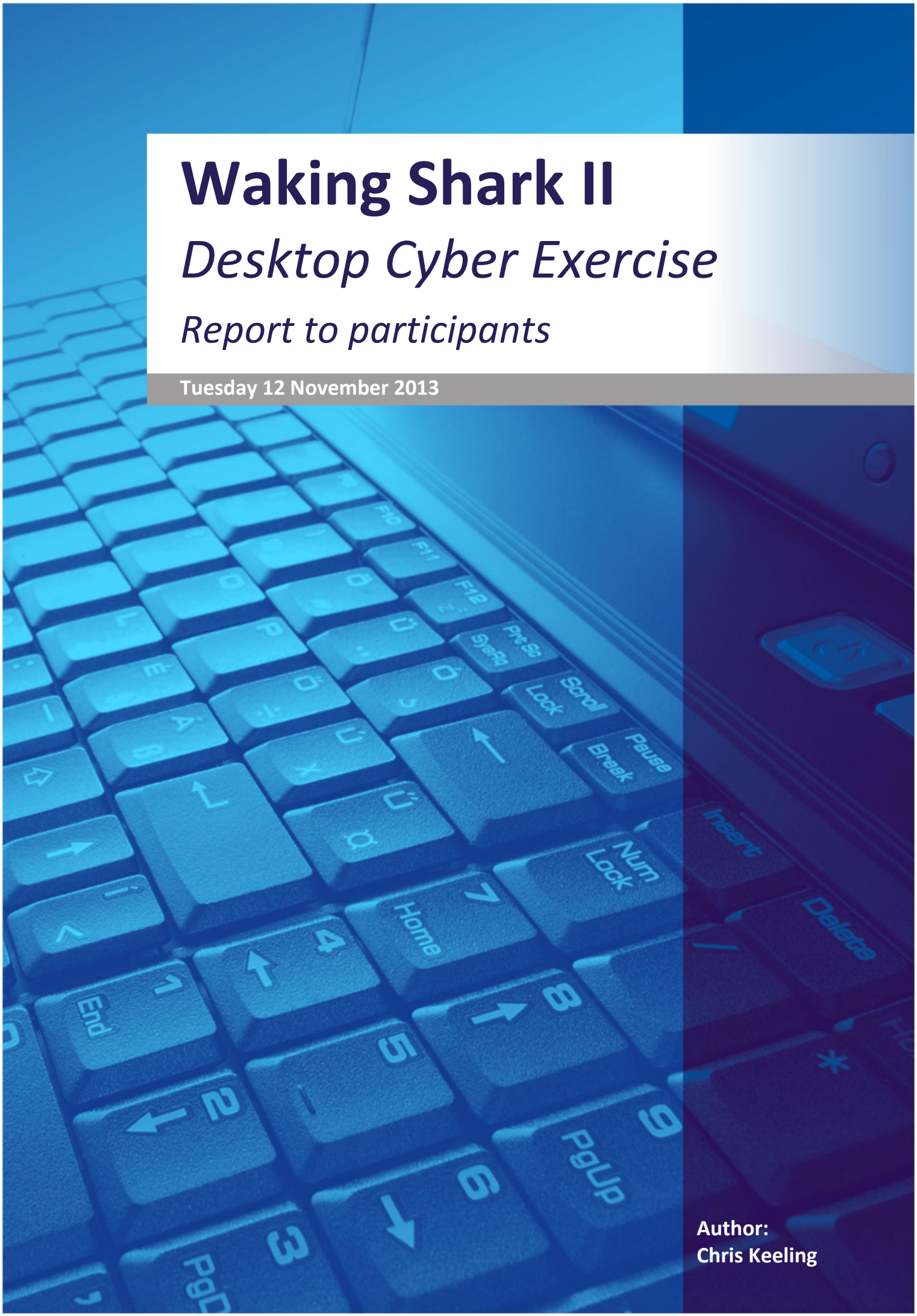
Waking Shark II

Desktop Cyber Exercise

Report to participants

Tuesday 12 November 2013



Author:
Chris Keeling

Summary

The Waking Shark II exercise, held on 12 November, was designed to rehearse the response of the wholesale banks sector, including investment banks and key financial market infrastructure, in working together to understand and minimise the impact of a cyber-attack on the sector, not to test individual firms' cyber response mechanisms.

