BANK OF ENGLAND

Speech

Resilience and continuity in an interconnected and changing world

Speech given by

Lyndon Nelson, Deputy CEO, Executive Director

20th Annual OperationalRisk Europe

13 June 2018

In just a few weeks, I will have completed 30 years in the City of London. Such milestones are obviously a cause for reflection and today I want to share some of those reflections with you in the area of technology. I had visited London less than half a dozen times before I started. My family were based in York and we banked with the local regional bank. Indeed, I had been a depositor with my bank since the age of five. On my arrival in London I found myself with only one ATM machine available to me at the branch of my regional bank on Cheapside. There was a small plaque on the ATM that read "in case of malfunction the nearest ATM is on the High Street in Reading" – a journey of 44 miles. Given my lack of access to an ATM, I was quick to apply for a bank account at the Bank of England, whereupon I now had access to 2 further ATMs, both next to each other in the Drawing Office in the main building in Threadneedle Street. Fortunately just a few years later my bank joined the Link network of ATMs and my days of hoarding cash came to an end. Link now has 38 member institutions and connects over 70,000 ATMs in the UK and represented a key development in building and maintaining shared services across the sector.

Of course, the major change in banking has been the rapid development of both Internet and mobile telecommunications and the consequent demise of the branch - "clicks not bricks". Dial-up Internet was first available in the UK in 1992 and the first consumer mobile phone in the UK was launched by Motorola in the same year. It had no screen and limited functions. The first phone capable of browsing the Internet was the Nokia 7110 that was launched in 1999. In 1990, I was one of 17% of UK homes who owned a personal computer. By 2016, 88% of homes owned a personal computer with the bulk of the growth occurring between 2000 and 2010 (when it grew from 38% to 77%). But we're getting ahead of ourselves, because, of course, there was a time when phones were used to make calls. In 1989, I was on the team responsible for the supervision of the large clearing banks. Midland Bank, which to put it mildly had had a difficult few years, launched First Direct, a division of the bank which offered a telephone banking service. At the time, Midland Bank would advertise itself as the "listening bank" and wanted to describe First Direct as the "talking bank". However as the term 'bank' was legally protected at the time it was only legally able to describe itself as the "talking division of Midland Bank". That really did not catch on.

10 years later the first online banking platform was launched by Nationwide Building Society in 1997, but it was not until the 2000s that such services gained meaningful status as consumer utilities. Behind the scenes, the first faster payments were sent in 2008 and in 2012 the Payment Services Regulations introduced the new requirement for payments to reach the beneficiary account no later than the day after the remittance account is debited - not the three or even seven days I was used to back in 1988. Also in 2010 mobile banking on smartphones and tablets was introduced. In 2014, PAYM (payment via mobile phone) was launched. So today, I think nothing of paying my groceries with my mobile phone, arranging for a BACS payment to go to the firm that has just mended my roof and to secure these transactions either with my voice pattern or my fingerprint.

It truly is an amazing time to be involved in financial services.

All new technology opens up new opportunities. Be it for the customer or for the bank itself. For the bank, it provides an opportunity to consider their business model and unbundle previously aggregated activities. This in turn, has enabled the second key development in my 30 years. The rapid growth of outsourcing and the use of third parties. Outsourcing was sometimes motivated by cost and efficiency (many banks had cost to income ratios of around 70% when I started) and in other cases to achieve improvements in the management of risk. These days many of these third parties are entities that are outside of the financial system. Like all outsourcing they create new dependencies on which the financial system must rely. Indeed, in some instances, firms are now entirely dependent on third party providers. Furthermore in some areas there are significant concentrations with many firms relying on one or a small number of third-party providers. Whilst regulators expect firms to manage the risks associated with outsourcing, managing this concentration risk is a challenging task. Especially when there are no ready substitutes, the power to negotiate is limited or substitution is insufficiently tested.

Whilst I have rightly celebrated the developments in new technology over 30 years in truth we have never quite left the past behind. Indeed, for some firms there is still live code on the systems written well before I arrived in the City. Consequently some technology experts appear to have more than a passing resemblance to the local archaeologist, as they scrape away each layer of technology in order to reveal the very old technology on which a system is built. Some of this buildup is not simply organic, but has been the result of mergers and acquisitions which forced the integration of evermore complex technology platforms with existing older platforms. And as most of those integrations were often explained in terms of promoting cost efficiency, it was often impossible to make the business case to simplify the technology. It was just too expensive.

