A Cyber risk

Cyber attacks can threaten financial stability by disrupting the provision of critical functions from the financial system to the real economy. Progress has been made in understanding the resilience of the financial sector to cyber risk, in part through new vulnerability testing following an earlier FPC Recommendation. The FPC has now recommended that this testing be made a regular part of core firms' cyber resilience assessment. To strengthen their resilience, firms and authorities need to build the capability to recover quickly from attacks. Building these evolving capabilities will require strong governance at both board and executive level, given the adaptive nature of the threat.

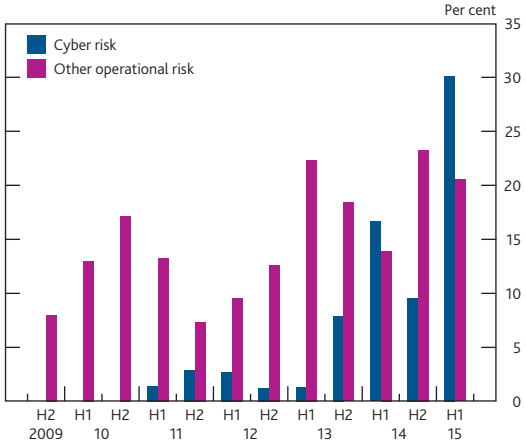
Cyber attack is a growing threat to financial stability…

Cyber attacks have the potential to threaten financial stability by disrupting the vital functions that the financial system performs for the real economy. Such disruption may occur even if firms providing the service remain solvent and otherwise operational. As with financial risk, cyber risk can be amplified by the interconnectedness of the financial system. In particular, a successful attack on a systemic institution or vital infrastructure (including non-financial infrastructure that the financial sector relies on, such as utilities) could cascade throughout the financial system.

The threat from cyber attack is growing, as financial services are increasingly offered via complex and interconnected IT platforms, while access to the technology and skills needed to commit cyber attacks has spread. A 2015 UK Government survey found that 90% of large businesses across all sectors had experienced a malicious IT security breach over the past year.(1) Attackers will change their strategies in response to defensive measures by firms and regulators. Further, cyber risk is a global issue: attacks often cross borders.

Chart A.31 Concern about cyber risk has grown

Systemic Risk Survey: proportion of respondents highlighting operational/cyber risk as a key concern



Sources: Bank of England *Systemic Risk Surveys* and Bank calculations.

…but awareness of the risk is growing…

Awareness of cyber risk has grown, with an increasing number of respondents to the Bank's *Systemic Risk Survey* naming cyber risk as a key concern over the past two years (**Chart A.31**). And the World Economic Forum has identified large-scale cyber attacks as one of the high-impact risks most likely to crystallise over the next ten years.(2)

…and action has already been taken.

Many financial services firms and regulators have made progress in building cyber resilience. For example, a number of industry-led initiatives, such as 'Waking Shark', have been set

(1) PwC (2015), '2015 Information Security Breaches Survey, Technical Report'; www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf.
(2) World Economic Forum (2015), 'Global Risks 2015 10th Edition'; www3.weforum.org/docs/WEF_Global_Risks_2015_Report15.pdf.

Table A.8 Previous industry and regulatory initiatives to address cyber risk

Waking Shark
Cyber attack scenario exercise held in 2011, to test information sharing and co-ordination by firms and regulators in a simulated cyber attack.

Waking Shark II
Repeat of 'Waking Shark' exercise, held in 2013, and focused on crisis communications.

FPC Recommendation
Issued in June 2013, this led to two initiatives: a cyber risk management questionnaire and CBEST vulnerability testing.

Source: Bank of England.

Table A.9 UK financial authorities with responsibility for cyber resilience

HM Treasury
HM Treasury is the lead government department for operational resilience in the financial sector. As such, it is responsible for advising ministers on the resilience of the sector to key risks, such as that of cyber attack, including through the annual Finance Sector Resilience Plan, and identifying policy priorities. It is also responsible for co-ordinating with other parts of government to strengthen resilience in the sector, and in any response to major operational disruption. HM Treasury works with the Bank of England and the FCA and other relevant government agencies to identify which firms and systems are the most critical parts of the UK financial sector.

Bank of England
The FPC is charged with taking action to remove or reduce systemic risks (including cyber risk) with a view to protecting and enhancing the resilience of the UK financial system (as set out in the Foreword to this *Report*). The Bank (including the PRA) develops cyber resilience policy, supervises PRA-regulated institutions, and also leads CBEST vulnerability testing.

Financial Conduct Authority
The FCA develops relevant policy, assesses and supervises FCA-regulated institutions, with a focus on consumer detriment and market integrity. For dual-regulated firms, the FCA liaises with the Bank of England (including the PRA). The FCA is named as a party to the current FPC cyber Recommendation.

Sources: Bank of England, FCA and HM Treasury.

Table A.10 Cyber questionnaire: selected thematic findings

- Overemphasis on technological (as opposed to management, behavioural and cultural) aspects weakens cyber defensive capabilities.
- Underinvestment in the capability to detect cyber attacks in progress, identify threats, and analyse indicators of malicious activity weakens defence capabilities.
- Effective oversight of supply chain and third parties that handle information processing or IT systems is critical to effective cyber resilience.
- Cyber attack can undermine existing recovery arrangements.
- Effective governance: board members must drive a culture of resilience throughout the firm.

