NETTITUDE

e-book

CBEST Demystified

Security author Paul Fisher and cyber security consultancy Nettitude present an in-depth look at CBEST testing for the financial services sector

CBEST

www.nettitude.co.uk

THE UNITED KINGDOM CAN BE PROUD OF ITS THRIVING FINANCIAL SERVICES SECTOR.

According to trade organisation The City UK[1], the country is now the world's leading exporter of financial services. The value of the UK's trade surplus in financial services is double that of the next largest country trade surpluses recorded by Switzerland, the US and Luxembourg.

Financial and related professional services contributed £174bn to the UK economy in 2012, representing 12.6% of total economic output. Altogether, more than two million people work in financial and related professional services, with two-thirds employed outside London. Some 20 towns and cities in the UK each have over 10,000 people employed in the sector. And of course London, the jewel in the crown, competes only with New York to be the world's financial centre.

This is all good news. **BUT SUCH SUCCESS IS VULNERABLE TO A GROWING THREAT FROM SOPHISTICATED CYBER CRIMINAL GANGS INTENT ON ATTACKING THE UK FINANCIAL SYSTEM.**

At the same time, technology is rapidly changing the way we use financial services. For their part, UK banks and other financial services have responded well to the opportunities that new technology has brought, with innovative banking apps and rapid online access to loans and other products. Thanks to digitalisation, money has never been more accessible.

However, in 2014 we saw how even major institutions like JP Morgan Chase were vulnerable to highly aggressive and targeted attacks by cyber criminals looking for financial data.

The data that financial institutions hold is growing in size and value exponentially. Smart banks are using the data they collect on customer behaviour to develop and bring to market better services and tailored products. This data is hugely valuable and banks are investing in data specialists to make sense of it all.

The interconnected nature of modern banking means that individual banks no longer have full control of the data and capital flows through their business as access points multiply.

Threat actors are targeting bank customers through e-mail, SMS and phone conversations with a view to gaining access to financial assets.

Attackers have access to sophisticated toolkits and malware that can target customers and bank employees through sophisticated phishing attacks. Once in, attackers can hijack online banking sessions.

Of course, the nature of banking and financial services means security has always been paramount and the sector tends to lead the way in cyber protection.

According to the British Banking Association (BBA) and PricewaterhouseCoopers (PwC)[2], £700M IS SPENT ANNUALLY ON CYBER SECURITY IN THE UK FINANCIAL SECTOR, WHILE 70 PER CENT OF BANKING AND CAPITAL MARKET CEOS IDENTIFY CYBER INSECURITY AS A THREAT TO THEIR GROWTH PROSPECTS.

As a sector, financial services is acutely aware of the risk and willing to invest in cyber defences, perhaps more so than other industries. For many banks, this has meant appointing dedicated risk departments, compliance managers, test managers, CISOs and CROs.

However as proactive as the banks have been, governments and regulators are now looking at co-operative and intelligence led ways that cyber defences can be enhanced within the financial sector.

The Bank of England is taking the lead. It has been at the forefront of the sector, working with a number of cyber security bodies to build stronger cyber assurance practices.

"THE BANK OF ENGLAND'S FINANCIAL POLICY COMMITTEE RECOMMENDS THAT THE RELEVANT AUTHORITIES SHOULD UNDERTAKE WORK TO TEST AND IMPROVE RESILIENCE TO CYBER-ATTACK OF THE FIRMS AT THE HEART OF THE FINANCIAL SYSTEM."

A number of key stakeholders came together to build certification programmes, define risk management frameworks and reporting standards designed to manage cyber related risk within the financial sector.

From this commitment came a new testing framework named CBEST, specifically designed to rigorously test the readiness of financial institutions to withstand sustained cyber attacks. The ethical testing body, CREST and the Bank of England jointly oversee the framework and only a select group of penetration testers are qualified and have been approved to carry out this enhanced testing.

I believe the arrival of CBEST is a significant step forward in giving the UK financial sector the level of security assurance it needs, to maintain its global pre-eminence.