The next biggest change has been the speed with which we work. When I started work we still had a typing pool and there were two computers, mostly for spreadsheet work, between eight of us. The pace of work was slower. When stock and futures markets crashed in 1987, computerised trading was blamed for exploiting existing market vulnerabilities and causing one of the biggest single day market declines in history. 23 years later, the 2010 Flash Crash, again showed the potential of technology to contribute to sharp market movements, but this time movements were measured in milliseconds rather than days. Faced with this reality, many trading companies have chosen to relocate some of their infrastructure or build super fast networks in order to beat their competitors to an arbitrage by the odd nanosecond. This speed means of course that the ‘oh no second’ (i.e. the time between pressing send and realising you have made a mistake) has radically reduced.

I will end my tour of developments, with one of the more recent changes - the Cloud. We have seen a huge increase in the number of firms considering a move to the Cloud. Regulators have also been active - the European Banking Authority issued guidance in December 2017 and they are applicable from 1 July 2018. In many ways, the Cloud is just another outsourcing option and consequently can be viewed in much the same way as we did, other technology outsourcing (to which I have already referred) or the moves by the

financial sector to move a number of technology and back-office functions offshore to India for example, twenty years ago. That means, for the Cloud, it is important for a firm to set out the relative importance of all of its information assets and processes and consequently determine which are within its appetite to put in the Cloud. After that, it needs to determine the level of effective control it retains. The right of access to review controls, and the strength of its contract for example. Then the quality of service it expects to get and finally what exit options it has. A firm can get very stuck if it has no effective options to move, when its outsource provider is no longer delivering an adequate service. Despite news of some outages, the Cloud can often provide a more secure environment for many firms than they can provide themselves. However the dominance of just a few providers means that many buyers are not in a strong position to negotiate contract terms with their Cloud provider. This can leave them badly squeezed between regulatory requirements that will often look through an outsourcing and little leverage with their Cloud Supplier who is unregulated to deliver against the regulations. The concentration of providers is also a concern - given the contagion effect and it has to be acknowledged that they must be a very tempting target to any cyber criminal.
Fortunately the Cloud providers are focused on these risks, given their entire business models are dependent on the provision of operationally resilient services.

So what sort of modern financial system has been created over this last 30 years? Well, it has many components (regulated and unregulated), multiple dependencies (that are no longer fully transparent to either its users or its regulators) and it is highly dependent on technology and data. It is in the truest sense a complex system. In such systems the impact of any shock is difficult to predict and contain. With many multiple transmission channels in play, its perimeter is hard to police.

As the Financial Crisis reminded us with a ferocious intensity, the shocks to the financial system from market or credit risk can be very severe. However, as we are now learning the shock from the operational side can be just as significant. And it will be upon these operational shocks and their consequences, that I shall devote the remainder of my time.

Recently I was asked to say a few words to a group of new Operational Risk managers. I told them that they would be pioneers. I foresaw that operational resilience would be seen to be on a par with financial resilience and a key part of a firm's risk profile. I felt that this would be transformational for many organisations.
So an exciting time? Yes, but operational resilience is hard. However, given the nature of the financial system we have, it is of critical importance.

Banks have been used to safeguarding their financial interests from fraudsters and even bank robbers for decades, but in the case of operational matters the barriers to entry for those who would seek to do harm to the bank are much lower. This brings us to the world of cyber - a key element to operational resilience.
As we have seen in recent years, the cyber attacker like a liquid has found every crack and gap in firms' defences and settled at the level where there are the fewest controls. These can be related to gaps in

process, or technology, people, skills and awareness. The cyber threat brings operational resilience into greater focus and requires organisations to understand themselves, their strengths and their weaknesses. It becomes essential for firms to understand their most critical assets and their most critical functions. What defines critical? Well, several things: the importance to the customer; the importance to the integrity of the firm; and the importance to the sector and the wider economy. Armed with this information they can then allocate their finite resources in the most targeted way. I shall return shortly to this idea of criticality, but I wanted to pause on one further vulnerability.

For many years now in a large number of polls of regulated entities, the number one risk has been the amount of regulatory change. Only recently, has cyber risen to number one on many people's lists. This no doubt is due to the increasing awareness of cyber but perhaps also the slowing down of regulatory change. In truth however, both risks are linked. Organisations are often at their most vulnerable when embarking on change. They often discover too late that weaknesses in their resilience can jeopardise the success of a major project even if those involved believe that they have carried out robust testing. Even though regulatory change may have slowed, the pace of overall change has not. This means, we must find a way to manage the financial system with this vulnerability.

