2024 CBEST thematic

The annual CBEST thematic is intended to inform the sector on the findings and lessons learned from our CBEST programme, which assesses the cyber resilience of key financial institutions through security testing performed in 'live' corporate environments.

The importance of cyber resilience

Overview of the CBEST process

Observations from threat intelligence

Themes from testing

Content

Foreword

This year marks the 10th anniversary of the CBEST programme. CBEST is a threat-led penetration testing assessment framework, that enables firms and Financial Market Infrastructures (FMIs) to identify, understand and remediate vulnerabilities in their cyber resilience.

The Bank of England, Prudential Regulation Authority, and Financial Conduct Authority view CBEST as playing an important role in ensuring the cyber resilience of systemically important firms/FMIs and by extension, the wider financial system.

The intention of this publication is to make the lessons learned through our CBEST programme widely available to benefit the entire UK financial sector.

Each year, the UK financial regulators provide their thematic analysis of recent CBEST findings so that firms and FMIs can better assess their cyber risks and ensure they have adequate resilience capabilities to prepare for, and respond to, cyber incidents that could cause operational disruption and impact financial stability.

This year our findings continue to highlight gaps in firms/FMIs foundational cyber defences.

Areas for firms/FMIs to focus on are:

- cyber security risks to assets and individuals;
- cyber risk management and impact-based approaches to the protection of key resources (people, process, technology, and data);
- detection and response capabilities leveraging the latest threat intelligence; and
- cyber incident response to eradicate threats and mitigate impacts.

Findings from the Threat Intelligence Maturity Assessment (TIMA), part of CBEST, showed that firms and FMIs displayed weaknesses in their threat intelligence operations. This was particularly around the integration of threat Intelligence with business lines and increasing the situational awareness in firms and FMIs.

With the cyber threat landscape constantly evolving, the regulators strongly encourage firms and FMIs to consider where the findings can support their implementation of foundational cyber practices and strengthen their cyber resilience capabilities.

To further enhance the sector's cyber resilience capabilities, the regulators intend to start consulting in the second half of 2025 on expectations around the management of Information and Communication Technology (ICT) and cyber resilience risks. This includes risks arising from IT transformations, and the sector's ability to detect, withstand and recover from disruptions in the event of ICT and cyber incidents. This strategic work will help the sector achieve higher standards of operational and cyber resilience.

CBEST will continue to emphasise the importance of strong cyber foundations and threat-led penetration testing will remain a core element of the regulator's supervisory approach.

Andrew Nye Head of Sector Resilience Division, Prudential Regulation Authority	**Suman Ziaullah** Head of Technology, Resilience and Cyber, Financial Conduct Authority	**Amar Radia** Head of Division, FMID, FMI Analytics, Bank of England

Objectives of publishing this CBEST thematic

> **This publication will be useful across your firm including to the Chief Information Security Officer, Chief Information Officer, Chief Operations Officer, Chief Risk Officer, as well as to cyber specialists and SMF24, SMF4 and SMF5.**

We encourage you to use these findings to:

1. consider the observations as well as the identified weaknesses and identify and address similar weaknesses in your organisation;
2. raise awareness in relation to your own cyber resilience in your board and senior executive team;
3. inform the work of your risk management and internal audit functions; and
4. for firms/FMIs that have participated in the latest cycle of CBEST to ensure transparency and accountability and timely reporting of any ongoing remedial actions to the regulators.

