Ensuring operational resilience with increasing digitalisation

Morten Bech

Head of Secretariat, CPMI,
Bank for International Settlements (BIS)

Avoiding a cyber mess

"Don't put all your eggs in one basket" is good advice for life, and for operational resilience too. The job of concentrating functions and risk in the financial system needs to be handled with care, and maximum resilience. Decades of work on financial market infrastructures have strengthened business continuity arrangements to ensure continuity of services through fires, floods and power outages, and pandemics. The eggs are safe in the basket.

Cyber risk has made keeping our eggs safe a far more complex and challenging task. Now, replicating data for a seamless failover to a backup site could help spread compromised data across all systems. It might not be obvious that any irregularities are even malicious until it is too late to share information. Outsourcing critical services might help better distribute operational risk, but if everyone uses a common service provider, then an issue can quickly become systemic. Cyber scrambled egg is a risk.

The CPMI's strategy to avoid the omelette is to "protect the core and secure the periphery". The core of the financial system comprises the financial market infrastructures that are covered by the CPMI- IOSCO Guidance on cyber resilience for financial market infrastructures, which led the way for standard setters in this field. Yet cyber defence cannot be boiled down to a pass-or-fail test; improving it requires a cooperative approach. A CPMI-IOSCO roundtable that brought together the 22 largest global and regional FMIs and their supervisors identified three key challenges that need a common solution: (i) data integrity, (ii) information-sharing and (iii) third-party service providers.

International industry-led working groups were set up to tackle each of these challenges. This is the first time this type of cooperative approach has been adopted. Each group has a tough challenge. For data integrity, or how to recover if underlying data are corrupted, there are a number of possible avenues to explore, including contingency arrangements, segregated ledgers and frequent reconciliations. For information-sharing, common protocols exist to share financial events, but operational incidents are still segregated by type of FMI, market and jurisdiction. Setting expectations and developing a practical arrangement for alerting on international operational incidents could enable faster and better-informed responses. Third-party services (eg cloud) can benefit from cooperation by users, provide a clearer view of risk management practices at the common service provider and avoid duplicating third-party risk assessments.

So, although the challenges are tough, financial authorities, infrastructure and their members all have an incentive to cooperate and avoid a cyber crisis. Working together now, to strengthen common operational resilience, can ensure we avoid scrambling our cyber eggs. If we fail to do this, we will all end up with egg on our face. ●

Simon Chard

Partner, Operational Resilience Lead, PwC

Standardised regulatory requirements can improve operational resilience

Everyone is talking about operational resilience. With a fast moving COVID-19 that may become the ultimate stress test, right in the middle of regulatory consultations across Europe, it's the key topic for firms. There is no shortage of policy areas to focus on to make both individual firms and the wider financial system more resilient. We covered a number of them in depth in our report "Operational Resilience: Time to Act" with theCityUK. In this article, I'd like to focus on four areas identified by the European Commission in their consultation: ICT and security risk management and incident reporting requirements, digital operational resilience testing and third party oversight.

The current state of ICT and security management requirements in Europe is inconsistent across sectors. While I don't believe anyone needs to be convinced that improved, consistent standards for risk and resilience across Europe would lead to ▶

an uplift in practices, let's talk benefits. Operational resilience is an outcome, not a process, function or methodology. So benefits must be evident from any initiative taken. For firms, having one standard means a level playing field in Europe, and clarity about what is expected for service chains which cross borders into different regulatory territories. For customers, improved management of risks means more reliable services and improved trust in financial institutions.

It goes without saying that even with the best risk management in the world, failure is inevitable. Industry-recognised standards on the timeliness and nature of reported incidents would enable customers to make decisions based on the relative resilience of firms. Increased consistency and transparency of reporting can also accelerate industry-wide detection of emerging systemic risks and help regulators and firms in their responses.

This understanding of emerging risks should be used to drive digital operational resilience testing. While almost all firms adhere to an operational testing regime, there is again currently no standardised framework. While such a framework may increase costs, if applied with appropriate proportionality, it could not only give firms more confidence in their own ICT and security estate but also that of other firms in their supply chain. For customers, improved and consistent testing will lead to greater confidence in the security and privacy of their assets.

Thinking about supply chains leads us to the final policy area: third party oversight. Third party failure is one of the most common causes of outages, so how well third parties are managed can clearly have a critical impact on the resilience of financial firms and markets. A common framework to manage third parties would not only reduce systemic risk by uplifting standards but also allow firms to leverage this framework to demand more of their suppliers via increased audit rights and participation in scenario stress tests.

Harmonisation of requirements across sectors in Europe can clearly be beneficial not just for customers but for firms and markets. While Brexit may create challenges for European harmonisation, we shouldn't lose sight of the fact that financial services routinely cross borders and therefore greater standardisation with shared global norms will surely be a good thing. ●

Nicola Russell

Director, Global Operational Resilience, HSBC Scotland

Operational resilience as an outcome

Technology to enable digitalisation and innovation has been a priority for financial firms as well as for financial services policy makers for some years now. However, as the financial sector becomes more digital, attention is beginning to turn in earnest to the risks posed by a greater use of technology. A renewed conversation is needed about how firms, and the financial system in general, can become more operationally resilient in the face of rapid technological change to the sector and the economy more generally.

Good risk management provides a strong foundation upon which to build resilience. While regulations for ICT risk and cyber security have existed for years, there has been an uptick in the amount of new regulation in these areas with more on the way. While necessary in the short term, eventually we will reach a point where more risk management offers diminishing returns for improving resilience. We must instead remain focused on achieving resilience as an outcome and not be distracted by a compliance driven exercise more concerned about ticking a box.

A focus on outcomes allows firms the flexibility they need to keep up with a shifting operational environment. The threat landscape for digitally-enabled businesses continues to change and the system is growing more complex, in part to deal with the expectations of consumers enabled by legislation like PSD2. This continuous change will make prescriptive regulation increasingly ineffective; for instance, a mandated risk control measure that was vital one year may be obsolete the next as the technology and threats evolve. In contrast, a focus on outcomes, monitored and enforced through supervision, allows firms to continuously innovate in risk management and resilience while ensuring that regulatory policy objectives are still achieved.

So what does the future of operational resilience look like for both firms and policy makers? All market participants including regulators, firms and policy makers have a shared motivation to ensure the financial system and its participants can continue to withstand, and operate through, disruption. As stakeholders in the financial system we must all recognise this common goal and develop more collaborative ways of working together toward that outcome if sustainable progress is to be made.

For firms, with the threats, system complexity and use of technology increasing, operational resilience must become more holistic. Firms are already shifting their focus to ensuring that they can continue to provide what is important for their customers, the market and their own operations in the event of disruption. That means ensuring the resilience of the systems, people and processes that support these services from top to bottom.

For policy makers, there is a need to step back and consider the macro context. Fragmentation has been an issue in financial regulation for over a decade. International bodies such as the FSB and BCBS have worked to address this and they will need to do the same in the area of operational regulation. Europe has a part to play in that effort. Finally, time is needed – time for current regulation to embed and begin to make a difference, and time for a new approach suited to the future financial services system to evolve. ●