Rowland Johnson
Chief Executive Officer, Nettitude Limited

CONTENTS

CHAPTER ONE

THE SYSTEMIC THREAT TO THE BANKING SYSTEM IN THE UK FROM CYBER ACTORS

Press reports from the past year show that the level of cyber attacks is not only increasing in regularity but also becoming more severe, and the repercussions longer lasting. There have been major attacks on world-renowned names such as Sony, Target and eBay, each one causing long term damage to brand and reputation.

The financial sector also suffered one of the biggest hacks in history. America's largest banking group, JP Morgan Chase, admitted in the final quarter of 2014 that the names, addresses, telephone numbers and emails of 76m households had been compromised by a cyber attack during the summer.

In 2014 highly organised cyber gangs aimed their fire on large US and Japanese corporations attracted by the sheer size of data that these companies hold.

The UK is also a highly attractive target for cybercriminals. According to US security vendor FireEye, around 17 per cent of all advanced persistent attacks (APT)[3] detected in the EMEA area since January 2014 were directed against the UK.

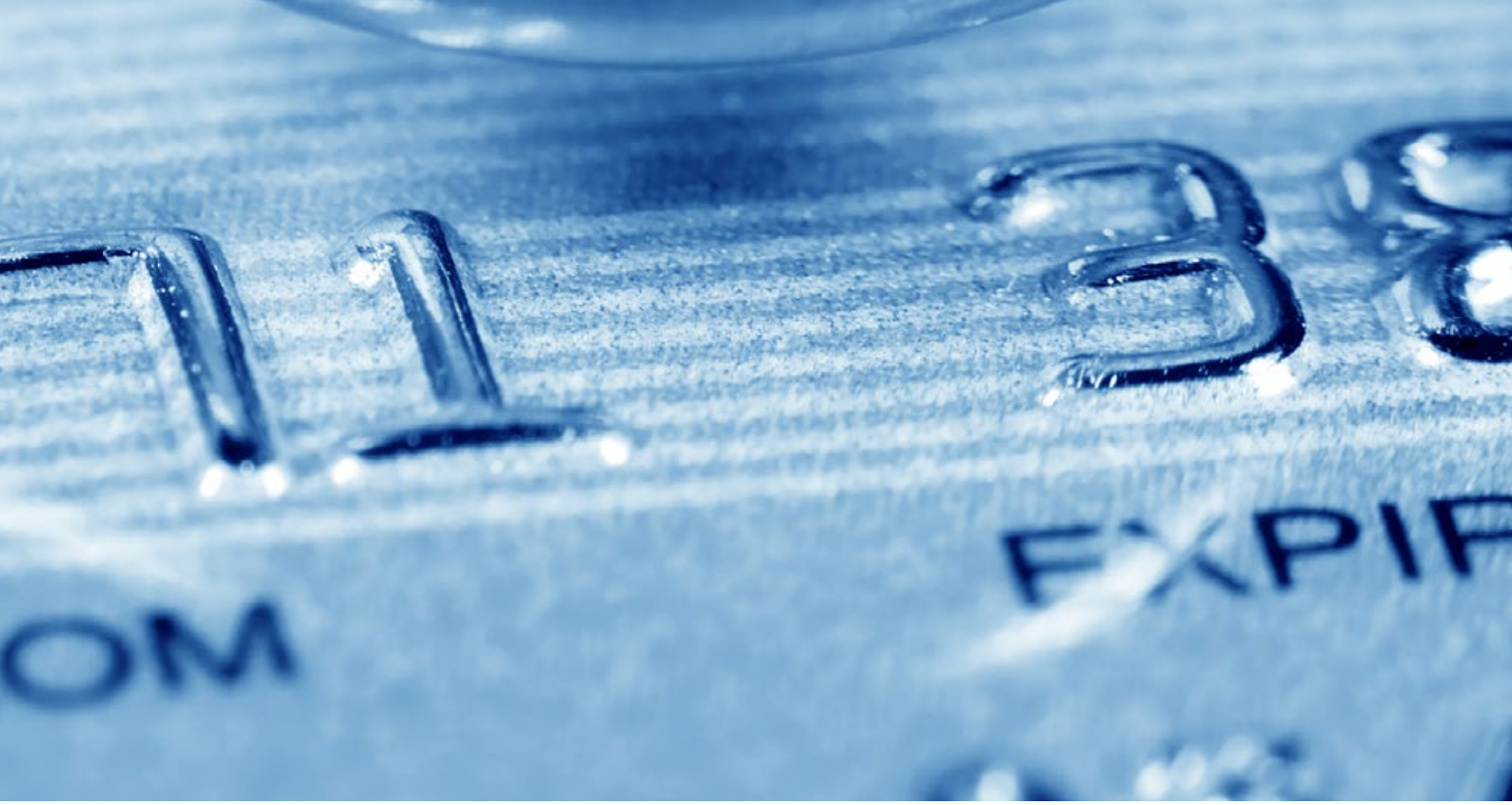
Undoubtedly, part of the UK's attraction to cyber criminals is the presence of its successful and internationally recognised financial services sector, which despite the financial crisis of 2008 still contains some of the world's most valuable financial institutions[4].

