrity; and

- Post-outage reviews: Conducting post-outage reviews to learn from each incident and improve resilience strategies, as well as adopting post-outage plans.

IOSCO's guidelines are designed to offer flexibility for adoption across various trading venues and jurisdictions.

While not rules as such, this report again echoes the FCA's stance that operational resilience, and the ability to withstand increasingly focused and effective attacks and outages, remain a preeminent focus for all in the financial services industry.

FINMA

Switzerland's financial regulator, FINMA, has also been proactive in enforcing stringent operational resilience requirements. In its June updates, FINMA emphasizes the importance of cybersecurity measures, mandatory reporting of significant cyber incidents, and the necessity for firms to conduct regular stress tests to assess their operational resilience.[5]

The guidelines focus on:

- Cyber incident response plans: Firms must develop comprehensive cyber incident response plans, including clear roles and responsibilities for managing cyber incidents;

- Regular cybersecurity assessments: Firms must conduct regular cybersecurity assessments to identify and mitigate vulnerabilities;

- Board-level oversight: Firms must ensure that boards of directors have oversight of cybersecurity risks and resilience measures.

These measures are in line with FINMA's overarching goal of ensuring that financial institutions can withstand, recover from, and adapt to adverse conditions, thereby safeguarding the financial system's integrity.

Recent Cyberattack Examples

The necessity for operational resilience frameworks is underscored by recent cyberattacks on critical infrastructure, including financial institutions and healthcare systems.

These incidents highlight the vulnerabilities that can be exploited, and the potentially significant impact of cyberattacks. What is also clear is that attacks are increasing in volume

and sophistication, and that regulators are concerned that firms are not keeping up with challenges.

Conclusion

Despite extensive regulatory efforts, a common consensus among global regulators — including the FCA, IOSCO and FINMA — is that no firm can be entirely immune to cyberattacks or operational disruptions, hence no regime setting a zero-tolerance baseline.

However, there is clearly a prevailing frustration over an apparent lack of preparedness and insufficient investment in preventive measures by many firms.

Regulators continue to stress the importance of proactive strategies and robust resilience frameworks to mitigate the impact of such disruptions, while also observing a disappointing level of engagement by the industry.

A global theme over the years has been the necessity for firms to plan effectively, identify risks and ensure that senior management is regularly informed about potential threats and resilience measures.

Regulatory bodies have consistently emphasized that resilience is not just about compliance but involves ongoing investment in technology, training and robust governance. From the regulators' perspective, these measures are required to limit disruptions and are yet to be taken on board fully by firms.

Investing in operational resilience is not just about compliance; it is about safeguarding the financial system and protecting consumers. Regulators expect firms to move beyond minimum regulatory requirements and proactively enhance their resilience capabilities.

Recent cyberattacks illustrate the real-world implications of operational disruptions and the critical need for effective resilience strategies.

By adopting a proactive and comprehensive approach to operational resilience, firms can better protect themselves, their customers, and the broader financial system from the increasingly sophisticated and frequent threats posed by cyberattacks and other operational risks.

Alix Prentice is a partner and Grace Ncube is an associate at Cadwalader Wickersham & Taft LLP.

[1] https://www.fca.org.uk/publication/consultation/cp19-32.pdf.

[2] Policy statement 21/3: Building operational resilience: Feedback to CP19/32 (PS21/3).

[3] https://www.fca.org.uk/firms/operational-resilience/insights-observations.

[4] https://www.iosco.org/library/pubdocs/pdf/IOSCOPD767.pdf.

[5] https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20160707-finma-aufsichtsmitteilung-03-2024.pdf?sc_lang=en&hash=A1A633E2246BE27B2020897E1A389049.