BANK OF ENGLAND

Speech

‘Operational resilience in financial services: time to act' report launch

Speech given by

Lyndon Nelson, Deputy CEO & Executive Director, Regulatory Operations and Supervisory Risk Specialists

The City UK 'Operational resilience in financial services: time to act' report launch, London

5 June 2019

I'd like to first congratulate the CityUK for organising this event and second to thank them for the invitation to speak today on the important topic of operational resilience and cyber. Initiatives such as the CityUK report are set to be important milestones in a drive towards improving the operational resilience of the UK Financial Services Sector.

To put some context around that statement, I've been thinking a lot lately about 1974. If you look at the headlines of that year they have a familiar ring to them: political turmoil, terrorism, extreme weather and economic uncertainty.

The notable finance event was the disorderly shutdown of German bank, Bankhaus Herstatt, which closed its doors at 15:30 on 26 June 1974 - so we are not too far away from the 45th anniversary. The disorderly failure of Herstatt and in particular that it failed inside the business day, shocked the financial world and sparked a host of reforms - particularly the creation of key principles of payments and settlement. Peter Allsopp of the Bank played a very significant leadership role in the response. Thanks to him and many others we have now largely removed so called Herstatt risk from the financial system. In contrast we have only just begun to reduce the risks arising from an operational failure.

We have seen that operational failures can happen and unless something dramatically changes we can expect them to happen again. Cyber adds a further sense of urgency as incidents are human led, intelligent and deliberately exploitative. Hence the fact that regulators and firms have been pushing operational resilience up the agenda.

Last year the UK authorities issued a Discussion Paper, setting out an ambitious and innovative outcome based approach to enhancing operational resilience of the UK finance sector. The Discussion Paper has received very positive feedback from industry and globally, particularly its outcome based approach and the concept of impact tolerance but it also raised issues that require clarification, most notably the family tree of operational risk, operational resilience, operational continuity in resolution and a number of other terms. We will respond to this and other questions in the Autumn.

Before leaving the Discussion Paper, I want to step back and look at just two of the mindset changes I believe it heralded. At a policy level it set out that firms should assume that operational disruption would occur and plan accordingly. The second change is one of strong collaboration. The Discussion Paper is a joint document from four different authorities - the Financial Policy Committee, the Financial Conduct Authority and the Bank of England's Financial Market Infrastructure supervisors and the PRA. It is the first of its kind. Clearly this does not come without cost and time, but it reflects how highly prized we consider collaboration to be in this area. We are acutely aware of the explosion of different standards across the globe and we are keen not to add to that problem. But the collaboration does not stop there. Just as the response to Herstatt required private and public sector cooperation, so we feel that Operational Resilience must follow suit. Historically the Cross-Market Operational Resilience Group was chaired exclusively by the Bank, but we have now re-shaped that group and have introduced a co-chair structure - I now co-chair with UK Finance. The most visible of CMORG's activities is to support a regular cross-sector operational exercising programme which helps industry and authorities alike understand our operational capabilities when things go wrong and build capabilities to address these before they do.

But there are others too. In addressing the threat from Cyber, we welcome the announcement by UK Finance of the formation of the Financial Sector Cyber Collaboration Centre, which promises to bring a step change to industry collaboration and therefore defensive capabilities on cyber. This is a great example of where firms can address risks which are unmanageable by firms individually by tackling the problem for the broader public good.

There is still room for industry to go further. The last sector exercise identified a number of areas which lend themselves to this approach and we will release a report shortly about these. But the key points are:

- Developing ideas on how to protect systems and data more robustly against both accidental and deliberate damage;
- balancing system availability with protecting data integrity during periods of operational stress;
- how to secure data against permanent loss, so that we can absolutely guarantee data integrity and availability; and
- how to resume key services safely when disruptions have occurred, without losing data, damaging integrity or causing contagion into the wider financial system.

These are all complex issues, which neither regulator nor firms can fix in isolation, but they do define the key operational disruptions scenarios for which I believe together we need better solutions than we have today.

I want to return again briefly to Herstatt or more precisely the response to it. In my view the collective effort to respond to the risks highlighted in this case transformed payment risk for more than a generation. It made settlement finality and contract certainty concepts that were not just expected but delivered. Operational Resilience and Cyber present a similar challenge and the key question is whether we collectively are up to that challenge. If we rise to the challenge we will have a more resilient financial system which meets the needs and expectations of the real economy. We will be protecting our services not just against unexpected operational disruption but also those seeking to damage or compromise our systems for malicious intent. This will be its own deterrence effect against those bad actors, but it will also be a positive feature of doing business in the UK.

In recent years, as there have been more challenges to trade and globalisation, we have all had cause to reflect on where business is conducted. The UK, and within that the City of London, has had many advantages (English Law, time zone, the depth of the talent pool, the availability of professional services and support) and has consequently been the location of choice for many. I believe operational resilience will increasingly be a key factor in determining where business is conducted. In the next ten to twenty years, we have the opportunity to add to the many advantages of the UK by making it one of the most operationally resilient locations anywhere in the world. Imagine being able to justifiably claim that even with operational disruption payments can be made and business can still be conducted after only a short delay. As a central bank and a regulator we are ready to take up the challenge. It is clear from reports such as this one from City UK, the sector looks ready to do so as well.