So, with substantial change a fact of life for the financial system and an increasing reliance and dependence on technology, we have seen an increase in the number of operational incidents - be they caused by internal failures or from external attack. In terms of operational outages the financial sector in the UK has had RBS in 2012 which suffered a major outage in its Irish operations and more recently, of course, TSB. In between, there have been many short-term outages. Cyber attacks have also been growing a with a number of very prominent cases: WannaCry and the problems it brought to the NHS, there have also been successful attacks on the Bangladesh Central Bank, Equifax, Yahoo, and Sony. It is not surprising, in this context, that management and boards of firms have been pushing operational resilience ever higher on their agenda.

It has become, therefore, more important than ever for regulators to set out clear expectations of firms in respect of their operational resilience. The Financial Policy Committee, for example, has been considering its tolerance for disruption to the key economic functions that the finance sector performs. As part of this work, it is likely that the FPC will set a minimum level of service provision it expects for the delivery of key economic functions in the event of a severe but plausible operational disruption. I expect this to be a substantial body of work, so it is likely that we will be focused at the beginning and focus on some key economic functions and key providers. As we have embarked on this work, it has been imperative for me to ensure that all of the financial regulators use a common framework. (The number one complaint I receive from industry is the growth in regulatory requirements across the globe that do not seem to be joined up.) A common framework does not mean common tolerances, but it will allow the regulators to build their own tolerances, expectations and approaches under the umbrella of the FPC's overall tolerance. The setting of supervisory expectations would then be used as an input to guide firms' actions in managing their own operational resilience.

My expectation is that these tolerances will use a combination of time, volume, market share and measures of interconnectedness. As any good risk manager will tell you, having a risk appetite is a good start, but you need a toolkit in order to manage to that appetite. We have also been developing a suite of supervisory tools that can be used to assess firms' resilience against our expectations and also inform the supervisory priorities we agree with firms. At its most intensive, we will continue with our very successful CBEST programme of threat-led penetration testing. We are also trialling some other diagnostic tools.

In many cases, this is pioneering work and consequently we will start with a Discussion Paper (joint with the FCA), where we will be inviting industry and fellow regulators for their views.

I will leave the detail of our expectations for the Discussion Paper but I thought I would spend a few moments to give you my perspective on these expectations. I would like our firms to be on a WAR footing: withstand; absorb; recover.

To withstand, we will expect firms to set their own tolerances for key business services. These tolerances should be in the form of clear metrics indicating when a disruption would represent a threat to a firm, to consumers or to financial stability. We will expect firms to test their tolerances and demonstrate to their supervisors that they have concrete measures in place to deliver resilient services. We will further expect firms' boards to play a key role as they develop their operational and cyber resilience strategies. This will include: the setting and reviewing of tolerance; promoting the development of management information; overseeing resilience programmes; and promoting and overseeing investments in technology, systems and people.

Whilst dedicated focus on building resilience may decrease the likelihood of an operational shock severely causing disruption to a firm's critical functions, we expect the firms to build into their approach that operational incidents will still occur. Hence, the need to absorb such shocks when they do occur. Firms will need to clearly define and regularly test their approaches to incident management. These should also include good communication plans both internally and externally.

And firms need to be able to recover from an operational incident. This requires viable, tested contingency plans for the resumption of critical functions. One pleasing development I can record over these last few years is that firms very rarely these days seem to believe that they should not admit to vulnerabilities. They accept that this is not a competitive issue. This has boosted collective fora such as the Cross Market Operational Resilience Group ('CMORG'), which provides a platform for coordinating and promoting work, both aimed at strengthening resilience of the financial sector and improving its ability to respond to operational incidents. The CMORG regularly conducts sector wide, scenario-based exercises that can help firms and the sector in this WAR programme. Past exercises in the UK have led to concrete deliverables, ranging from sector wide contingency plans on how to recover critical economic functions to specific enhancements of joint response protocols. The growth in this collective and collaborative approach has lead to improvements in the timely notification of incidents, their underlying causes and successful remedies, to both the authorities and appropriate stakeholders. It is another key plank in the WAR approach.

