Andrew Gracie: Cyber resilience – a financial stability perspective

Speech given by Mr Andrew Gracie, Executive Director of Resolution of the Bank of England, at the Cyber Defence and Network Security conference, London, 23 January 2015.

* * *

In the last few weeks in mainstream media cyber has been to the fore. The hacking of Sony[1] and related reports of attacks on nuclear reactors in South Korea[2] provide a salutary reminder of what we are up against. The threat is there not only to steal data but to disrupt or destroy the functions of a firm. Detecting threats, being ready to respond to attacks and the capability to recover all pose new challenges for firms in every sector.

In the finance sector, we have to contemplate the possibility that core functions in firms, the financial market infrastructure that links them together or the supply chains that support them, may be damaged in a cyber attack, either through the corruption or loss of data or outright loss of systems.

These are issues we already think about in the context of other types of major operational disruption.

But the risks around cyber are different. Detection of a problem may be more difficult. There is not the same symmetry of information that there might be in the event of bomb, flood or fire. And the mechanisms we have put in place to manage these risks may not protect against a cyber attack. Our current approach to ensure firms are able to continue to operate core functions in a major operational disruption involves ensuring that firms have primary and secondary sites at a safe distance from each other and the capacity to switch operations between the two without any extended interruption in activity. But with cyber such common systems environments between primary and secondary sites and mirroring of data between the two could, in the event of a successful attack, result in a complete loss of systems, disrupting a firm's capacity to operate and leaving the timeframe and route to recovery uncertain.

Unlike most other forms of operational disruption, we know too with cyber that this 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. Their capabilities vary, but it is in the nature of cyber that attack types are constantly evolving and readily scalable. And the threat is international. Attacks can originate anywhere around the globe.

This all implies a different disposition for cyber defence. We should not expect to build an impermeable perimeter that, through technology design, will withstand attack. Rather we should expect the cyber threat to be ever-present, ever-evolving and networks to be penetrated. The capability to identify where this has occurred and to respond is key. Part of this is active engagement with threat intelligence to understand likely adversaries, their motivations and ways of working.

For all these reasons, addressing cyber risk in the financial sector is a high priority for the Bank of England. It touches on most of our responsibilities – as prudential supervisor of financial firms, as supervisor of financial market infrastructure – and operator of financial market infrastructure (of real time gross settlement (RTGS)) – and as UK authority responsible for financial stability. Financial stability is the unifying objective in all of these responsibilities. It means that, in the spectrum of cyber attacks, we are much more concerned about those that have the potential to disrupt the UK system by damaging the operations of key firms or financial

---

1 http://www.bbc.co.uk/news/entertainment-arts-30512032.

2 http://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack.

market infrastructure and to understand how that damage could transmit through the sector, than to deal with individual cases of cyber fraud. Such cases of consumer detriment are for the Financial Conduct Authority (FCA), law enforcement agencies such as the National Crime Agency, the police and the Home Office to address.

In response to the rise in the potential threat to UK financial stability from cyber, the Financial Policy Committee (FPC) in June 2013 recommended that the UK authorities should work with firms at the core of the system to test and improve cyber resilience. I want to spend the rest of this speech outlining what we have done in response. The accent has been on assessing the vulnerability of the UK financial sector to cyber attack. We are doing that in two ways: a cross-sector review of current risk management practices with regards to cyber and vulnerability testing via CBEST. Let me describe these in turn.

As a first step in diagnosing the sector's cyber resilience, the UK financial authorities[3] issued a questionnaire to thirty six firms that make up the "core" of the UK financial system. This included the largest UK and foreign banks active in London and the key payment and settlement systems, clearing houses and exchanges that together are critical for delivery of the financial services that the wider economy depends on.

The questionnaire provided for a detailed self-assessment by firms of how they organise their cyber defences. Its purpose was to enable UK authorities to take stock of resilience across the sector and identify best practice across firms. Part of this was to be able to play back to individual firms where they stood relative to best practice. But lying behind this is the objective of raising resilience in individual firms by ensuring that the network as a whole is resilient. And given the importance of these firms to the stability of the financial system, this 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) that are the hallmark of some state-sponsored attackers.

We are currently discussing the results from these questionnaires directly with firms. You will appreciate that I cannot go into specifics. But overall the responses did not reveal any immediate critical shortcomings in the cyber resilience of the firms involved. But they did point to areas for improvement that we will be following up on with firms. Let me list some common themes.

