Bank of England

FCA FINANCIAL CONDUCT AUTHORITY

Prudential Regulation Authority

Please note: This letter has been prepared for the website. Square brackets show where this letter may differ slightly, along with formatting from those versions sent directly to firms

Sent by the supervisory teams of the Bank, PRA, and FCA

[Dear Senior Management Function (SMF) with responsibility for cyber]

31 January 2023

2022 CBEST thematic findings

We are writing to you to share the thematic findings from the latest annual cycle of CBEST assessments conducted by the Bank of England, Prudential Regulation Authority, and Financial Conduct Authority (collectively, 'the regulators') on participating banks, insurers, asset and investment managers and Financial Market Infrastructure.

About the CBEST programme

CBEST is a framework for intelligence-led penetration testing which focuses on an organisation's security controls and capabilities when faced with a simulated cyber-attack. The simulated attacks used in testing are tailored to the threat and vulnerability profile of each organisation and represent an evidence-based and robust testing approach.[1]

[1] The CBEST Implementation guide provides guidance to firms participating in the CBEST programme: **https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf**.

Key findings

We analysed the outcomes of CBEST assessments and identified trends and findings descriptive of the sector's current cyber-posture.[2] These themes are based on over 350 findings from intelligence-led penetration tests conducted on 14 firms during this cycle of testing and are presented together with examples of the most common control weaknesses within those areas.

The purpose of making these findings available to you as SMF[3] with responsibility for cyber is three-fold:

(i) to ensure that your firm can benefit from the identified weaknesses and thereby address potential similar weakness in your firm;

(ii) to raise awareness in your senior executive team; and

(iii) to inform the work of your risk and internal audit functions.

The regulators may use these findings to structure future supervisory interaction and understand the level of engagement firms have achieved with the senior executive team, risk, and audit functions on the issues identified as in need of remediation. For firms that have participated in the latest CBEST cycle, the remediation plans that have been agreed with supervisors will remain the primary focus for addressing their cyber resilience issues. The thematic feedback included here may provide additional information that can be incorporated in these plans.

The thematic process

The regulators and the National Cyber Security Centre (NCSC) have worked together to produce these findings. To provide more details for technical audiences, we mapped each of the themes to the National Institute of Standards and Technology (NIST) framework.[4] We have also provided links to the relevant NCSC guidance for these topics and other NCSC cyber resources. These links represent recommended technical guidelines but are not intended to set new regulatory requirements.

---

2 The National Institute of Standards and Technology defines 'cyber posture' as the security status of an enterprise's networks, information, and systems based on information security resources (eg, people, hardware, software, policies) and capabilities in place to manage the defence of the enterprise and to react as the situation changes.

3 Financial Market Infrastructures (FMIs) are not subject to the SM&CR regime and should therefore interpret SMF as relating to an equivalent individual who is the most senior person responsible for managing the IT security posture of the FMI.

4 Available at: **https://www.nist.gov/cyberframework**.

The regulators continue to engage with firms, international regulators, and government agencies to develop CBEST and to ensure that, where possible, our approaches are aligned. We would welcome any feedback or comments on these thematic findings to **CBEST@bankofengland.co.uk**.

Yours faithfully

[Signature]

Sent by the supervisory teams of the Bank, PRA, and FCA