Sources: Bank of England and FCA.

up to promote cyber resilience (**Table A.8**). And in 2013, the FPC made a Recommendation that HM Treasury, working with relevant government agencies and the other financial authorities (**Table A.9**), 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. In response, the authorities issued a cyber risk management questionnaire to core UK firms, and themes from this have been used to identify areas for future work. Based on this assessment, the capabilities needed to address cyber risk can usefully be divided into three categories: defensive capabilities, recovery capabilities and effective governance.

Defensive capability should focus on both IT and non-IT vulnerabilities…

Defensive resilience capabilities enable firms to identify and withstand attack.(1) The cyber risk management questionnaire has been used to identify gaps in firms' defensive capabilities (**Table A.10**). A common failing was viewing cyber risk as a purely 'technological' issue, without recognising that people matter as much as technology. Attackers can exploit weaknesses in personnel security (for example, deceiving employees so that they reveal passwords) before turning to more sophisticated hacking. The survey also revealed underinvestment by firms in their ability to detect cyber attack, which creates a risk that firms react to attacks too slowly, or misdiagnose incidents of disruption as internal IT failures rather than deliberate attacks. Further, defensive capabilities need to extend to the suppliers and infrastructure that the financial system relies on.

Vulnerability testing can be used to understand a firm's specific risks and further develop its defences. A vulnerability testing framework — known as CBEST — was launched by the Bank in May 2014 in response to the FPC's 2013 Recommendation on cyber resilience. This provides a framework for bespoke, controlled cyber security tests, based on government and private sector expertise on the threats that firms are likely to face. CBEST tests are voluntary and have been offered to core firms. A number of core firms have already begun CBEST testing, but the process of testing the core of the system is not yet complete. Compared with the benefits of cyber resilience, which while not reasonably practicable to quantify are substantial, the direct costs to firms of CBEST testing (estimated at around £150,000 per test) are low.

…while recovery capability is equally important…

Promoting resilience through defensive capabilities, while important, is not enough to safeguard the system against disruption of critical economic services. It is likely that some cyber attacks will successfully breach firms' defensive arrangements. Developing the capability to resume vital

(1) Defensive resilience capabilities include firms' ability to protect themselves by identifying and detecting attacks, as well as capabilities relating to leadership and learning.

services quickly and reliably after an attack will require effective backup and recovery systems. Cyber attacks can cause data corruption, which can spread between connected systems. Managing this threat is likely to require segregation between primary and backup systems, in contrast to the management of other business continuity threats, where the focus has tended to be on building immediate system backup capacity, through closely connected backup systems that allow for the rapid resumption of services.

…and these require effective governance.

Another important theme from the cyber questionnaire was governance — in particular, the importance of boards viewing cyber risk as a core strategic issue, and challenging senior management where resilience and recovery plans are inadequate. Effective governance includes ensuring that leadership teams have the skills and knowledge required to understand cyber risk, particularly given the adaptive nature of the threat. Cyber resilience is likely to remain an important challenge for boards and senior management.

The FPC considers it vital that work on cyber resilience continues.

The first step in mitigating cyber risk is to have an accurate understanding of where the system's vulnerabilities lie. At its meeting in June 2015, the FPC therefore replaced its existing cyber Recommendation with the following Recommendation targeted at completing the current set of CBEST tests and making them a regular part of supervision:

The FPC recommends that the Bank, the PRA and the 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, the PRA and the FCA should also establish arrangements for CBEST tests to become one component of regular cyber resilience assessment within the UK financial system.

The FPC considers that this Recommendation will have a positive impact on the PRA's and the FCA's objectives. While CBEST test results are expected to be an effective measure of core firms' defensive capabilities, further work is also needed to promote recovery capabilities and effective governance. The FPC therefore endorsed a broader work programme, designed to develop these evolving capabilities (**Table A.11**), for all firms at the core of the financial system. This work will be undertaken by the Bank, the PRA, the FCA and HM Treasury, and will enable the FPC to consider whether additional action is needed to address cyber risk. Recognising that firms outside the financial system provide essential services to the financial system, the work programme includes reviewing the list of those firms so that relevant regulators can take account of that dependency in their own cyber planning. And recognising the global nature of the cyber threat, the programme will involve further co-ordination with international authorities.

Table A.11 Cyber resilience work plan

The work programme endorsed by the FPC will focus on:

- Reviewing the list of core firms to ensure that it captures those most critical to financial stability in the event of a major cyber attack, including those not regulated by the authorities.
- Defining and developing a clear set of capabilities that will enhance *ex-ante* cyber resilience within the UK financial system and improve the effective *ex-post* collective capability of the sector and the authorities to respond to and recover from a major cyber attack.
- Developing co-operation with international authorities to assess and improve cyber resilience in the financial sector, recognising cyber as a potentially cross-jurisdictional threat.

The FPC asked for a report back by Summer 2016.

Source: Bank of England.