In this respect, the exercise successfully demonstrated cross sector communications and coordination through the CMBCG, information sharing through the use of the CISP platform and enabled participants to better understand the requirements of the UK Financial Authorities, in particular the PRA and the FCA, in responding to a cyber-attack.

As with all exercises there is an element of artificiality in the issues encountered and the demands of running a three-day scenario in a four-hour session. Exercises of this kind are not simply about validating and rehearsing existing response arrangements. They also provide opportunities to identify areas for further improvement and in this respect the Report highlights several lessons learned that will be progressed in 2014:

- Consideration will be given to the identification of a single coordination body from industry to manage communications across the sector during an incident.
- The PRA and FCA will coordinate to ensure dual-regulated firms are fully aware of the regulators' incident reporting requirements and update frequencies. The Authorities will also provide further clarification to the sector on the respective roles of the Authorities, Government agencies and the sector in responding to major cyber-events and reinforce with firms the importance of reporting major incidents to their respective regulators as soon as possible.
- The CISP platform will continue to be enhanced through close collaboration between firms and Government partners.
- Organisations will be reminded of the need to report attacks which constitute a criminal offence to the appropriate authorities e.g. law enforcement.

As was recommended in Waking Shark I, financial sector participants should continue to regularly review their internal cyber-incident response procedures, and ensure that they maintain engagement with the FSIE, CISP and other external information sharing groups.

With representatives from all the major UK wholesale banks and the UK authorities participating, supported by key industry experts, Waking Shark II successfully challenged the sector in a realistic manner. The lessons learned will not only influence the finance sector's preparedness for a real-life cyber-event, but also serve as an example of how other sectors in the UK's finance industry can test their own capabilities in the future.

Waking Shark II was part of a long-running series of cyber exercises which in turn are part of a wider collective exercising partnership between industry and the Authorities. Encouragingly, post-exercise there is a clear appetite amongst participants to continue this partnership through further and more challenging exercises and a number of useful suggestions were made regarding the shape and content of future events.

Introduction

The financial sector cyber exercise, Waking Shark II, was delivered on Tuesday 12 November 2013 in London. It was designed to follow up and reinforce the lessons learned from previous cyber exercises (Waking Shark I and the 2011 Market Wide Exercise (MWE)) and reflect the continued evolution of the nature, intensity and sophistication of cyber threats over the past two years.

Approximately 220 people attended the event, comprising participants, observers, experts and the facilitation team. The participants included fourteen Firms, six Financial Market Infrastructure (FMI) providers, the Financial Authorities (Bank of England (including the Prudential Regulation Authority (PRA)), Financial Conduct Authority (FCA), HM Treasury) and government agencies.

Exercise objectives

The exercise focused on disruption/dislocation in wholesale markets and in the financial infrastructure supporting those markets as a result of a concerted cyber-attack.

The specific aims of the exercise were:

- To assess whether firms had adopted the feedback and lessons learnt from Waking Shark I, which recommended that financial sector organisations should:
  - Review their internal cyber-incident response procedures;
  - Review their representation and engagement with the existing external crisis, security coordination and information sharing groups (e.g. CPNI, CSIRTUK, etc.) and
  - Assess the mechanisms in place to ensure that the external and internal information available would be leveraged in the event of a cyber-incident.
- To exercise communication and information flows between firms, and between firms and regulators, during a cyber-attack (as established in Waking Shark I), most notably:
  - FSIE as a technical information sharing forum and by using the CISP platform;
  - CMBCG in the role of industry coordinator for such events.
- To improve understanding of the impact of a cyber-attack on the financial sector and how the sector should respond, as identified by the 2011 MWE.

Scenario

To meet the exercise objectives a scenario was devised that placed the sector under severe stress. As such, the elements of the scenario were extreme relative to the cyber-attacks that have been seen to date. The scenario was based on a concerted cyber-attack against the UK financial sector by a hostile nation state with the aim of causing significant disruption/dislocation within the wholesale market and supporting infrastructure. Although the impacts caused by the cyber-attacks would have had an international as well as a UK dimension, for the purposes of the exercise, the scope of the exercise was restricted to management of the UK impacts.

The scenario was set over a three-day period the last day of which happened to coincide with “Triple Witching” (when contracts for stock index futures, stock index options and stock options all expire on the same day).

The three-day period was broken into phases, playing out various technical and business impacts from the scenario. The scenario examined how firms would manage their response to the cyber-attacks both on a technical level (in particular information-sharing amongst the firms via the CISP tool), and from a business perspective.

