BANK OF ENGLAND

Speech

The Bank of England's approach to operational resilience

Speech given by
Charlotte Gerken
Director, Supervisory Risk Specialists

Operational Risk Europe 2017 Conference, London
13 June 2017

Thank you to Op Risk Europe for inviting me to speak at this year's conference.

There is a growing literature on operational resilience and the short working definition I'll use is the ability to adapt operations to continue functioning, when – not if – circumstances change.

Operational resilience is an outcome or result of other practices, processes and culture working effectively: for example of looking at functions end-to-end, having a healthy understanding of the organisation's strengths and weaknesses and practising rigorous operational risk management. The operational resilience of the financial system is an outcome critical in the pursuit of the Bank of England's financial stability objective.

The Bank's approach to operational resilience is still developing. We are working collaboratively on its development with financial services firms, other private and public stakeholders and with other regulatory authorities. We need to play our part to improve the resilience of the system, both in our function as a central bank whose operations provide critical functions for the economy and in our function as supervisor of PRA-regulated firms and of the financial market infrastructures.

The Bank's approach to operational resilience

In this session, I will discuss how we think about operational resilience – our aim and purpose. Then share with you some of the work we have underway to prioritise our resources on the main risks to operational resilience, how we are seeking to build the resilience of the sector in the face of those risks and our work with international partners.

Our approach to operational resilience incorporates cyber resilience and I will give some information about activities in relation to this particular threat. And lastly touch on our plans.

Our aim

How do we think about operational resilience and our role within it?

With regards to financial resilience, the Governor has spoken in the past about the need for the finance sector to be able to absorb shocks, not to contribute to them. This has guided our approach to building financial resilience. And we approach operational resilience with much the same purpose.

Our aim is to improve the ability of the financial services sector to absorb the impact of an unexpected event while continuing to perform its most important activities for the UK economy.

As in our supervision of financial resilience, this means our approach to operational resilience first looks at individual firms as providers of financial services. We need to assess how well firms' business activities and supporting services are designed to adapt to failures in any part of their infrastructure. And to test their resilience in a variety of scenarios.

As with lessons learned from the crisis on financial resilience, it is not sufficient to assume that because each firm is supervised and assessed in terms of its own safety and soundness, we have done our job to ensure financial stability. Our approach to operational resilience also aims to take into account firms' interconnectedness and looks at their links and dependencies. And at both the domestic and international environment in which firms operate – does this act to support or threaten resilience?

How do we think about operational resilience?

At an operational risk conference, I would be unwise to discourage any or all participants from their work to identify, measure or assess, manage and prevent operational risks crystallising. However, to an extent our operational resilience approach assumes risks do crystallise.

Operational Resilience means, not only planning around specific, identified risks. We want firms to plan on the assumption that any part of their infrastructure could be impacted, whatever the reason. Business continuity and disaster recovery planning are necessary but not sufficient disciplines to achieve operational resilience as an outcome. We – the Bank itself – and firms need to consider whether we have designed our organisation, people, processes and technology to adapt and ensure critical services can continue to be delivered through disruption.

As it is impossible to rely on set piece planning for every eventuality, a significant part of the design is leadership – if everyone working on a critical function understands what they are trying to achieve, and what level of disruption is tolerable, that mindset can enable and empower flexibilty in planning and response.

For example in our CBEST cyber assessment, those firms that did best in the testing tended to be those that really understood their organisations. They understood their own needs, strengths and weaknesses and reflected this in the way they built resilience.

For example, one firm that performed particularly well demonstrated that they led their cyber resilience strategy from the board level. The firm had taken the time to understand how it would be affected by an incident involving its most critical functions. The firm had a strong awareness of the business – from a people, process and technological perspective. It had established the necessary mechanisms to bring the business together to respond where and when risks materialised, no matter why or how.

Operational resilience objectives

So what do we want to achieve?

Our objectives are to assess and build the operational resilience of the sector through:

a. Proactive micro-supervisory interventions with firms. Setting expectations and assessing against them.
b. Macro interventions. Looking at the system level and intervening where vulnerabilities exist.
c. Working together with the financial services sector. Working with firms to develop and share good practice and running sector wide exercises. And through international engagement learning from and sharing good practice with other supervisory organisations.
d. Using these three elements to form a sound base on which to build and contribute to the sector's response capabilities. Making sure the right mechanisms – both public and private sector - are ready to respond when failures happen, working in concert with other authorities.

I will speak about each of these areas in the context of our wider strategy to improve the Bank's ability to assess and build the resilience of the finance sector.

Operational resilience strategy

Our strategy is in three parts:

The first part is in identifying and focussing on the most critical functions and supporting activities the financial system depends upon, so we can prioritise effectively. This includes identifying vulnerabilities and keeping up-to-date with threats.

To ensure we identify where we need to focus our work, we are:

a. Strengthening our understanding of the potential impact of disruption to different firms and parts of the system. This answers the question: 'what is critical?'
b. Mapping the structure of the critical economic functions, such as payments and settlements, that the finance sector provides and the firms that contribute to them. This means we can identify key areas of vulnerability. These may be a result of concentration risks, dependencies or single points of failure.
c. And we are building a picture of the most pressing threats to firms and the system as a whole. As our capability grows, we will be better able to target our proactive interventions. We will have a good view of the threat, the vulnerabilities and the parts of the system which could have most impact on financial stability if they are disrupted.