In a Daily Telegraph report, Richard Horne, a cyber security partner at PwC said, "Cyber crime has always been a focus for banks but the scale of the threat has increased. The financial system is now more vulnerable because of interconnected networks[5]."

Indeed few businesses can sit behind secured perimeters and conduct all their business there, probably none. The cloud, mobile working and the internet itself have long since transformed commercial activities.

In the banking sector we have seen years of mergers and consolidation bring together different and complex legacy systems, many not as well protected as they should be and some designed for the pre-cyber age.

Payment and transaction systems are also vulnerable. The convenience of online banking is brilliant for customers but brings its own risks. Consumers have for the first time direct access to the banking network and are at risk from phishing and other forms of malware that criminals use to try and access the networks.



IN A REPORT IN THE BANKER, FREDRIK HULT, A CYBER RESILIENCE ADVISOR WITH A CAREER IN BANKING SAID, "CYBER SHOULD BE VIEWED AS AN ON GOING BATTLE BETWEEN THE COMPETING INNOVATION CURVES OF ATTACKERS AND DEFENDERS. THE BAD GUYS ARE INNOVATING VERY QUICKLY, SO BANKS NEED TO INNOVATE QUICKLY AS WELL TO MATCH THE CAPABILITIES OF THOSE LOOKING TO HARM THEM[6]."

It's fair to say then that financial services are at greater risk from the open nature of modern business, simply because they are more interconnected than most. These institutions need full knowledge of what's happening on their active networks. It's not just data they hold but capital.

However the vulnerability points on networks and systems remain hidden. Cyber gangs and hackers are looking to find them, and are constantly probing and pushing to locate them before the banks.

In addition to different legacy networks, there are multiples of security technologies that don't necessarily work together, or even defend against today's sophisticated attack methods such as APT. Banks and other financial institutions are not cyber negligent, instead they arguably face much greater challenges than other industry sectors and are hugely dependent on technology.

In an interview with the Financial Times, Sir David Walker, Chairman of Barclays said, "I don't think I knew what cyber was five years ago. It's a gap. In every area of what Barclays does, technology is a critical, permitting ingredient[7]."

The banks are not then unaware of the threat or the need to test and harden their defences against those who are able to exploit vulnerabilities before the bank itself has found them. The question is therefore, HOW AND WITH WHAT TOOLS WILL DELIVER THE DESIRED LEVEL OF CYBER RESILIENCE?

