BANK OF ENGLAND

Speech

Cyber in context

Speech given by
Andrew Gracie, Executive Director, Resolution, Bank of England

The UK Financial Services Cyber Security Summit, London
2 July 2015

It is the prerogative of the keynote speaker to take an Olympian view. I am not sure what the gods on Olympus would have made of cyber. Indeed from the goings on in Greek mythology, it could well have been that they were cyber perpetrators rather than protectors. So perhaps it is fitting that there are hacks now like ZEUS that carry their names.

But my Olympian view will try and put the work that we are doing as authorities and with the sector in context. The sector's role is important. After all, it is the responsibility of firms first and foremost to ensure that they are resilient to cyber attack. From an authorities perspective, cyber is somewhat different, but it relates to the same underlying goals that drive our policy interventions elsewhere in relation to operational resilience. I want to describe this relationship before turning to the specific steps that we have taken in the UK over the last two years under the aegis of the Financial Policy Committee (FPC).

Cyber is relevant to many of the functions of the Bank of England as a financial authority. We are responsible as prudential supervisor for the safety and soundness of banks, large investment firms, insurers and financial market infrastructure. As the financial stability authority we are also responsible for monitoring stability at the level of the sector as a whole. While we have multiple policy hats the common denominator in this space is ensuring that the sector has adequate operational resilience – that is that firms can continue to provide critical services that are important for their own integrity and the functioning of the sector. If a firm's operations are interrupted, we want to be sure that they can be recovered quickly and reliably especially where they are systemically important.

Three observations at this point:

a) First to stress our accent on financial stability. Our efforts target first those firms where operational failures may result in disruption to the provision of vital financial services to the real economy or in dislocation to the rest of the sector. That does not mean the failures in customer facing applications do not matter. It is just that, where no immediate systemic dislocation results from such an outage, any consumer detriment will be a concern for our colleagues at the Financial Conduct Authority (FCA) more than it is for us.

b) Second, operational resilience is different from operational risk. In operational resilience we are describing a policy outcome we want to deliver in terms of the system functioning. This may be a by-product of effective operational risk management. But the operational risk regime in Basel III[1] is designed to address another potential cause of financial failure in firms and to ensure that banks are adequately capitalised against these risks. It does not target the continued availability of services and resilience directly.

[1] This refers to the capital regime only. Additional guidance on operational resilience can be found in the Basel core principles (http://www.bis.org/publ/bcbs195.pdf)

c) The third observation is that at the level of the sector our risk appetite has targeted limited disruption in firms that are critical for system functioning. For example FMIs supervised by the Bank as systemically important, set their standard of availability above 99%. And where firms suffer outage we expect them to have business continuity arrangements that allow them to recover immediately or within hours. Firms as a result have established primary and secondary sites, at a suitable distance from each other, with data mirrored between the two. At the sector level as authorities we have concentrated on ensuring that in the event of a significant disruption to one or more firms we can share information and coordinate actions across firms in the UK market to minimise the impact of system stability and to speed full recovery. These arrangements, including senior level groups for coordination in and out of crisis – Cross Market Business Continuity Group (CMBCG) and Cross Market Operational Resilience Group (CMORG) respectively, are tested periodically to work through how the system would function in the face of particular types of shock or the loss of key systems. By definition, crisis events are unpredictable but regular exercising helps to establish common reflexes that will manage the consequences of a major operational disruption, including aspects that may not have been foreseen.

Having set out the context and described our interest in operational resilience, let me turn now to cyber. It is one shock among many that could result in operational disruption. But cyber has specific characteristics that differentiate it from other threats to operational resilience.

First it is not a game against nature. There are groups out there that are motivated to attack the sector. For most, the motivation is economic; that accounts for the rise in fraud. But there are actors out there, sometimes state-sponsored, who may be motivated to bring systems down and cause harm to the sector.

Second it is adaptive and changing. Attackers do not stand still. Attack types are constantly evolving and readily scalable. In the cyber arms race, costs are stacked in favour of the attacker, not the defender. Organisations cannot rely on building a hard perimeter. They too need to develop defensive capability that is adaptive and invest in threat intelligence to understand potential attackers and attack types.

Third detection is not easy. Compromise of networks or attacks themselves will not always be obvious. Diagnosis may take time. By contrast physical threats to operational resilience – bombs, fires, floods – are immediately apparent. And apparent too to the rest of the sector.

Fourth capacity to recover may be threatened. Standard approaches to achieving continuity – operating with common systems environments between primary and secondary sites and mirroring data between the two, could, in the face of a successful cyber attack, be vulnerable to complete loss of applications or destruction of data, disrupting a firm's capacity to operate and leaving the timeframe and route to recovery uncertain.

