Deloitte.

CENTRE for REGULATORY STRATEGY EMEA

Belgium | FSI Insights | 19 December 2016

Regulatory Newsflash
Regulating cyber resilience

Looking ahead to 2017, one of the most important areas of regulatory development that we see in financial services is rising supervisory expectations of firms' cyber resilience. A spate of recent incidents of cyber-crime and IT failure have sharpened the focus of firms on their cyber preparedness, but management and boards should now also expect to be more routinely challenged by their supervisors on how well they understand and what they have done to limit their exposure to cyber and IT risks.

We see an important shift in motion this year and next: regulators are pivoting from exploring cyber as an issue to articulating more specific and more demanding expectations of firms. The UK Financial Policy Committee's (FPC) statement on cyber resilience supervision the Bank of England's (BoE) November Financial Stability Report (FSR) exemplifies how this pivot is now well underway.

As these regulatory efforts continue to gather pace, they will be increasingly likely to cause firms to reconsider their cyber resilience and IT investment strategies.

What are regulators doing?

Although making sure that firms have adequate controls in place to protect their clients' data has always been a concern, the rising exposure of firms to cyber risk has raised potentially greater fears around whether cyber failures could pose a systemic risk to financial markets or cause serious reputational damage to a sector that depends on the confidence of its participants.

As a result, regulators have begun to look particularly closely at cyber threats facing systemically important banks, exchanges and other financial market infrastructures (FMIs). Following the theft of $81 million using the SWIFT network from the Central Bank of Bangladesh,

the Bank for International Settlements established a committee that may eventually develop standards for the protection of inter-bank transfers. Similarly, guidance from the International Organisation of Securities Commissions (IOSCO) and the Committee on Payments and Market Infrastructures (CPMI) earlier this year on the cyber resilience of FMIs included an expectation that such infrastructures have sufficiently robust capabilities in place to ensure that downtimes following a cyber failure will last no longer than 2 hours.

National regulators are responding in turn. In October, the US regulatory agencies jointly released an Advanced Notice of Proposed Rulemaking (ANPR) consulting on Enhanced Cyber Risk Management Standards that they would apply to large banks and FMIs. If pursued, these standards would represent some of the most detailed expectations around cyber risk management that financial regulators have developed so far.

Similarly, the UK FPC's statement on cyber resilience in November's FSR indicated that the first round of the BoE's CBEST cyber vulnerability testing framework has been completed for 30 out of the 35 firms and FMIs identified as 'core' to the UK financial system. CBEST will now be increasingly integrated into the normal supervisory process with firms conducting their own internal testing and additional 'threats' being tested by authorities in coordination with the UK's new National Cyber Security Centre. This forms part of the UK authorities' efforts around cyber resilience, along with ongoing work on developing standards for the supervisory assessment of firms' cyber resilience capabilities. As stated in the FSR, the objective of this work is to ensure that firms' "cyber risks will be subject to the same standard of regulatory requirements as prudential risks are in future."

Efforts are also underway to link firms' cyber and IT resilience with their financial resilience. The European Banking Authority's recent consultation on Guidelines to assess information and communication technology (ICT) risk in banks sets out a methodology for supervisors to gauge the level of exposure firms face to cyber and other IT risks, the measures they have put in place to control them, and to link that assessment with the operational risk score in their annual Supervisory Review and Evaluation Process. This could eventually lead to supervisors setting higher Pillar 2 capital requirements for firms if they are seen to be unprepared for dealing with their cyber risk exposure.

What are supervisors looking for?

When assessing the cyber and IT resilience of financial services firms, regulators are seeking to ensure that firms have sufficiently prepared themselves in three principal areas:

- **Risk identification and management:** Firms need to demonstrate that they understand the extent of their exposure to cyber and IT risk at all levels of their organisation. This includes understanding their exposure to technology-related failures in outsourced service providers and significant counterparties. Firms should also assess the threat of malicious or criminal activity internally (e.g. employees and contractors) and design appropriate controls to limit this risk. Although this may seem straightforward, for large internationally-active firms with numerous subsidiaries and legacy systems, the task of mapping and understanding their exposure to cyber risk has often proven to be very difficult. The UK FSR also noted that some of the most widespread vulnerabilities found in the CBEST exercises have been weaknesses in basic controls that firms' have to protect the integrity and availability of their systems.

- **Risk governance:** Regulators will expect firms to develop robust internal governance models to cope with the complexity and pervasiveness of cyber risk. Firms will need to show that appropriate procedures have been put in place to identify and

respond to cyber and IT risks as they arise across the three lines of defence. At the level of senior management, firms will need to determine the appropriate role to have overall responsibility for cyber risk and may also come under pressure to demonstrate that their Board has access to sufficient expertise in and understanding of cyber and IT risks. The UK Prudential Regulation Authority's recent consultation on appointing a Senior Operations function as part of the Senior Managers Regime is evidence of this.

- **Risk resilience:** Firms must also demonstrate that they have developed contingency plans and capabilities to effectively respond to cyber breaches and IT failures in a way that allows them to minimise disruption to their own operations and the rest of the financial system. One focus here will be on ensuring minimum downtimes for critical systems. In their ANPR, the US agencies extended the IOSCO/CPMI 2-hour downtime target for FMIs to critical systems in banks. Another area that may come under regulatory pressure is real-time information sharing on cyber threats, where public authorities will likely be keen to see threat intelligence shared quickly thoroughly the industry. Recent signals from the European Commission hint that they may be considering acting as or establishing a central EU coordinator for such a purpose.

What's next?

Regulators and supervisors will progressively move to integrate these heightened expectations around cyber and IT resilience into their normal supervisory work, with their scrutiny increasing for firms and systems that are more critical for maintaining financial stability.

With this new regulatory approach, firms can expect authorities to gradually notch up their expectations as they attempt to move firms along a transition path to a higher (but potentially evolving) state of desired cyber resilience. Given the investment and attention that meeting these expectations will take, firms should follow these developments closely and engage with their supervisors early on to understand how best to respond.

Contact

For further information with respect to this subject, please contact Caroline Veris or Maarten Mostmans.

Caroline Veris
Partner – Governance, Regulatory & Risk

Maarten Mostmans
Partner – Cyber Risk Services

David Strachan
EMEA Lead, Deloitte Centre for Regulatory Strategy