CHAPTER TWO

A BRIEF HISTORY OF PENETRATION TESTING

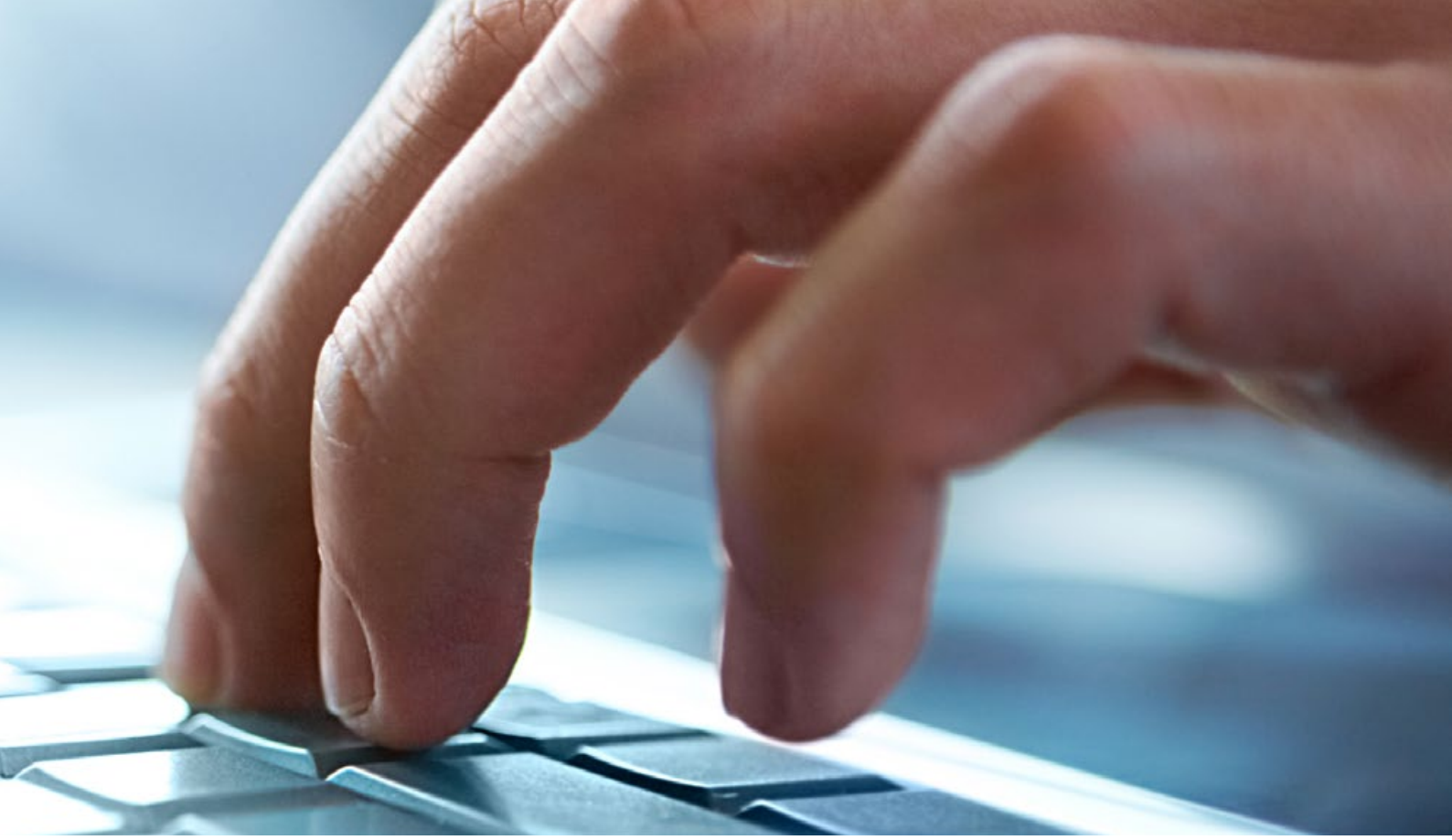
As soon as computers were networked together, concerns over security arose. IT WAS IN THE 1960s THAT NETWORKS BEGAN TO BECOME COMMONPLACE IN THE GOVERNMENT AND MILITARY, AND THE INTERNET WAS DEVELOPED BY THE US MILITARY TO KEEP NETWORKS ONLINE IN THE EVENT OF A NUCLEAR ATTACK.

