It'll Be Alright on the Night: Operational resilience in Financial Services

Whether as a result of nefarious activity, self-inflicted problems or plain old bad luck, scarcely a week goes by without another major outage or data loss hitting the news. One of the most significant of these this year was the TSB system outage after a system 'upgrade' that left up to 1.9 million customers locked out of their accounts. The problem persisted for several weeks and resulted in secondary impacts such as fraud. It is fair to say that the firm significantly underestimated the risk, impact and duration of the problem. The reputational damage was compounded by the unfolding scenario being played out in public and ultimately cost the Chief Executive, Paul Pester, his job following rebukes from both the Treasury committee and FCA.

It is perhaps not surprising therefore that the Bank of England, PRA and FCA have recently issued a discussion paper on operational resilience in the financial sector entitled "Building the UK financial sector's operational resilience". Although this is at the consultation stage, the paper lays out much of the regulators' current thinking in this area. Probably the most fundamental proposal put forward in the paper is that operational resilience should be addressed by focusing on business services rather than individual systems and processes.[1] As someone who spent most of his career in financial services operations I fully support this approach. There were a number of occasions when even a five minute system outage could result in hours, potentially even days, of operational clean-up so, while the technological impact could be minimal, the operational impact could be significant. In the same vein, the discussion paper takes this a step further and challenges firms to look at the impact on their customers and the wider market.

Practically, however, this is easier said than done. Firms have historically tended to focus on system resilience as a more tractable approach to the problem, i.e. make sure the systems are up and running and de facto the services should be available. Unfortunately, this approach is proving to be increasingly unreliable for a number of reasons. As systems have become decentralised and cloud-based, the inter-dependencies internally and externally become increasingly complex and the probability of an outage or other disruption (e.g. cyber-attack) somewhere in this extended, heterogeneous technology estate increases. Add to this the rapid pace of change, ageing systems and cost pressures and it is a brave person who assumes 100% availability of all systems all the time.

An approach that starts with managing operational resilience through the lens of the end business service to the customer / market is more challenging. Tracing back from a particular business service to the web of processes and systems, both internal and external, that support the service can be complex. Add to this the variety of disruptions that can occur and the permutations increase exponentially. It is key therefore that firms are pragmatic in their approach to operational resilience. The discussion paper lays out a number of the elements that need to be considered and outlines a process that firms can follow to develop their approach.[2] The challenge (quite rightly!) sits with firms to translate the guidance into practical solutions.

[1] "Building the UK financial sector's operational resilience", FCA DP18/04, July 2018, chapter 2 pp.10
[2] Ibid, chapter 4 pp.25

Practicality and complexity tend to run counter to each other, and at the heart of the challenge is how to simplify the planning for operational resilience, while maximising the benefit in terms of meeting business service standards. It is beyond the scope of this note to go into a detailed exposition of all the practical elements that need to be covered, however some of the key points to consider are:

1. Take an 'outward in' approach – start with the service to the customer and work back to the internal and 3rd party dependencies.
2. Understand and set realistic impact tolerances that meet the firm's responsibilities to its customers and the wider market. Similarly, understand the relative priorities between services, customers etc.
3. Identify the types of disruptions that can occur (both internally and externally, self-inflicted or third-party) and how these impact the business service. Remember timing can be a factor – a brief outage just before market close or payment cut-off can have a much more significant impact than one earlier in the business day. Try to group scenarios into related families to simplify the resolution planning.
4. Plan for the likely scenarios (e.g. major system outage, data breach, third-party outage) identifying the relevant roles and responsibilities, systems/processes and governance to handle these scenarios.
5. The actual disruption is unlikely to correspond exactly to pre-planned scenarios so it is important that any framework is prescriptive enough to provide clear guidance but flexible enough to respond to the inevitable uncertainties.
6. Communication is key. Clear communication internally and externally are fundamental to managing both the disruption and its impact on stakeholders.
7. Think about the tail – not just restoring the systems and processes, but resolving any residual issues and capturing the lessons.
8. Testing is central to assuring the practicality of the elements of operational resilience and the overall approach.
9. Design for business resilience. Ideally, operational resilience planning should be built into the introduction of new systems, process and products. Whether it is a new or existing service the operational resilience needs to be an ongoing, iterative process (e.g. of monitoring and applying lessons learned).
10. How is operational resilience informing your investment decisions alongside other strategic priorities?

In closing, I am reminded of a quote from the late Dennis Norden - *"There's an unseen force which lets birds know when you've just washed your car"*. Unfortunate things will always happen – it is how you plan for and respond to them that counts.

GDFM will be chairing a roundtable on Operational Resilience at the 1LoD Summit in London on 15 November 2018 https://www.1lod.com/london-2018. We hope to see you there.