BANK OF ENGLAND

Speech

# Operational resilience – a progress report

Speech given by

Nick Strange, Director, Supervisory Risk Specialists

21st Annual Operational Risk Europe Conference, London

14 May 2019

I'm delighted to have been invited to give the keynote address today, and to be able to set out what we in the regulatory community here in the UK are doing to build a more resilient financial system. The concepts underlying the discussion paper we issued last year are attracting international attention too and have been described as a 'mindset change' by one of our international regulatory colleagues, and that's exactly what they are.

Operational risk and operational resilience are in the spotlight as they never have been before as the richness of content in this year's conference clearly demonstrates.

Two years ago at this conference my colleague, Charlotte Gerken, set out the aims and objectives of the Bank's approach to operational resilience and our strategy for delivery.

We at the Bank of England been very busy since then, as I'll go on to explain, but first we have to acknowledge that our cyber adversaries have been very busy too. In the last two years we have seen a number of serious cyber-attacks. The 2017 WannaCry and NotPetya attacks had a global reach and caused significant impacts for certain sectors, including the NHS, shipping and pharmaceuticals. High-profile data breaches, such as those affecting Ticketmaster and Dixons Carphone in 2018, underscored the growing intent of attackers to capture huge volumes of customer data. Sophisticated attacks against banks in Mexico and India last year showed us once again that the financial sector is not immune.

And disruption resulting from last year's TSB IT upgrade served as an important reminder that our organisations need to be resilient to a far wider range of potential operational issues than the cyber threat alone.

So we in the finance sector cannot be complacent. In another two years' time there will probably be a whole host of new incidents for us to look back on.

Enhancing the operational resilience of the financial sector is therefore a priority for us all: it won't completely stop bad things happening, but it will make us better at weathering their impacts.

It's for this reason that the discussion paper that we released last year starts from the premise that operational disruptions will happen and robust, well-tested response and recovery plans will be key to maintaining your important business services.

But I'm getting ahead of myself, let's first take stock…

First let's remind ourselves what operational resilience is and why it matters to us as a central bank and as a supervisory authority.

In the discussion paper we define operational resilience as “the ability of firms, FMIs and the sector as a whole to prevent, respond to, recover and learn from operational disruptions”.

This definition helps us to clear up some of the confusion we often see between operational risk and operational resilience:

We regard operational resilience as an outcome, something we should strive for, just like financial resilience, and both are key to the Bank’s mission to maintain financial stability. The financial system should be able to absorb both the financial and the operational shocks and continue to provide the key business services we all expect the financial sector to provide to the wider economy, both in benign and in stressful times.

Operational risk, on the other hand, is as the name indicates, a risk, which if not properly controlled, threatens operational resilience; in fact it threatens financial resilience too. Credit risk, traded risk, liquidity risk etc. by contrast tend to impact adversely on financial resilience alone. The role that operational risk managers play in controlling operational risk is therefore key to both minimising financial losses and to maintaining the ongoing provision of business services.

So, to recap, operational resilience is the outcome we are seeking and to do that we must manage operational risk effectively.

Traditional supervisory approaches have been primarily focused on ensuring the financial resilience, the safety and soundness, of the firms we regulate – the logic being that if the firms can stay solvent and have the liquidity they need then they will continue to provide the business services we all depend on. As part of this supervisory approach we have always concerned ourselves with firms’ operational risk management capabilities. For example, we look at operational risk management frameworks and at how firms manage their IT risks, particularly during periods of major IT change. Some of you here might have benefited from our reviews (but you may not always have appreciated that close attention!).

But operational resilience gives us a clearer focus for our supervisory effort. The growth of cyber threats has shown us that firms may well be unable to provide the business services we all depend on for prolonged periods without they themselves being at risk of failing.

So as a supervisory authority it is clear that we need to concern ourselves with both the financial and the operational resilience of the firms we supervise.