Hence the FPC recommendation in 2013 that relevant authorities should undertake work to test and improve resilience to cyber attack of the firms at the heart of the financial system[2]. You will have seen from the FSR published yesterday[3] that interest in and awareness of this risk continues to grow. This is why it is so vital that firms – and authorities – take the necessary action to address their cyber vulnerabilities.

In response to the FPC's 2013 recommendation our work has been mostly diagnostic, concentrating on assessing the vulnerability of the UK financial sector to cyber attack. Our focus has been twofold: a cross-sector review of current risk management processes via a detailed firm self-assessment questionnaire and bespoke voluntary vulnerability testing, known as CBEST[4]. The conclusions we have drawn from this work can be broken down into three core areas:

1. Defensive capabilities
2. Recovery capabilities
3. Effective governance

1. Defensive capabilities

Yesterday's Financial Stability Report (FSR) describes defensive capabilities as capabilities that "enable firms to identify and withstand attack." This is important from a financial stability point of view not only for those firms that, as part of the cyber programme, we have identified as 'core' to the sector, but also relevant to their suppliers and other firms they trade with. It implies a level of resilience that goes beyond basic cyber hygiene but aims instead to ensure that firms are in a position to manage Advanced Persistent Threats (APT). While not wanting to go into too much detail on the cyber work programme[5], three key themes are relevant here.

- The first is that **cyber is not just about technology**. People matter. More often than not attackers may seek to exploit potential weaknesses in personnel, to establish a bridgehead for attacks. It is therefore essential that firms have the right arrangements in place so that all staff understand cyber risk and their responsibilities for information assurance.

- The second is that **cyber requires investment**. In people and in systems. Underinvestment in cyber defences may mean that firms are behind the game in terms of their ability to respond to crystallised threats. For example, they could risk misdiagnosing a cyber attack as an internal IT failure rather than a deliberate attack.

[2] http://www.bankofengland.co.uk/publications/Documents/records/fpc/pdf/2013/record1307.pdf
[3] http://www.bankofengland.co.uk/publications/Pages/fsr/2015/jul.aspx
[4] http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx
[5] For more detail see http://www.bankofengland.co.uk/publications/Documents/speeches/2015/speech792.pdf

- The third is **the importance of regular vulnerability testing**. We launched CBEST, a controlled, bespoke, voluntary cyber security testing framework which aims to bring to bear the best available intelligence on potential threats to test directly a firm's ability to protect, detect and respond to cyber attacks.

2. Recovery capabilities.

But even with improved ex ante resilience, no network is impenetrable. Hence why firms' recovery capabilities are equally important. We still need firms to work to be able to resume vital services quickly and reliably in the event of operational disruption. We are keen to see firms adapt their approaches to business continuity planning to take account of cyber. One possibility raised in the FSR is seeking more segregation between primary and backup systems.

3. Effective governance

I mentioned earlier it is for firms in the first place to be responsible for their cyber resilience. I've also noted that cyber is about people as much as it is about technology. And let me be clear, the responsibility for understanding this risk extends beyond technology specialists; firms' boards need to view cyber risk as a core strategic issue and be in a position to challenge senior management in all business areas on the adequacy of their arrangements to deliver cyber resilience.

Going forward

So this is where we've got to on cyber. But now it's clear we need to place cyber on a more permanent footing. This is why the FPC has replaced its existing cyber recommendation with a recommendation targeted at completing the current set of CBEST tests and making them a regular part of supervision. The FPC has now recommended that the Bank, PRA and FCA "work with firms at the core of the UK financial system to ensure that they complete CBEST tests and adopt individual cyber resilience action plans. The Bank, PRA and FCA should also establish arrangements for CBEST tests to become one component of regular cyber resilience assessment within the UK financial system."

In response, following on from the FPC's recommendation, the Bank will therefore:

- Seek to embed CBEST within our supervisory framework;

- Undertake a broad, joint work programme with the FCA and HMT to enable the FPC to consider whether additional action is needed to address cyber risk. Both to improve ex ante cyber resilience in firms and ex post responsiveness; and

- Ensure the framework for cyber resilience is both alive to the special features that cyber possesses but is also joined-up with our approach to deliver operational resilience of the sector more generally.

And of course with all of this, we know that cyber knows no borders. Hence the importance of continued cooperation with our international counterparts.

At the beginning of this speech, I set out the Olympian view of the threat cyber poses and its broader context i.e. cyber matters because the operational resilience of the sector matters to financial stability.

On the ground however, we still have a lot of work to do, hence the importance of a new FPC recommendation and ensuring that cyber has a permanent footing in management of the sector's operational resilience.