We can always go further and with this in mind CMORG has commissioned a review of incident management in the financial sector (“Project Strider”). The review has concluded that there is a need for greater coordination and more rapid information sharing during a cyber incident. Recommendations included: creating a standing cyber response capability for the financial sector (both during and outside standard working hours); creating a common incident taxonomy and maintaining the industry’s guidance on how to respond to a cyber attack; and bringing together risk assessment capabilities from across the financial sector and the NCSC, with a view to regularly reporting shared analysis and creating a joint risk register.
I’m pleased that some of these lessons are being taken forward internationally. The Financial Stability Board is building its own taxonomy. The G7 is testing incident management protocols. Cyber actors know no boundaries, so the response needs to be cross-border and co-ordinated. There is much still to do, but I am happy to say that in the issue of cyber and operational resilience I have found the most collaborative approach in all my thirty years as a regulator.

Before I draw to a close, I wanted to spend a few moments on the response to incidents. The UK authorities have a well established response protocol. It is imaginatively called the Authorities Response Framework or ‘ARF’. It consists of the Treasury, FCA and the Bank. In cases of cyber events the National Cyber Security Centre is also a member. Any member can trigger the ARF and it has three response levels: monitor, engage and manage. These response levels are managed by increasingly levels of seniority in the authorities. Typically it is triggered when events need coordination across the agencies or there are sector-wide implications. A few years ago the ARF was rarely triggered, but more recently this has been increasing. Partly because we deliberately lowered the barrier to trigger - in response to our observations on how operational events developed - but also because of the greater frequency of events. The ARF provides an important co-ordination function for the authorities, which all have their independent functions to carry out. It allows intelligence to be pooled and common issues to be discussed and approaches agreed. In the case of operational resilience or cyber this is vital. The UK regulatory system is largely drawn up for consequences not causes: financial stability - the FPC, consumer and market conduct - the FCA and safety and soundness - the PRA. The ARF also feeds into the Government-wide incident response framework - ultimately up to COBRA.

In my thirty years, operational resilience is certainly not a new topic nor are all of its challenges unique, but two broader trends have conspired to make it today one of the most important.

- First, the cyber threat has highlighted why operational resilience matters: cyber incidents exploit weaknesses in the resilience of organisations, its technology, its systems and its people. Moreover, the cyber threat is constantly evolving. And there is growing evidence that those evolutions are happening over much shorter time intervals. As such, when the G-7 published its cyber guidance in late 2017, it emphasised the need for firms and authorities to be adaptive; to embrace continuous learning and to avoid a static fortress mentality.

• Second, there is an increasing awareness that technological change, and our own behaviour in response to change, creates new fragilities. Armed with online applications, market participants can respond quickly to market news. They also expect instant access to accounts and payment services. With the advent of social media, market participants can comment on operational incidents, within seconds. So if someone is unable to access their funds online, the world will know about it a few seconds later.

I was speaking at a conference the other day. I was on in the first session after lunch. In the morning the conference ran a series of plenary sessions and in the afternoon, there were two streams: one was on FinTech and one, mine, on Cyber. I remember thinking that this was a very good personality test: optimists to the left and to the FinTech talk, pessimists to the right and to the Cyber talk. Today I want to close by being more balanced and remind you of the huge opportunities that technology brings and the incredible change that I have witnessed in my career. Technology can help create new financial services and products, new approaches to risk management and indeed reach new customers.

So what about the next 30 years? Clearly the last 30 years has taught us that there can be few certainties. What will the impact be of consumers wishing instant access to their account or even being able to switch provider in an instant? Or the changes brought about by challenger banks using the latest technology to offer state-of-the-art banking services? Or the incumbent bank finally deciding that keeping their legacy infrastructure is no longer compatible with a robust approach to operational resilience? Or technology firms, large or small, able to offer new approaches to data analysis, risk management, or frontline financial services? Who can predict the impact of machine learning and artificial intelligence or of FinTech? And given the break-up and re-building of business models, where society will draw the future regulatory perimeter?

But, I'd like to offer two certainties for the future. The first, unless my savings have been taken in a cyber attack, of which I'm currently unaware, I'm clear that I will not be supervising the sector in thirty years time. Second, and as I haven't gone yet, I commit and indeed I call upon you also to commit that whatever the next 30 years brings in terms of technological change, alongside we will have built a far more resilient system. One able to withstand growing threats, able to absorb shocks when they do occur and able to recover quickly from any operational incident so that the critical functions in which customers, the sector and the economy rely are unaffected. That would be something to celebrate.