Taking a wider perspective as a central bank, we also need to be mindful of our financial stability remit, which gives us a more systemic objective for operational resilience. In a recent paper, my colleagues Anil Kashyap and Anne Wetherilt list the following factors, which in their view may lead to distinct systemic concerns:

a. The central bank is likely to be more interested in system-wide scenarios of disruption; individual firms will often focus on and test firm-specific scenarios;
b. The central bank is likely to be more concerned about common vulnerabilities, for example firms relying on common third parties; and
c. The central bank may wish to test whether collectively firms have adequate resources to deal with a severe operational disruption; individual firms may be undertaking their contingency planning without full knowledge of the availability of common resources;

So that means that in acting as both supervisor and central bank we need to look at the whole range of business services the financial sector provides and understand the most important contributors to these functions and the characteristics of the system as a whole that may amplify the damage done by severe shocks. For example, lack of diversity or substitutability could weaken the resilience of the system, as the ability for one entity to step in on behalf of another may be limited.

And we will want to set clear expectations both for the operational resilience of individual firms and for the system as a whole.

In the Discussion Paper on operational resilience that we published in July last year, we set out our proposed approach towards strengthening our supervision in this area.

And in its March communication, the Bank's Financial Policy Committee, who have a systemic risk focus, provides more detail on its cyber resilience work plan. I will take each in turn.

The discussion paper was a joint publication between the Bank, the PRA and the FCA. This was a first, and demonstrates that the three UK regulatory bodies are aligned and are taking a joined-up approach to policy development, to enhancing our supervisory approaches, and to providing thought leadership on international operational resilience developments. We intend to remain aligned, although the detail of implementation will need to reflect the unique perspective and remit of each supervisory body.

The discussion paper attracted a lot of attention, and was one of the most downloaded papers from the Bank's web-site, ever. Compared to other such papers we've had 5 times the number of responses. The feedback to the paper was overwhelmingly and reassuringly positive and provided useful input to help us develop our thinking.

That level of interest is a clear indication that the financial sector wants to engage with us in a constructive discussion about what operational resilience means for financial services. This is encouraging for us and those who care about resilience of financial services.

It will certainly help us to think of operational resilience as a shared goal. As Sam Woods said in his speech Good Cop/Bad Cop, this is an instance where industry and the regulator face a shared challenge, most clearly visible in the case of cyber. And we have a shared interest in mitigating that risk.

The DP makes it clear that we regard operational resilience as a board and senior management responsibility.

In particular the DP proposes that senior management should:

a. Plan on the basis that disruption will occur: "Assume it will happen". How will you respond and recover when it does?
b. Identify and focus on the resilience of your most important business services;
c. Set your impact tolerances, describing the maximum tolerable disruption to these important business services from a consumer, business and financial stability perspective; and
d. Test your ability to stay within these tolerances through severe but plausible scenarios.

Effective internal and external communication plans are also needed, the latter particularly important now that social media can very quickly highlight any disruption, however minor.

So our proposed approach is built on two key concepts: impact tolerance and business services. Let's look at each of those in turn.

Firstly, impact tolerance: we define this as a firm's tolerance for disruption – in the form of a specific outcome or metric – for example the proportion of payments made; the number of customers affected; the maximum allowed time for restoration of a business service.

- Crucially tolerance is built on the assumption that disruption will occur and that the tolerance remains the same irrespective of the precise nature of the shock. The tolerance is cause-agnostic.
- So, rather than limiting risk mitigation efforts solely towards minimising the probability of a disruptive event occurring, impact tolerance focuses the board and senior management on minimising the impact, the actual disruption that would occur.
- Impact tolerance thus provides a focus for response and recovery, for contingency planning, alongside traditional operational risk management.

Impact tolerance is a very general concept, so to make it more practical, we link it to business services.

- In the DP, we define business services as 'the products and services that a firm provides to its customers'

- And by attaching an impact tolerance – remember this is a specific metric or outcome – to a business service, we provide a clear focus for firms' efforts to enhance their operational resilience: this may include plans to upgrade IT systems; business continuity exercises; communication plans, for example.

Importantly, our focus is on business services not IT systems. So long as you can continue to provide a service we are agnostic as to how you do this. Substitutability can play a significant role here: if you can switch to another system to provide your service then you can take more time to ensure the first system recovers fully.

The consultation paper we will publish later this year will set out our proposed policies and explain our approach to supervising operational resilience. Aligning our supervisory approach towards continuity of services necessitates a review of that approach. However, where possible we will build on existing policies and rules, placing them within a clear and consistent framework. Key elements of the existing supervisory approach, such as reviewing the effectiveness of firms' governance and risk management functions, will continue to be important components in assessing firms' operational resilience capability. Similarly, firms' existing business continuity, incident management, change management and third party management functions are within scope of the existing rulebook and should continue to support firms' operational resilience.

