BANK OF ENGLAND

Speech

Managing cyber risk – the global banking perspective

Speech given by

Andrew Gracie, Executive Director, Resolution, Bank of England

British Bankers' Association Cyber Conference, London

10 June 2014

I would like to talk today about the financial stability dimension of cyber and the steps we are taking in the Bank to combat the threat.

Financial stability usually conjures up questions about capital and liquidity and the network of financial exposures and interdependencies that make up the financial sector. But the sector is an operational network too. On a daily basis it delivers financial intermediation between market participants and end users, whether the transmission of salaries and other payments from one bank account to another or the settlement of securities trades through a web of settlement banks, clearing houses, settlement systems and custodians. The Bank as supervisor of banks, insurance companies and financial market infrastructure needs to ensure that each of the nodes in this network is operationally resilient and in a position to provide the services that are important to the system as a whole. We also need to ensure that where disruptions do occur firms can continue to operate or recover quickly, minimising any adverse impact on the functioning of the system as a whole. We have worked closely on these issues with industry, in partnership with HMT and FCA, over the last decade or more since 9/11, and have a well-established response framework for dealing with major operational disruptions in the sector when they occur.

But cyber presents new challenges. It is not a game against nature. Unlike other causes of operational disruption like fires and floods, we know there are agents out there – criminals, terrorist organisations or state sponsored actors – that have the will, if not necessarily the means, to attack the system. Motivations vary. More often than not they are economic – to defraud banks or their customers or to extract information. But we have seen cases where the motivation is to damage the system, either to destroy data or cause non-availability of systems or both. The capabilities of these actors, and thus the nature of the threat, are rapidly evolving – barriers to entry are low in cyber space and attacks are readily scalable. Low level attacks are now not isolated events but continuous. Unlike physical attacks that are localised, these attacks are international and know no boundaries. Cyber defence as a result has become not a matter of designing a hard perimeter that can repel attacks but detecting where networks have been penetrated and responding effectively where this occurs. As it changes and multiplies cyber is elusive, hard to define and to measure. But it is clear that the risk is on the rise and a growing cause of concern to industry and authorities alike. In 2013 the Bank of England's Systemic Risk survey reported a 10% increase in concerns regarding operational risk (the highest level it has been since the survey began). The risk was cited by 24% of respondents. The threat of 'cyber' attacks was the most commonly mentioned specific risk in this category.

In response, in June 2013, the Bank of England's Financial Policy Committee recommended that the relevant authorities should undertake work to test and improve resilience to cyber attack of the firms at the heart of the financial system[1].

[1] *"HM Treasury, working with the relevant Government agencies, the PRA, the Bank's financial market infrastructure supervisors and the FCA should work with the core UK financial system and its infrastructure to put in place a programme of work to improve and test resilience to cyber attack."* The full FPC report can be found on the Bank of England's website: http://www.bankofengland.co.uk/publications/Documents/records/fpc/pdf/2013/record1307.pdf

In response to the recommendation, the Bank and FCA first undertook a systematic survey of cyber resilience within the sector. A number of firms, comprising the largest banks, investment firms, payment systems, clearing houses and exchanges, completed a questionnaire on their cyber risk management practices. The questionnaire serves both microprudential and macroprudential objectives. It allows supervisors to evaluate cyber defences in individual firms. But it also allows us to look across the sector to identify good practice and benchmark capabilities between firms. No firm is an island and ultimately one firm's resilience will be reliant on that of its neighbours. There is a shared interest therefore in ensuring that the sector as a whole is adequately robust to a similar standard. Our aim via the questionnaire is to be able to tease out where good practice lies and the level of cyber resilience we should be seeking from the firms that are most important from a systemic perspective. This is likely to go beyond existing standards like the Ten Steps[2] if firms are going to be able to withstand Advanced Persistent Threat (APT) attacks that might have a systemic impact.

The questionnaire can help establish a framework of good practice but ultimately it is a self-assessment process. We still need to know how this compares to reality and how far the capabilities that firms have in place are adequate for the threats they face.

This is why we have worked with industry and the official sector to devise a new framework – CBEST[3] – for testing cyber vulnerabilities. The idea of CBEST is to bring together the best available threat intelligence from government and elsewhere, tailored to the business model and operations of individual firms, to be delivered in live red team tests, within a controlled testing environment. The results should provide a direct readout on a firm's capability to withstand cyber-attacks that on the basis of current intelligence have the most potential, combining probability and impact, to have an adverse impact on financial stability.