Overview of CBEST and this thematic

- Cyber and operational resilience is one of the top priorities for the regulators. Operational resilience is the ability of firms, FMIs and the financial sector to prevent, adapt and respond to, and recover and learn from operational disruption. Ensuring the UK financial sector is operationally resilient is important for consumers, firms, and financial markets. An operationally resilient financial system is one that contributes to making sure the UK is an attractive, safe place to do business and enhances its competitiveness.
- CBEST uses threat-led penetration testing (TLPT): an approach that mimics the actions of cyber attackers intent on causing disruption to the people, processes and technologies supporting a firm's/FMI's important business services (IBSs). To ensure that testing is as accurate as possible, CBEST is performed on the live production systems of systemic financial institutions to assess their detection and response capabilities.
- Internationally, there is an increased use of regulatory-led TLPT to inform the cyber resilience of regulated entities based on the G7 Fundamental Elements for TLPT. This also supports TLPT at cross-border level with participation and technical alignment between the UK regulators and counterparts to assess cyber as a global risk for the financial sector.
- In this thematic the regulators have analysed the findings from the latest cycle of their CBEST assessments on participating banks, insurers, asset and investment managers, and FMIs. These findings are closely aligned to the National Institute of Standards and Technology cyber security framework. Where we refer in this publication to findings in relation to firms/FMIs we are referring to the specific firms/FMIs that took part in the latest cycle.
- This thematic involved the regulators analysis of several key components of the CBEST TLPT assessments, including:

    1. The results of penetration testing, as prevention activities. These include controls to anticipate cyber-attacks, reduce their likelihood and minimise their impact when they happen.
    2. The results of detection and response assessments. These include controls required to identify active threats and initiate cyber response capabilities to stop cyber-attack.
    3. The results of TIMA. These can be helpful for firms/FMIs in developing or maturing a threat intelligence function.

- This thematic is the result of collaboration between the regulators and the National Cyber Security Centre (NCSC), the UK's national technical authority for cyber security.
- This thematic includes commentary relating to the key thematic findings, as well as links to

recommended technical guidelines by the NCSC. Neither our commentaries nor the links included are intended to set new regulatory expectations.

- This year’s thematic findings again highlight the critical importance of implementing good cyber hygiene practices, as well as having controls and capabilities to detect and analyse adverse events that might indicate a cyber attack.
- The regulators continue to engage with firms/FMIs, international regulators, and government agencies to enhance CBEST. We welcome any feedback or comments on these thematic findings. Please send them to ✉ **CBEST@bankofengland.co.uk** and ✉ **CBEST@fca.org.uk**.

Thematic findings from testing

Prevention

Identity management and access control

In this CBEST thematic, the regulators identified four areas where inadequate identity management and access controls were most common. These weaknesses increase the risk of unauthorised access to critical systems and sensitive data:

- **Having overly permissive access controls** – including having inadequate role-based access controls and a lack of restrictions on administrator accounts.
- **Not maintaining strong credential hygiene practices** – including having weak passwords, storing passwords insecurely in plain text and allowing inadequate or inconsistent password policies.
- **Not enforcing multi-factor authentication (MFA)** – including having administrative logins without MFA and having only single factor authentication to critical systems.
- **Having weak controls around privileged access management** – including allowing the shared use of privileged accounts and the insecure storage of credentials.

This CBEST thematic suggests that weak, and absent identity management and access controls expose firms/FMIs to techniques such as privilege misuse, credential theft and social engineering. The regulators consider identity and access management to be a fundamental element of cyber hygiene.

Infrastructure security, asset management and application maintenance

The results of the regulators' CBEST assessments suggest that insecure configurations and vulnerabilities, that have not been patched in a timely manner, could be exploitable by threat actors. Such practices included:

- **Having weak configuration management practices** – resulting in inconsistent system hardening and unpatched and vulnerable systems.

This CBEST thematic suggests that having effective configuration practices and ensuring the timely application of patches as essential practices, minimised organisations' attack surfaces and maintained overall security of firms'/FMIs' infrastructure. The regulators consider robust asset management capabilities, including the identification and mapping of the ICT environments, helped with better patching and vulnerability management.

Network security

The regulators identified several areas where weak or improperly configured defences, such as firewalls, could facilitate the access of malicious actors to systems:

- **Having ineffective network and service** segmentation – including having a lack of network segmentation such as insufficient administrative account tiering, overly 'flat' networks, and a lack of segregation between development and production environments.
- **Having ineffective network monitoring** – including having ineffective traffic inspection enables attackers to hide their malicious activities in seemingly legitimate traffic or enable outbound connectivity from unmonitored devices.

The results underscore the importance of adopting strong cyber hygiene in regularly reviewing and updating protective and detective network security controls.