The following technical and business impacts were included in the scenario:

- DDoS attacks, causing the firms’ global websites and certain other internet-facing systems to be unresponsive or intermittently available.
- APT and PC wipe attacks that penetrated the firms’ networks for disruptive and destructive purposes.
- Issues with end-of-day market data pricing files for some equities markets, causing challenges with overnight risk and margin calculations.
- Issues with Central Counterparty Clearing processes for fixed income, with resulting events causing significant liquidity and funding issues.
- Issues associated with processes used to instruct payments through agent banks and manage balances in accounts at agent banks.

Exercise findings

The exercise findings have been collated from feedback from participants during the exercise (via electronic voting questions) and subsequently (via feedback forms).

Overall the feedback on the exercise was positive with the vast majority of participants finding the exercise to be extremely useful. As with all such exercises, a number of issues were raised in the feedback and this information has been analysed and the key findings presented in the following section.

Objectives

The feedback from the participants was overwhelmingly positive that all the objectives were met.

A particular focus of the exercise was the use of the CISP platform. This demonstrated significant improvement from Waking Shark I in the channels available to share technical information on cyber-attacks and was well received by the participants. It did, however, present a number of technical challenges for CPNI (who were running the Fusion Cell [1] during the exercise) as there were multiple threads running throughout the exercise, making the platform difficult to manage.

Communication and information sharing was generally good throughout the exercise with close collaboration demonstrated between FMIs and communication from the FMIs to the firms. It was noted that there is no central industry coordination for financial sector information sharing and communication to the wider public and it was suggested that consideration should be given to allocating this role to a single coordination body from industry (possibly the BBA) to manage communications across the sector during an incident.

A number of the participants stated that they were unclear as to the process for communication with regulators in the new institutional framework and some dual-regulated firms were unaware that notification to both regulators was a requirement.

The CMBCG was convened during the exercise successfully testing the mechanism for the mobilisation of the group. Some firms thought the group should have convened earlier in the exercise and others felt that when the group did meet, there was little to do beyond sharing information, as there were no systemic issues that needed to be discussed at that time.

Some of the participants considered that the cyber scenario resulted in moderate risk, minimal impact and/or limited challenge while others felt that there were major challenges particularly in relation to payments issues. A number of the participants suggested that the scenario could have been more technically challenging with greater market stress over a longer period. The impact of the cyber-attack was primarily focused on the participating firms and further stress could have been applied to the FMIs, which would have created greater systemic impact. However, it was agreed that the scenario was thought-provoking

[1] The CISP Fusion Cell is comprised of a number of analysts from different Industry sectors and Government departments. The analysts collate and assess cyber incident information from a wide range of sources, and use this analysis to inform a range of products and services. The overarching objective of the Fusion Cell is to improve cyber situational awareness within UK Industry and Government.

and individual firms would have the opportunity to add further stress if they utilised the scenario as part of their internal exercising.

Specific issues that were identified by the participants included the challenge of communicating with clients and understanding how a cyber-attack would impact business transaction flow and service outage.

Delivery

There was overwhelming agreement that the exercise was well organised and delivered.

While the majority of participants agreed that the exercise format was successful in facilitating engagement and interactive discussions, it was recognised that the size of the audience, and possibly the presence of the Authorities, did tend to stifle the discussion. It was suggested that in future exercises, breakout sessions could be used to facilitate more open discussion.

Future considerations

Many of the participants intend to re-use the scenario to run internal exercises; in particular to review the specific impacts and the available mitigations, their incident response frameworks and re-examine internal risk management structures. This will help in identifying the contacts that would need to be mobilised to support internal responses to a significant cyber-incident and when the CISP platform would be triggered.

These exercises should help to deliver improvements in early warning of cyber-incidents across the sector.

Suggestions were also made regarding future scenarios. The most frequent included:

- Broadening the scope to include cross-border issues and possibly participants from outside the UK.
- Increasing the stress on the sector in the cyber scenario, perhaps including more focus on the APT strand, more asymmetry in impact on different firms and greater systemic impact (extended outages, increased pressure on liquidity and funding and more market dislocation).
- More flexibility within the setup of the exercise to increase the impacts of the scenario during the exercise.
- Inviting service providers to attend as participants such as British Telecom.