One of the first commercial networks made its debut in 1964. Using IBM's Sabre (Semi-Automatic Business Research Environment)[8], a reservation system was created for American Airlines.

Using telephone lines, the technology linked 2,000 terminals in 65 US cities to a pair of IBM 7090 computers, delivering data on any flight in less than three seconds. An updated version is still in use around the world today.

According to Wikipedia, one of the first major conferences on computer security was held In June 1965. It states that, "Attendees requested 'studies to be conducted in such areas as breaking security protection in the time-shared system.' In other words, the conference participants initiated one of the first formal requests to use computer penetration as tool for studying system security[9]." And so the concept of ethical penetration testing was born.

At a subsequent conference, delegates were warned that "deliberate attempts to penetrate such computer systems must be anticipated and that on-line communication systems "are vulnerable to threats to privacy," including "deliberate penetration". A representative from the National Security Agency (NSA) declared that network activity "could provide large amounts of information to a penetrating programme." If new then, all three statements apply just as well today.



In the 1970s a simple blueprint for penetration testing was established, as follows.

1 Find an exploitable vulnerability

2 Design an attack around it

3 Test the attack

4 Seize a line of code in use

5 Enter the attack

6 Exploit the entry for information recovery

Simple as it is, this six-point plan captured the essence of a penetration test. But the world has changed fundamentally since the 1960s. Few at those conferences would have anticipated the hugely complex hyper connected world we now live in, still less the demands that businesses and customers now put on those networks.

It was the onset of the World Wide Web and mass adoption of the internet in the 1990s that saw the next development in penetration testing, AS CRIMINALS AND HACKERS HAD OPPORTUNITIES LIKE NEVER BEFORE.

If the penetration tests of the 1960s and 1970s dealt with a fairly predictable set of circumstances, the operating environment is vastly more complex now.

Penetration tests have evolved to meet the requirements of industry sectors, individual businesses and a thriving private sector penetration and vulnerability assessment industry has grown up.

CHAPTER THREE

VULNERABILITY ASSESSMENTS, RED TEAMING AND THE EVOLUTION OF INTELLIGENCE BASED TESTING.

VULNERABILITY ASSESSMENTS

A vulnerability assessment is a related series of checks on the security effectiveness of an organisation. It essentially looks for points of weakness in networks, infrastructure and applications and then produces a report. While useful, the assessment cannot determine whether hostile actors could exploit those vulnerabilities, or how. Nor can they measure the potential level of damage that may occur if this was to happen.

This is not to say that such assessments are not useful, they are, but in today's threat landscape they should be seen as just one part of a mix of testing to accurately assess the critical defence posture of an organisation.

RED TEAMING

Taking its name from military exercises, red teaming is a more focused type of penetration testing, designed to emulate how hackers or cyber criminals may actually enter an organisation.

Such exercises look at the organisation as a whole and include people, processes and technology rather than simply focus on network infrastructure. Some may also include external factors such as supply chain and cloud installations. The best red teams will do as best they can to emulate the most persistent and skilled of hackers. To be successful and to paint an accurate measurement of the organisation's defence posture, red teaming depends on the skills and knowledge of the team involved. It remains virtually impossible to emulate or second-guess the best hackers working in the digital underground.

A COMBINATION OF RED TEAMING, PENETRATION TESTS AND VULNERABILITY ASSESSMENTS CAN GIVE AN ORGANISATION A REASONABLY ACCURATE PICTURE OF HOW IT MAY WITHSTAND A CYBER ATTACK. BUT WE CAN GO FURTHER.

SIMULATED TARGET ATTACK AND RESPONSE

CBEST was created to respond to the need for more accurate and intelligence based testing, to further this, the technical certification and accreditation organisation, built a new framework known as STAR (Simulated Target Attack and Response). This blends red teaming with cyber threat intelligence and incident response assessments. It conducts assessments of both defensive and responsive controls. STAR was created to support the newly established CBEST framework.

The key difference is the use of threat intelligence. STAR assessments use current cyber intelligence focused on the target client, industry, partners and locations of operation.