The second element of our strategy is to build resilience. To an extent some of the assessment work associated with building resilience is needed to work out what is most critical. Building resilience includes:

a. Developing our operational resilience supervisory framework. We are working on how to express our expectations of the firms we supervise. And working on our own operational resilience as a provider of critical services.
b. Coordinating activity between firms and leading exercises such as SIMEX, which we ran in late 2016. This simulated and tested the industry's response to an extended outage of the Bank's High Value Payment System - RTGS. It tested lines of communication and how we would make key decisions for contingency and recovery.
c. We use existing tools such as our CBEST threat-led assurance testing and the Dear Chairman Exercises which assessed the resilience of a number of major banks' IT systems.
d. We are also developing and piloting new assessment tools.

For firms, this will provide greater clarity over what we expect and will identify any practices needing improvement across their infrastructure.

We also recognise that the interconnected nature of the finance sector means that international engagement is essential. It is, as often the case, that the global system is only as strong as its weakest link. So we work with other bodies such as:

a. The G7 Cyber Expert Group;
b. The G20 and the Financial Stability Board; and
c. The European Systemic Risk Board's (ESRB);

To learn from partners and develop the resilience of the international financial system.

The next element of our strategy surrounds response. Which is served partly through exercises run with our key partners. An example of this is a joint exercise we did with the USA in November 2015: Resilient Shield. This looked at how we can improve cyber security cooperation. And how we share information about threats between our governments and with the private sector. The exercise enabled mutual understanding and helped us build the right joint response functions.

We also work alongside the FCA and HMT to maintain and run the sector-wide response capability. We keep this capability under review in order to ensure it remains effective and draws on the right expertise across Government. This enables us to mitigate the impact of incidents through:

a. Coordination of communications.
b. Industry action. And, where necessary,
c. Regulatory intervention.

Systemic risk survey

Now let me turn to cyber risk within the operational resilience agenda. In principle our operational resilience programme is designed to be agnostic to the source of threat, whether self-inflicted, from another's technical fault or from cyber attack.

However, the cyber threat is particularly and peculiarly challenging and clearly of increasing concern to all of us. The chart from the Bank's H2 2016 systemic risk survey shows 28% of firms citing cyber attacks amongst the most challenging risks they have to manage. Cyber also has a number of features that make it different from other threats to operational resilience.

a. It is an activity undertaken by individuals, groups and sometimes states. It is not a natural or error based risk. There is a human protagonist.
b. The threat is adaptive. Attackers adapt, adjust and scale their activities to discover what works.
c. Detection and identifying the attacker is complex. It is often hard to detect that an operation is under attack and it can be difficult to trace the source.
d. Recovery may be threatened. Our standard approach to business continuity involves operating with common systems environments between primary and secondary sites, mirroring data between the two. This could, in the face of a successful cyber attack, be vulnerable to complete loss of applications or destruction or corruption of data.

Cyber attacks exploit gaps in the resilience of an organisation. These can be related to gaps in process, or technology or people's skills and awareness. The cyber threat throws operational resilience into greater focus and again requires organisations to understand themselves, their strengths and weaknesses.

Cyber and operational resilience

So, what cyber outcomes does our operational resilience programme aim to deliver?

Our operational resilience strategy aims to identify, evaluate and drive mitigation of cyber risks. We are working to assess more effectively cyber capability of the UK financial sector and through this knowledge strengthen capability.

We have used a cyber triage questionnaire as part of our supervision of firms and are extending its use to more firms. This gives us a baseline view on the maturity of different parts of the sector.

We also continue CBEST assurance testing of the most systemically important firms. Through this work we have already identified some important themes.

a. For example, those that performed best not only had strong defences but had strong detection, response and recovery capabilities.
b. They also understood the need to approach resilience as a people, process and technology issue. Not only focusing on technical controls.

We continue to share and compare practice in cyber penetration testing and broader cyber assessment through international fora and with other critical sectors, for example telecoms, in the UK.

Assessing the sector's resilience

This year we are continuing to support smaller scale industry exercises. Next year, we will run another sector-wide exercise, similar in scope and scale to last year's SIMEX16 sector-wide exercise.

Another previous example of one of these large scale exercises was Waking Shark, run at the end of 2013. This involved about 220 people from fourteen PRA and FCA regulated firms, six Financial Market Infrastructures, the financial authorities and government agencies. The exercise focused on disruption and dislocation in wholesale markets. Recommendations related to coordination, communication and information sharing, including aiding the authorities in criminal investigation of attacks; and have been acted upon since.

We continue to develop our collaborative work with industry, the other financial authorities and wider Government. This includes developing guidance on dealing with specific types of cyber attack, like DDOS or various forms of malware.

Our plan

I said up-front that our approach to operational resilience is still developing.

Over the coming months we will articulate the Bank's tolerance for disruption in the sector. This will help inform our firm-specific and sector-wide interventions – targeting them on the parts of the sector which could have greatest impact on financial stability if they were to be disrupted.

We are also developing our micro prudential, firm level supervision approach. This will set clear expectations of firms and provide tools to assess firms' resilience.

We continue our system-wide work through the Financial Policy Committee. Next month's Financial Stability Report will announce the next steps for the FPC cyber work programme.

We also continue to work through international fora. We have key pieces of work which we will help deliver in the coming months through the Financial Stability Board and G7.

In conclusion, the need for operational resilience is not new – firms have long needed the capacity to absorb shocks in order to stay in business. However, the evolving cyber threat has focused and brought together the finance sector's thinking around operational resilience. And the interconnectedness of the system has amplified the need for system-wide attention on shock absorption.

We will continue to develop our approach through collaborative working, with financial services firms, other authorities and public and private sector. Together we will improve the ability of the financial services sector to absorb the impact of unexpected events and to continue to serve its critical role for the UK economy. I look forward to working with you.