Turning now to the Financial Policy Committee's work programme in this area. The FPC's role is to identify, monitor and take action to remove or reduce systemic risks to protect and enhance the resilience of the UK financial system as a whole. Cyber risk is one of the key risks they are focused on. The FPC's work here has a wider read across to operational resilience and the core components are similar: impact tolerance and vital services (which we can think of as groups of business services).

The FPC has indicated that it will establish a tolerance for the amount of disruption to the delivery of vital services, setting this tolerance at the point after which it judges that disruption would begin to cause material economic impact.

And where we will expect firms to test their own impact tolerances, the FPC will ask firms to test its tolerances too in severe but plausible scenarios. We refer to this as cyber stress testing.

By testing firms' ability to contain any disruption to business services in severe but plausible scenarios to a pre-defined tolerance level, we inject a suitable degree of proportionality. There are two important messages here: firstly we do not expect firms to able to withstand the most extreme forms of disruption – that would be inefficient and make the cost of providing critical business services prohibitive. And secondly we recognise that disruption will happen and it is unrealistic to expect that in today's complex and connected world that we should have a zero tolerance for disruption.

We are going further than simply defining tolerances though; we need to satisfy ourselves that firms can actually meet the tolerances that they or we define. Stress testing is one tool we can use here. For a number of years now we have stress tested the larger UK banks to ensure that under prescribed scenarios they have sufficient capital to continue to lend to the real economy. We will build on our experience with financial (concurrent) stress testing, to pilot cyber stress testing. This a new undertaking, and so we are keen to work with industry and get your input as well.

- Specifically, later this year, we will test an impact tolerance for payments in a hypothetical scenario where firms' IT systems supporting their payments function become unavailable;
- We will be working with a small number of firms to 'test the test' and also gather some initial information on whether an end-of-value date tolerance for this vital service would be appropriate from a financial stability point of view; and
- The FPC also indicated that in future it may consider a data integrity scenario.

So these are two key planks of the Bank's operational resilience current work programme:

a. Developing the supervisory approach to operational resilience in line with the discussion paper; and as part of that
b. Developing a cyber stress testing programme.

But cyber risk knows no boundaries, so we are not pursuing this work programme in isolation here in the UK. We are working closely with our international colleagues. I'll give two examples.

In recent years, the G7 has been the leading international forum, progressing the international cyber agenda. In particular, the G-7 Cyber Expert Group, which represents 23 financial authorities, has issued four 'Fundamental Elements' publications to build common and consistent understanding both within and outside the G-7.

These documents encapsulate cybersecurity related effective practices for public and private sector entities of all sizes, on important topics such as effective assessment, third party cyber risk management and threat-led penetration testing.

This last document on penetration testing may be of particular interest.

- Since the Bank of England pioneered CBEST, threat-led penetration testing has been adopted in a number of jurisdictions, and I should add, other economic sectors as well;
- But, as more jurisdictions and more sectors develop threat-led penetration testing, concerns have started to arise over potential risk of duplication, and also slightly different approaches;

- The G7 elements are helpful in this regard: whilst not setting a common standard, they provide useful common guidance and can as such take us towards greater compatibility.

The next step for the Cyber Expert Group is to establish a collective view of vulnerabilities which it can then use to prioritise its future work stack.

But the Cyber Expert Group isn't just a think tank – it also provides a forum for G-7 authorities to develop their collective operational capabilities. In just a couple of weeks' time they will be facilitating a cross-border simulation exercise to explore how authorities would communicate and coordinate in the face of a significant cyber incident.

The group will also examine the consequences of a multi-day disruption resulting at a large international bank which may be financially viable, but operationally disabled.

Secondly, and more recently, the Basel Committee established the Operational Resilience Working Group (ORG) with the intention of contributing more broadly to the international effort on both cyber and operational resilience.

In December, the group published its "Cyber Resilience: Range of Practices" report, identifying, describing and comparing the range of observed cyber resilience practices across jurisdictions. This is a really good read, with case studies, and I can recommend it.

The report should help banks and supervisors navigate the regulatory environment. It will also serve as useful input for identifying areas where further policy work may be warranted.

Going forward, the Basel Committee will integrate the cyber dimension into its broader operational resilience work.

