CFTC BRIEFING 2 JUNE 2015

CYBERSECURITY

CONSIDERING BANK OF ENGLAND'S CBEST PROGRAM

BANK OF ENGLAND

Objectives

- Provide an overview of the CBEST program
- Overview will include answers to the following questions:
  - What types of financial institutions are participating in the CBEST program?
  - How was the program developed? And how is it maintained?
  - What is the scope of testing?
  - How does CBEST accommodate the evolution of threats and changing technology landscape? How does the program remain up-to-date?
  - What are the lessons learned from the experience so far?

- Facilitated Q&A with an aim of understanding:
  - What some of the costs / benefits of having a similar program would be for CFTC registrants?

BANK OF ENGLAND

CBEST

Origins of CBEST

- Financial Policy Committee, June 2013

  "HM Treasury, working with the relevant government agencies, the PRA, the Bank's financial market infrastructure supervisors and the FCA 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. "

- September 2013

  "…ensure that the various institutions at the core of the financial system, including banks and infrastructure providers, had a high level of protection against cyber attacks to ensure such attacks do not undermine the system."

- A review of testing practices revealed that the variation in activities (scope, methods, goals, frequency etc) was large.
- The testing provided no insight to capability against likely attack methods.
- As a result the Bank was unable to assess adequacy of cyber security capabilities.
- Therefore could not, at the time, provide assurance that the 'core' of the UK financial system had [or knew what it needed to do to achieve] a *"high level of protection"*.

BANK OF ENGLAND

CBEST

Building CBEST

- The Bank of England set about building a repeatable and scalable vulnerability testing framework

Principles

- Each test should include the same steps, no matter which organisation is to be tested
  - Tests should be holistic in nature, ensuring that people, processes and technology are tested
- The content of each step should be bespoke to each organisation being tested
- Intelligence (commercial and government) should influence the behaviours of the testers
- The tests should provide an accurate understanding of the threats faced by each institution (and therefore the core as a collective)

BANK OF ENGLAND

CBEST

Building CBEST (2)

Principles continued

- The tests would be conducted in partnership with the regulator
- They would benefit from GCHQ input
- The resource commitment on the regulators and the involvement of GCHQ would limit participation to the 'core' only
- Participation was not to be mandatory (at the time we felt this would undermine the partnership principle)
- The tests should provide an assessment of where each firm's current capability is vs where it needs to be

Building CBEST (3)

- The test framework was piloted on the Bank of England
- A small industry working group was established to take development from pilot phase to launch
- Working group included banks and infrastructures, penetration testers, threat intelligence providers, regulators and agencies
- New accreditation standards, including examinations, for penetration testers and threat intelligence providers were created.
  - They are maintained by the Council of Registered Ethical Security Testers on behalf of the Bank of England

BANK OF ENGLAND

CBEST

Accreditation

- To carry out CBEST tests, penetration testing and threat intelligence companies must demonstrate to the Bank of England, via written application process, the following:
  - CREST membership (evaluation of company operating procedures and standards; personnel security and development; approach to testing; data security)
  - Personnel qualified to the right levels
  - Personnel have the required minimum experience
  - Verifiable references

BANK OF ENGLAND

CBEST

Accreditation (2)

- The Bank of England conducts a site visit (penetration testing and threat intelligence companies)
- Interviews company staff, clairifies any anomalies in the application process
- Issues recommendation:
  - Be accredited
  - Be accredited subject to certain requirements being met
  - Application rejected
- The Bank of England reserves the right to revoke accreditation

BANK OF ENGLAND

CBEST

Maintenance of CBEST

- The Bank of England maintains CBEST
- Liaises with supervisory functions to ensure relevance
- Consults with penetration testers, threat intelligence providers and industry on effectiveness – seeks feedback
- Close liaison with CREST
- Promotion of CBEST via industry events; international liaison etc
- Updates webpage periodically

BANK OF ENGLAND

CBEST

Testing

- Threat intelligence identifies threat actors and tactics, techniques and procedures for the test
  - This ensures that no matter which organisation is being tested, or when, the test is based on current threat intelligence
- The scope is agreed by regulators and the financial institution
  - Functions which if disrupted could have an adverse effect on UK financial stability
  - Technology systems supporting those functions are identified – 'target systems' (no-go areas, de-scoping is kept to an absolute minimum)
- Goals are pre-determined
- Penetration testers and financial institution devise a robust control framework
- Financial institution controls the test on a day-to-day basis

BANK OF ENGLAND

CBEST

Post-test activity

- KPIs on both process, and outcome captured
- Workshop to discuss testing activity conducted
- A remediation plan is agreed by regulators and financial institution
  - The plan looks to address gaps identified in where they are vs where they need to be
- Progress against agreed actions is monitored via routine engagement
- Re-test may be part of the remediation plan

BANK OF ENGLAND

CBEST

Lessons to date

- CBEST attracted considerable media attention
- Each test takes approximately 6 months from start to finish
- Procurement process can be drawn out (especially with threat intelligence providers)
- Outsourcing majority of accreditation work greatly reduces the burden on the Bank of England
- Working with industry to finalise the test helped achieve buy-in within industry
- Nervousness within industry remains at some levels
  - As more undergo CBEST testing we expect this nervousness to dissipate
- Raises unanswered questions on next steps for those firms not considered ‘core’

BANK OF ENGLAND

CBEST

QUESTIONS

Dave Evans, Senior Manager
Sector Cyber, Bank of England
david.evans@bankofengland.co.uk
http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx

BANK OF ENGLAND