Staff awareness and training

The results suggests that without regular training, employees may fail to recognise and report potential security incidents, mishandle sensitive information, or fall victim to social engineering attacks such as phishing. Commonly identified weaknesses included:

- **Staff being manipulatable by social engineering that seeks to discover passwords or token codes** – often enabled by the over-exposure of sensitive data e.g. in job descriptions on social media platforms.
- **Staff being manipulated by phishing** – because of the ubiquity of email and employees' susceptibility to phishing messages.

- **Having unprotected credentials or exposed credentials** – including the presence of unprotected credentials on internal fileshares and external platforms.

These results underscore the importance of firms/FMIs embedding a positive cyber security culture as a key cyber security practice.

Detection and response

The regulators identified where firms'/FMIs' failure to detect cyber attacks in the early stages, and to manage incidents effectively, may increase the impact of operational disruption. Insufficient detection and response capabilities, including the capability to analyse events and near misses may also hinder firms'/FMIs' ability to understand the root cause of incidents and learn from them. Commonly identified weaknesses included:

- **Insufficient detection of adverse events and monitoring gaps** – including having a lack of sufficiently tuned endpoint detection and response, and a lack of detection of data exfiltration.
- **A lack of communication channels during incident responses** – this can give attackers with a foothold in the network the ability to view the coordination of incident response and containment activity.
- **Insufficient containment of red team testers during post-detection containment efforts** – once malicious activity had been detected there was a lack of capabilities to contain the activity.

The results underscore the importance of firms/FMIs practising and refining both detection and incident management capabilities.

Threat intelligence in CBEST

The regulators identified that firms/FMIs demonstrated a range of maturities across cyber threat intelligence management domains. Through the use of the CREST Cyber Threat Intelligence Maturity Assessment Tool[1] we observed how effective threat intelligence can improve a firm's/FMI's understanding of the specific threat environment that they operate within. Our observations about threat intelligence could be helpful for firms/FMIs considering their own threat-led testing programmes.

CBEST requires penetration testers to simulate threat actors as identified by cyber threat intelligence experts. Threat actors simulated included highly capable state actors, organised criminal groups as well as insider threats. Simulations of threat actors seeking to cause disruption and/or make financial gains were the most commonly used.

The regulators identified the following key findings:

- **Firms/FMIs had relatively effective foundations behind their cyber threat intelligence operating models**, with higher maturity scores around their governance and resilience. This could positively benefit the management and repeatability of cyber threat intelligence.
- **Threat intelligence was not well integrated within firms/FMIs**, with lowest scores for the programme planning and requirements, and operations for cyber threat intelligence **such as the approach to staff and management of resources in a CTI function, and the end-to-end intelligence lifecycle.** This could negatively impact the effective production and dissemination of threat intelligence deliverables.

The results of this CBEST thematic underscore how:

'Strong situational awareness, acquired through an effective cyber threat intelligence process can make a significant difference in the firm's/FMI's ability to pre-empt cyber events or respond rapidly and effectively to them. Specifically, a keen appreciation of the threat landscape can help a firm/FMI better understand the vulnerabilities in its critical business functions and facilitate the adoption of appropriate risk mitigation strategies'.[2]

These observations are not intended, and should not be interpreted, as a substitute for a firm's/FMI's own internal intelligence activities and should not be used as an articulation of the entire threat landscape.

NCSC perspectives on CBEST themes

The NCSC has provided the regulators with the following observations on the CBEST themes, based on its expertise and best practice. Neither the commentaries nor the links included are intended to set new regulatory expectations.

Identity management and access control

Identity management is necessary to ensure that activities on a network are attributable to known users or systems. Organisations need to understand, document, and manage access to networks and information systems. This should include ensuring users that can access data or services are appropriately verified, authenticated, and authorised. Activities to support this area include policy development, establishment of identity, architectural design, monitoring, and privileged access management. Privileged access management requires additional separation, authentication, monitoring, and controls to prevent or detect unauthorised activity from privileged accounts.

