Desktop Cyber Exercise (Waking Shark) - Friday 11 March 2011

1. This exercise took place on Friday, 11 March in the auditorium at the Credit Suisse building in Canary Wharf and ran from 13.00hrs until 16.30hrs. In attendance there were just over 100 representatives from 33 participating organisations representing a broad range of financial firms, infrastructure providers and the financial authorities. There was also an Expert Panel comprising representatives from the Centre for the Protection of National Infrastructure (CPNI), the Serious Organised Crime Agency (SOCA), the Cyber Security Operations Centre (CSOC), the Payments Council, BT and O2. In addition there were 28 non-participating observers mainly from the financial authorities.

2. The idea for this exercise arose from a series of discussions stretching back over many months between the FSA and a range of firms regarding the increasing frequency, intensity and sophistication of electronic attacks upon the IT systems of firms operating in the financial sector.

3. A Governance Group was put in place to oversee the planning and delivery. It was agreed that the focus of the exercise should not be upon the robustness of individual firm's resilience plans but upon how the participants would communicate with each other in order to coordinate their responses to a widespread and systematic cyber attack on the financial sector. Thus the main objectives for the exercise were to:
   - Identify key industry coordination issues in the event of a major attack.
   - Establish recommendations to address any perceived issues or gaps
   - Establish rules of conduct for cross-firm and regulator communication during a cyber attack.

4. A further objective of the financial authorities was to use the lessons learned from the event as input to the design of the scenario for the next Market-wide Exercise (MWE) scheduled for late November this year in which they expect to include a cyber dimension.

5. The exercise was facilitated by Credit Suisse, with the scenario released in three segments. At the end of each segment, participants were required to vote electronically on a number of questions following which there was a facilitated discussion of the responses. Although voting was anonymous, it was open to participants to identify and explain how they had voted.

6. At the end of the event all of the participants were asked to complete feedback forms before they left the venue. All did so. The feedback was overwhelmingly extremely positive with all of the participants indicating that they had found the exercise to be worthwhile and that they would wish to be consulted or engaged in future exercises or follow-up work.

7. With regard to cross-industry communications and coordination - the key aspects of the exercise - there was extensive feedback around the following issues:
   - There is a multitude of existing industry groupings which can be used as mechanisms for cross-firm communications in relation to the business impacts of a major disruption. Is there a potential role for a single agency to perform the role of industry coordinator in such an event? Several respondents suggested that role might fall to the Cross Market Business Continuity Group (CMBCG).
   - Conversely, respondents thought the exercise highlighted the lack of comparable cross-firm communications structures in the IT/Security field. There was awareness of a number of relevant bodies such as CSIRTUK (Combined Security Incident Response Team UK), NSIE (Network Security Information Exchange) and FSIE (Financial Services Information Exchange) but a lack of familiarity with their potential role in a cyber event. Respondents thought that a) this was a gap that needed to be filled, b) consideration needed to be given to how any structures would interact/engage with existing sector-wide groups and c) key infrastructure, technology and security providers should be engaged as part of the coordination.
   - In a similar vein, a number of respondents thought that the sector needed more clarity around the roles of official bodies such as the Financial Authorities, the CPNI, CSOC and SOCA.

8. In order to address these issues the Governance Group has agreed on the following next steps:
   - The Governance Group will remain in place to act as the focal point for follow-up actions.
   - The CMBCG Sub Group will consider whether its membership and terms of reference might be enhanced to enable it to perform the role of industry coordinator that was discussed during the exercise (and what changes this might necessitate in its Terms of Reference).

- Discussions will be held with representatives from CPNI, CSOC, SOCA, the telecoms industry and the providers of IT Security systems regarding a) the possible establishment of a technical forum on cyber issues and b) how that forum might engage with the CMBCG Sub Group.
- The financial authorities will engage with CPNI, CSOC and SOCA on how to provide the financial sector with more clarity on their respective roles during a cyber event.
- On the back of these discussions the Governance Group will consider the extent to which it is possible to fully meet the third objective of the exercise to “Establish rules of conduct for cross-firm and regulator communication during a cyber attack.”
- The Governance Group will produce a report for participants within three months on progress made on these action points.

9. There were several suggestions from participants regarding ways of improving the logistics and content of future cyber exercises. These will be fed into the planning and delivery structure for the November MWE. This will enable the authorities to refine and sustain the level of challenge the MWE poses to participating firms.