I would like to go back to my earlier point about facing a shared challenge in achieving the goal of operational resilience. There are two aspects of this that I'd like to cover, firstly the relationship between you and your firms and ourselves as regulators, and secondly what you and your firms can accomplish by cooperating more closely with each other. And the key question here is: to what extent can firms work together, pool resources, share information – in short, develop non-competitive solutions to a shared threat.

We are keen to seek views from industry as we progress our work on operational resilience. During the consultation process for our discussion paper we engaged extensively with many different stakeholders to take their views. We will listen carefully to responses to the consultation paper when it comes out. It's also good to have opportunities like this event today to get our message out to a potentially wider audience.

We also engage with the financial sector in other ways. Again I'll give just two examples:

Firstly, together with UK Finance, we co-chair the Cross Market Operational Resilience Group (CMORG). CMORG's job is to promote work that strengthens the resilience of the financial sector and its ability to respond to operational incidents. It does this in part by ensuring there is open and rapid sharing of information as an event develops and then, after the fact, disseminating the learnings more widely.

CMORG oversees our long-established sector exercising programme, the highlight being the bi-annual market-wide simulation exercise. In 2016 we tested the impact – and countermeasures – to a prolonged central payments system outage. And in November last year, SIMEX 18 tested the potential impact of major disruption to financial services stemming from a cyber incident.

Our sector-wide exercising programme helps to ensure that the finance industry and its regulators are prepared and can respond effectively to a potential major disruption or event, thereby protecting the UK's financial system, its participants and customers.

It is a joint undertaking, in partnership with other UK financial authorities and the UK financial sector. It is an opportunity to rehearse existing communications mechanisms and identify improvements to our collective response arrangements, which will, in turn improve the resilience of the sector as a whole and it highlights possible areas for new work. Following SIMEX18, we are now in the process of developing several follow-up workstreams in partnership with industry.

The second initiative I would like to highlight relates to industry coordination in the event of a serious cyber event. Following a successful fact finding mission (nicknamed project Strider), the finance industry has come together to initiate the Financial Sector Cyber Collaboration Centre. FS3C is an industry-owned initiative established to support UK finance sector collaboration on cyber risk. Its principal aims are:

- to draw together existing, but fragmented cyber capabilities;
- to ensure information is shared across sector through an effective trust framework; and
- to work collectively to support outcomes that benefit the sector as a whole.

But is there more that industry could and should be doing to collectively build the cyber and operational resilience of the UK finance sector? A possible (and I only say possible) outcome of the cyber stress testing we are piloting may be that on their own, firms cannot meet the FPC's proposed tolerance for payments systems outage. If this were the case then it would either fall to the public or private sector to come up with a collective solution.

In the US, a private sector initiative has been set up called Sheltered Harbor to protect customers, financial institutions, and public confidence in the financial system if a catastrophic event like a cyberattack causes

critical systems—including backups—to fail. Under this scheme firms provide customer account data in a consistent form to a centrally maintained data vault. Firms designate a restoration partner (another participating firm) so that if the Sheltered Harbor Resiliency Plan is activated, that partner can restore critical customer data. Although yet to be tested in a real cyber event, this shows that by working together innovative and ambitious solutions can be initiated within the sector itself. Is there a lesson here for all of us?

The positive response to our discussion paper is evidence that we are all on the same side and should be working together to create a more resilient financial sector. Enhancing the operational resilience of the financial sector is a priority for us all. We in the Bank will do our bit, but I would also encourage all of you to consider how you can continue to make your firms and, by working together the sector as a whole, more operationally resilient.

As operational risk managers you will no doubt continue to try to reduce the probability of a disruptive event occurring, but it's unrealistic to think disruption can be prevented entirely. A zero tolerance for disruption, however desirable, isn't practical, so you should consider how much disruption your firms are prepared to tolerate from a consumer, business and financial stability perspective. Then you can work to ensure that you have robust response capabilities and can recover your most important business services within the tolerances you set. Focusing on recovering business services, not just IT systems, may help you to deliver more innovative solutions.

Thinking of operational resilience as the outcome we are seeking, and operational risk management as the means by which this is achieved gives a clear focus for investment in both. This renewed interest in operational risk and resilience, suggests to me that there's never been a better time to be an operational risk practitioner.

I wish you an enjoyable and productive conference and look forward to working with you as we make the UK's financial sector more operationally resilient.