Infrastructure security – asset management and application maintenance

As organisations develop, the number and variety of assets in their environment tends to grow, increasing the likelihood of legacy, unmanaged, or otherwise vulnerable assets being overlooked. As such, it is important to establish effective asset management processes as early as possible. To accomplish this, organisations need to identify, document, and manage all business assets (including hardware, software, systems, services, data, and staff) in accordance with their importance to business needs. This lowers the risk of legacy and unmanaged systems and enables more accurate risk assessments, reducing exposure to unidentified risks. Management of the hardware, software, and services of both physical and virtual platforms should be conducted in accordance with an organisation's predefined risk strategy. This includes maintenance of hardware and software platforms, controls to prevent installation or execution of unauthorised software, and replacing or removing platforms once at end of life.

Network security

Network security controls are fundamental to preventing malicious access to systems. To improve their network security, organisations should focus on documenting and reducing their attack surface to lower the likelihood of compromise and segregating their networks, by separating critical network services systems from public facing services, to limit the impact of an incident. Organisations should also avoid common security architecture 'anti-patterns', ineffective or even counterproductive patterns often seen in system designs, which variously increase the risk to systems or entail significant cost for zero benefit.

Staff awareness and training

Staff awareness and training is crucial to building operational resilience and ensuring policies and procedures are followed. Developing a positive security culture (i.e. a culture in which employees see security as a shared responsibility that supports their day-to-day work), encourages employees to be open about security issues and reduces the use of shadow IT services. To support a positive security culture, organisations should clearly communicate cyber policies and instate a cyber security training programme. An incident reporting tool can also be a useful way to allow employees to raise concerns, saving time and money.

Proactive monitoring, detection and response

Continuous monitoring enables compromise detection and reduces the impact of compromise. Organisations need to monitor the security status of the networks, services, and systems supporting their essential functions, detect potential security events, and track ongoing effectiveness of protective security measures. They should also monitor personnel and external service provider activity for adverse events.

Adverse event analysis is the investigation of anomalies, indicators of compromise, and other potentially adverse events to detect cyber security incidents or better characterise false positives. Organisations need to draw information from multiple sources, including contextual information and cyber threat intelligence, and compare this against previously defined criteria to identify whether incident management processes should be invoked.

Useful links to themes

Theme	Relevant NCSC links
Identity management, authentication and access control	• Introduction to identity and access management • Multi-factor authentication for your corporate online services • Security architecture anti-patterns: 'Browse-up' for administration
Identity management and access control	• Introduction to identity and access management • Multi-factor authentication for your corporate online services
Infrastructure security	• Asset management • Architecture and configuration • Anti-pattern 6: The un-patchable system
Network security	• Security architecture anti-patterns • Preventing lateral movement
Staff awareness and training	• Engagement and training • NCSC's cyber security training for staff now available
Proactive monitoring	• Logging and monitoring • Log sources
Incident management, analysis and response	• Incident management • Detection practices: Triage as an Objective • Cyber incident response processes: Playbooks and regulatory issues • Cyber incident response processes: Incident Triage

Theme	Relevant NCSC links
Threat modelling	• **Understanding the cyber security threat** • **Threat modelling**

Additional NCSC cyber security resources

- Consider using the **Cyber Assessment Framework (CAF)** to achieve and demonstrate cyber resilience. The CAF is a tool developed by the NCSC to assist organisations in managing the risks posed to their essential functions while remaining compatible with existing guidance and standards.
- Register for the NCSC's **Early Warning Service**. This free service helps organisations investigate cyber attacks by notifying them of malicious activity that has been detected in information feeds. **If already registered, use the Early Warning Portal to view and make changes to registered assets and contact details**.
- Register for **CISP**. CISP is a joint industry and government digital service to allow UK organisations to share cyber threat information in a secure and confidential environment.
- **Ensure that your organisation knows how to report a cyber security incident**.
- Find general and specific **guidance on the NCSC website**, to help improve the cyber security of your organisation. Recent publications include:
    1. **Multi-factor authentication for your corporate online services**
    2. **Business email compromise: defending your organisation**
    3. **Principles for security of machine learning**
- **Attend CYBERUK, the UK government's flagship cyber security event**.

[1] **Cyber Threat Intelligence Maturity Assessment Tools**.

[2] **FR07/2016 Guidance on cyber resilience for financial market infrastructures**.

©2025 Bank of England