BANK OF ENGLAND

Press Office
Threadneedle Street
London EC2R 8AH
T 020 7601 4411
F 020 7601 5460
press@bankofengland.co.uk
www.bankofengland.co.uk

News release

10 June 2014

Bank of England launches new framework to test for cyber vulnerabilities

In a speech today at the British Bankers' Association, Andrew Gracie, Executive Director, Resolution at the Bank of England, formally launched a new framework to help identify areas where the financial sector could be vulnerable to sophisticated cyber-attack. This is part of the Bank of England's response to the Financial Policy Committee's recommendation to test and improve resilience to cyber-attack.

The new framework called CBEST uses intelligence from Government and accredited commercial providers to identify potential attackers to a particular financial institution. It then replicates the techniques these potential attackers use in order to test the extent to which they may be successful in penetrating the defences of the institution. On completion of the test there will be workshops for the firm to work through the results with the testers and supervisors.

CBEST provides the following:

- access to considered and consistent cyber threat intelligence, ethically and legally sourced from organisations that have been assessed against rigorous standards;
- access to knowledgeable, skilled and competent cyber threat intelligence analysts who have a detailed understanding of the financial services sector;
- realistic penetration tests that replicate sophisticated, current attacks based on current and targeted cyber threat intelligence;
- standard key performance indicators that can be used to assess the maturity of the organisation's ability to detect and respond to cyber-attacks; and
- access to benchmark information that can be used to assess other parts of the financial services industry.

The combination of these will allow a firm to understand where they are vulnerable. They will then be better prepared to implement remediation plans. The inclusion of specific cyber threat intelligence will ensure that the tests replicate, as closely as possible, the evolving threat landscape and therefore will remain relevant.

CBEST differs from other security testing currently undertaken by the financial services sector because it uses real threat intelligence and focuses on the more sophisticated and persistent attacks on critical systems and essential services. The implementation of CBEST will help the boards of financial firms, infrastructure providers and regulators to improve their

understanding of the types of cyber-attack that could undermine financial stability in the UK, the extent to which the UK financial sector is vulnerable to those attacks and how effective the detection and recovery processes are.

In his speech, Andrew Gracie said: “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 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.”

The Bank of England has worked with the Council for Registered Ethical Security Testers (CREST), a not-for-profit organisation that represents the technical information security industry and Digital Shadows, a cyber-intelligence company, to develop new accreditation standards. This is the first time that commercial cyber intelligence providers will be subject to accreditation standards which are bound by enforceable codes of conduct and supported by a range of CBEST documents on security testing and cyber threat intelligence.