STAR is also different to conventional red teaming, as it is used to provide assurance around an organisation's detection and response capability.

All traffic, resources and activity generated as part of a STAR assessment is logged and recorded. At the end of the testing programme, an Incident Response Maturity (IRM) assessment takes place.

The IRM assessment will review the client's ability to detect and respond to varying traffic profiles, whilst also identifying their ability to detect multiple types of events that could represent an all out attack on an organisation.

STAR assessments are industry agnostic, and are currently regarded as the most sophisticated type of assurance assessment to measure an organisation's defence, detection and response controls.

Up to date threat intelligence is hugely important to STAR based testing. If an organisation has been targeted by a nation state for example, then the testing would be stealthy and the tools, techniques and practices mimic those of the nation state actors, as far as possible.

CHAPTER FOUR

THE NEED FOR REAL-WORLD TESTING AND THE INTRODUCTION OF CBEST BY THE BANK OF ENGLAND

The financial sector traditionally used a combination of all these assessments but never on live production environments. Testing takes place under emulated environments, the downside of which is that an emulated network can only ever be that, it cannot recreate actual vulnerabilities that may be hidden on the production environment. YOU CANNOT RECREATE WHAT YOU DON'T KNOW.

Cyber criminals will be aggressively looking for exactly those unknown vulnerabilities. There is an urgent need for banks and other financial institutions to test on production environments but can it be done safely?

In early 2014, concerned at the growing threat to UK banking sector and the impact a sustained cyber attack could have on the economy, THE BANK OF ENGLAND LAUNCHED A NEW TESTING ENVIRONMENT IN WHICH BANKS WOULD BE SUBJECT TO MUCH MORE RIGOROUS CYBER STRESS TESTS BASED ON STAR[11]. IT WAS CALLED CBEST, which sounds like an acronym but actually isn't. In October 2014 only a small number of UK companies were considered expert enough to carry out CBEST testing, and authorised by the Bank of England.

Significantly, CBEST has been designed for live testing. Because of this all parties involved in a CBEST project are required to sign up to an agreed risk and control framework. This includes the scope of the test, boundaries, contacts, actions to take and any liabilities including insurance where applicable.

Those businesses approved to carry out CBEST testing had to prove that they possessed suitably qualified personnel, which in real terms means the best testers in the UK. Testing on live systems requires supreme technical ability and competence to discover vulnerabilities without damaging banking operations.

However for extra reassurance, CBEST is delivered in stages and at all times during the testing stages, the financial institution is in control and can request a temporary halt at any point if concerns are raised over damage (or potential damage) to a system.

The CBEST process is a fully developed and documented framework. The process includes standardised reporting formats for providers, and a series of Key Performance Indicators (KPIs) used by the Bank of England to assess the performance of both providers and participants.

CBEST IS INTELLIGENCE-LED. Crucially, it's the only source of testing that funnels intelligence direct from UK Government agencies and supported by commercial intelligence providers. Given that GCHQ and other UK intelligence agencies are considered, along with their US counterparts, as world experts in monitoring cyber activities, this is quite an advantage.

CBEST also adapts to changing threats. The direct feed from UK Government and commercial intelligence means that the threats CBEST mimics remain up-to-date. This is crucial to ensure that CBEST can be used in the long-term.

CHAPTER FOUR

CONTINUED...

SCOPING IN CBEST

One of the early phases in a CBEST engagement involves scoping, a process that is typically conducted in a formal workshop. The scope is discussed and determined by all key stakeholders. During the initial workshop, considerable focus is given to identifying and categorising key systemic assets that have a critical impact on the financial institutions operations. From a security tester's perspective, this is less about the specific device and application descriptions, and more about their function and level of criticality.

The scope of the test is based on the information provided by the threat intelligence provider, combined with the information established during pre-CBEST activities. This may include the most significant and current ways in which the organisation is being targeted or how other similar organisations are being targeted.

The focus includes all aspects of cyber from policy and processes to technology, further to this, understanding data classification policys and the risk register, business continuity and data backup plans. In addition, considerable attention is paid to determining interconnections of systemically important banking functions.