I know that there are other security or 'penetration' tests in the market right now. However, let me unpack the description above to be clear why CBEST is different and why we see it as a core component to improving the sector's resilience to the threat of cyber-attack:

- **CBEST is intelligence-led**. It is the only source of testing that funnels intelligence direct from UK Government agencies supported by commercial intelligence providers.
- **CBEST is bespoke**. Based on threat intelligence from Government and accredited commercial providers, the test is built around the key potential attackers for a particular firm and the attack types they would deploy. This combination of intelligence and testing goes beyond much current penetration testing. In doing so, CBEST should help to identify vulnerabilities and what needs to be done to address them.

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf

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

- **CBEST adapts to the reality of changing threats.** The direct feed from Government and commercial intelligence means that the threats CBEST mimics remain up-to-date. This is crucial to ensure that CBEST can be used in the long-term; just as cyber threats are constantly changing, so must the content of the framework we've built to help defend ourselves.
- **CBEST is safe**. We have worked with the Council for Registered Ethical Security Testers (CREST), to develop new accreditation standards, including with Digital Shadows on standards for threat intelligence. This is the first time that commercial intelligence providers will be subject to accreditation standards which are bound by enforceable codes of conduct.

CBEST was launched with industry in May. Participation will be voluntary but we expect take-up to be significant given the benefits it will deliver. And as firms take part, not only will the authorities be able to improve their understanding of the resilience of cyber defences in the UK sector, we expect to share the benefits in playing back to the sector the results of CBEST, the vulnerabilities that the tests have identified and how they should be mitigated.

This is part of a broader effort to strengthen information sharing on cyber within the sector. There is already a range of official sector and private sector forums for sharing around cyber threats. Some are business led, others among technology experts. Some are long-established, some are relatively new. But overall there is still a sense that information sharing may not be proportionate relative to the need. Part of this may be coordination, a matter of joining up across different networks within and across firms. Part of it may be overcoming any unwillingness to share but it is increasingly recognised that managing cyber threats should be a space in which industry should collaborate not compete. Indeed, given the prevalence of threats, silence on cyber risks would be a cause not for comfort but for concern.

The establishment of a national framework for sharing information on cyber attacks in CERT-UK[4] is a clear signal that the UK Government is committed to improving the coordination of the cyber effort across all sectors. We support this initiative but will continue to work with industry to improve the effectiveness of existing groups within the financial sector, both for ex ante information sharing on threats but also arrangements ex post for coordinating the sector's response should a major cyber attack occur causing a material disruption to system functioning.

What I have mentioned so far – information-gathering, testing and information sharing – are essential ingredients to improving the sector's resilience to potential cyber threats. Underpinning all of these is a longer-term question about culture. Cyber risk is not just for technology specialists; this is part of a broader issue of how organisations defend themselves against attack.

In some ways, this should not be new. Firms already have defences in place to protect against physical attacks, such as armed robbery or bomb threats. This was ever-real in London in the face of potential

[4] https://www.cert.gov.uk/

terrorist threats. The City woke up to the seriousness of the threat; protective measures such as reporting suspicious packages or checking post for smudges became part of peoples' day-to-day routines. Such measures operate on a few simple premises:

- Just because it has not happened, does not mean it will not.
- Having strong, obvious defences will be a good deterrent against opportune threats but is no guarantee against more sophisticated attackers.
- It is therefore essential that measures remain robust, up-to-date and consistently applied throughout a firm.

This should be no different when it comes to cyber. The threat may have changed – it is now virtual as well as physical but the defences that firms have in place should follow the same logic.

In other ways, however, things will be different. Unlike physical attacks, which are likely to be localised, the impact of a successful cyber attack on the financial system as a whole is potentially more serious from a financial stability point of view. We will still be interested, of course, in firms' backup plans in the event of a cyber attack. Indeed to the extent that a cyber attack could simultaneously take out a firm's primary and secondary sites this is an important issue to address. But we will be as interested in a firm's upstream defences and capacity to withstand or to respond to threats.

This leads me onto a broader question of framing our expectations. Detailed prescription is not going to work. As technology, and the threats related to it, evolve, any attempt to etch standards in stone is likely to become outmoded and ineffective. But we will take a systemic, risk-sensitive, intelligence-based view as to what good practice looks like in relation to cyber; and we will take action in the face of inadequate preparation on the part of firms. Just as the threat evolves and adapts, so will our expectations. Continued dialogue between the Bank and industry will be essential to ensure that these expectations are clear. Given the cyber threat transcends borders, we will also need to work with international counterparts, to ensure that any expectations are clear and coordinated from a global perspective.

The FPC's recommendation sent a strong signal of the focus of UK authorities on the threat that cyber attacks may represent to financial stability. CBEST is an important part of the response and will help firms improve their defences. But beyond this, it is vital that we continue to work together, regulators and industry, UK and international colleagues, to improve the resilience of the sector as a whole.