Lessons learned and recommendations

The findings of the exercise identified a number of lessons:

1. **Financial sector communication**

   Whilst there was some communication between the participating firms and the FMIs and good communications with the authorities, it was identified that there is no formal communication coordination within the wider sector. A number of sector groups are already in place including SIBCMG, IBSIG, CMBCG, FSIE that provide for a framework for communication amongst their members but there is no cross-sector infrastructure in place currently for communication to other financial institutions outside the core systemic wholesale and retail firms.

   Recommendation 1: Consideration will be given to the identification of a single coordination body from industry to manage communications across the sector during an incident.

2. **Regulatory engagement**

   The exercise tested interactions between firms and the authorities highlighting the requirement in the new regulatory structure for dual-regulated firms to communicate with both the PRA and the FCA, and to complete a separate MIDAS form as required by each regulator. Not all firms were fully aware of the requirement to notify both regulators in the new institutional framework. Some firms questioned the reactive nature of the official response and whether the authorities should be more proactive in identifying any adverse systemic impact of the event on firms and in leading or coordinating the sector response.

   Recommendation 2: Firms should be aware of the need to report major incidents to their respective regulators as soon as possible. The PRA and FCA will coordinate to ensure dual-regulated firms are fully aware of the regulators' incident reporting requirements, including frequency of updates. The Authorities will also provide further clarification to the sector on the respective roles of the Authorities, Government agencies and the sector in responding to major cyber-events and reinforce with firms the importance of reporting major incidents to their respective regulators as soon as possible.

3. **CISP platform**

   The CISP platform was heavily used during the exercise, truncating three days of activity into a few hours. This highlights the value of the facility in identifying and responding to a cyber-event and also the amount of work required from the Fusion Cell in managing the information. This has been recognised and the platform will continue to be enhanced to facilitate the timely and secure exchange of information amongst the members.

   It should be noted that the CISP platform was launched in March 2013 and therefore this was the first time many of the users had actively used CISP. Furthermore, the exercise helped raise awareness and increase membership amongst the finance

sector participants. As they become more practised, so they will find it easier to use and get more out of it.

Recommendation 3: The CISP platform will continue to be enhanced through close collaboration between the financial sector firms and Government partners.

4. Engagement with law enforcement

The participants did not engage directly with law enforcement during the exercise in reporting the cyber-attack, primarily because there were no law enforcement representatives present. It is possible that participants considered that law enforcement agencies were aware through the extensive media coverage, or assumed incorrectly that reporting via the CISP platform constituted advising law enforcement.

Recommendation 4: The types of attack witnessed during the Waking Shark exercise would constitute a criminal offence and organisations will be reminded of the need to report such incidents to the appropriate authorities, including law enforcement.

Future exercising

There is a clear appetite amongst the participants for further and more challenging sector exercises. In addition to creating more challenge, other suggestions included:

- Although the exercise provided an opportunity to test CMBCG, it was felt that the group would benefit from more focused and rigorous exercising.
- It is likely that in any cyber-attack, retail elements of the firms' businesses would also be impacted. This would result in significantly greater media pressure than was provided in the exercise. Future exercises should address issues related to cyber-attack impacting retail operations.
- In future exercises it may be beneficial to provide firms with more scenario detail in advance of the exercise and possibly allow part of the exercise to be played out internally before convening in an exercise to respond as a sector.

Participants' suggestions regarding future exercises will be shared with the Sector Exercising Group (SEG), newly established under CMORG, which will:

- Consider shorter and more focused sector exercises on specific issues for certain groups e.g. the inability to settle overnight to be considered by Operations Departments and a short CMBCG exercise for senior executives to consider strategic implications.
- Review how greater challenge could be applied in future exercises.
- Determine how future sector-wide exercises could be delivered, for example, 'pre-exercising' elements of the scenario within firms to consider their individual response in advance of congregating to consider the sector wide issues and responses.

Glossary

APT	Advanced Persistent Threat
BBA	British Bankers Association
CISP	Cyber-Security Information Sharing Partnership
CMBCG	Cross Market Business Continuity Group
CMORG	Cross Market Operational Resilience Group
CPNI	Centre for the Protection of National Infrastructure
CSIRTUK	Computer Security Incident Response Team UK
DDoS	Distributed Denial of Service
FCA	Financial Conduct Authority
FMI	Financial Market Infrastructure
FSIE	Financial Services Information Exchange
IBSIG	Investment Banking Special Interest Group for Information Security
MIDAS	Major Incident Damage Assessment
PRA	Prudential Regulation Authority
SEG	Sector Exercising Group
SIBCMG	Securities Industry Business Continuity Management Group