1. ***Cyber has changed the rules***: existing operational resilience arrangements are often geared to dealing with physical threats. These still matter. But cyber changes the game. Cyber is a dynamic, intelligent and adaptive threat. In the cyber arms race, costs are stacked in favour of the attacker, not the defender. To meet the challenge, organisations need to have policies and processes that are dynamic, intelligent and adaptive too. This means investment in capability to identify threats and detect cyber attacks. Without this situational awareness it is hard to determine and achieve appropriate maturity levels for cyber defence and to allocate resources effectively to meet the threat.

2. ***Cyber is not a minority sport for technologists only***: Of course the first line of defence is critical and we still need IT specialists who understand the technical challenges cyber presents. But good cyber resilience is about much more than technology. It is about culture too and this means people and processes. When Morgan Stanley reported recently its customer information had been breached, this wasn't due to sophisticated hackers, rather an employee who stole data from over 350,000 customer accounts. All parts of an organisation need to understand cyber risk and their responsibilities towards improved cyber hygiene. This includes Board level engagement. Front line business areas need to understand and own the risk. Management of cyber vulnerabilities needs to feature in strategic planning.

---

[3] The Bank, Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA).

3. ***Cyber requires effective and regular testing***: Of people, processes and technology. Industry investment in cyber is significant but testing the effectiveness of this investment has not kept pace. Assurance is often based on audits and control sampling which is not sufficient, not least because of the challenge for internal audit departments to keep pace with change in this area. And of course, given the dynamic nature of the threat, such tests should take place on a regular basis.

This leads me onto the other element of our response to the FPC recommendation I wanted to talk about: vulnerability testing through the CBEST[4] program. CBEST is a framework that we have developed working with government, industry and commercial providers of penetration testing and threat intelligence.

The idea is 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. The scope of a CBEST test is tailored to the business of the firm and the critical services it provides. Given the scope, relevant intelligence on threats and attack types is drawn together from threat intelligence providers, including government sources, and is used to design a series of tests that mimic the methods that are most likely, according to the threat intelligence, to be deployed against the firm. The companies providing the penetration test are accredited within a framework that has benefitted from GCHQ input and delivery of the test is within a controlled testing process agreed between the firm, the authorities and the test provider.

The results should provide firms – and us – with a direct read on the robustness of their defences to more sophisticated attack types and a gaps analysis so that firms know what steps they need to take to improve their resilience.

This is not a regulatory requirement though we are encouraging firms to participate. Rather it is a voluntary process. But we think the benefits to firms of CBEST are significant. This is why the FPC in December encouraged firms to undergo a CBEST as "soon as practicable"[5]. By going through this process, firms will not only understand where their vulnerabilities lie, but also which threats should cause them most concern and what steps they should take to combat them. Access to direct feeds of commercial and government intelligence, via accredited red team testing by cyber experts, ensures that the test involves the most up-to-date threats, most relevant to their specific situation. And we are keen for other sectors, and other jurisdictions, to benefit from our experiences[6].

CBEST was officially launched in the summer with the same thirty six firms that participated in the questionnaire. Tests are at an advanced stage for a number of firms and we expect to include the results when we report back to the FPC in the coming months.

So this covers how we are responding to the FPC's recommendation. But we are also looking beyond this.

I have already noted the benefit for individual firms of enhanced cyber resilience across the sector. To realise that, firms need to cooperate not compete in this space. With that in mind, we are working with industry to strengthen arrangements for information sharing, reviewing existing forums for tactical information sharing and supplementing them where necessary with arrangements for more strategic information sharing including on good practice. We are also working with the sector on how existing arrangements for responding to a major operational disruption would work in the event of a severe cyber attack. We have used simulation exercises

---

[4] Further information on CBEST can be found on the Bank of England's website: http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx.

[5] http://www.bankofengland.co.uk/publications/Documents/records/fpc/pdf/2014/record1412.pdf.

[6] All of the CBEST material is available under Creative Commons Copyright (free) on the Bank of England's website.

like Waking Shark II[7] to test response frameworks. And, as was announced last week, a joint testing programme between US and UK governments and authorities will start this year. This answers to the fact that cyber knows no borders and the significant operational interlinkages between our systems and it reflects the growing dialogue with the US and others as to how best to manage the risk to financial stability from cyber.

So it is clear the world has changed; cyber is an ever-present threat. Firms need to stand ready to manage this risk. And just as cyber has changed the world for firms, it has also changed the landscape for authorities; we need to adapt our approach to operational resilience of the financial sector as a whole. Our work in response to the FPC's recommendation typifies this; but we will continue to work with firms, government and cyber experts to learn and evolve our approach.

[7] http://www.bankofengland.co.uk/financialstability/fsc/Documents/wakingshark2report.pdf.