RISK MANAGEMENT IN CBEST

CBEST engagements are designed to identify cyber risks in systemically important financial institutions. As a consequence, this means that the testing has to focus on systemically important devices, applications and interconnections. These types of systems are inherently important, and consequently it is absolutely critical that a robust risk management programme is developed from start to finish of the testing period.

A project risk assessment is completed with input from all stakeholders involved in the CBEST engagement. After measuring all of the quantitative and qualitative information that is collected within the project workshops, the testing organisation will present a formal risk assessment to the client.

CHAPTER FIVE

CBEST FAQS

Who is involved in a CBEST engagement?

CBEST engagements draw stakeholders together from multiple parties. There is representation from the Bank of England, the testing provider, the threat intelligence provider and the end client itself. It is not possible to for a CBEST engagement to be initiated without the presence of all these stakeholders.

Who can conduct CBEST engagements?

CBEST testing can only be delivered by organisations that have a proven track record of working within the financial services sector and approved by the Bank of England. **CBEST TEAMS ARE USUALLY COMPRISED OF CREST CERTIFIED SIMULATED ATTACK MANAGER (CCSAM) AND CERTIFIED SIMULATED ATTACK SPECIALIST (CCSAS) ACCREDITED PERSONNEL.** Having passed extremely stringent CREST approved examinations[12], they represent the highest levels of capability within the UK market today.

How many days do the tests run over?

The number of days when testing will take place depends on each case. Given that CBEST is designed to more closely replicate an attack, the time for the test may be longer than conventional testing. All parties should establish the length of the test and agree on when the test report will be delivered.

How are risks managed throughout the engagement?

Given the nature and importance of the target assets and systems, there will inherently be elements of risk associated with CBEST. Once the test plan has been finalised a further workshop should be established to conduct a risk assessment of the CBEST activities. These activities must be as real as possible but should not disrupt any part of the organisation's critical economic function.

All potential risks should be identified and for each of them risk mitigation must be agreed. It's essential that all those involved in CBEST, both internal and external, are fully aware of the detail of the risk assessment and sign up to the risk mitigation strategy.

How is CBEST funded?

The UK Financial Authorities and CREST have jointly funded the development and implementation of the scheme. This collaboration is seen as an essential part of delivering a scheme that will be acceptable to the financial services industry and can be delivered at a cost that provides real value for money. The financial institutions themselves pay for individual CBEST tests.

CONCLUSION

Since the introduction of CBEST, cyber attacks have continued to make headlines and the high profile attack on Sony, for example, has focused minds on the commercial impact of sustained and aggressive cyber events.

The CBEST programme has seen renewed momentum from the Bank of England and elsewhere. In January 2015 the Financial Times reported that the BBA is planning to launch a Financial Crime Alerts Service, which will share information on the activity of fraudsters, cyber criminals and terrorists, providing another level of much needed intelligence.

Also in January, following high level meetings between the UK and US, it was announced that British and US agents will carry out mock cyber attacks on the Bank of England and commercial banks in London and New York this year, as part of tests on critical infrastructure.

"A REVIEW BY THE BOE INTO HOW RESILIENT 36 OF THE LARGEST UK AND FOREIGN FINANCIAL COMPANIES ARE TO CYBER ATTACKS IS YET TO BE COMPLETED BUT HAS ALREADY HIGHLIGHTED THE RISK OF HACKING BY NATION STATES."
Executive director at the Bank of England (BoE).

The Bank is encouraging more companies to take part in the CBEST programme. The results will be reported to its Financial Policy Committee, which assesses the safety and soundness of the financial system.

RESOURCES

1 http://www.thecityuk.com/research/our-work/reports-list/key-facts-about-the-uk-as-an-international-financial-centre/

2 https://www.bba.org.uk/wp-content/uploads/2014/06/BBAJ2110_Cyber_report_May_2014_WEB.pdf

3 http://www.symantec.com/theme.jsp?themeid=apt-infographic-1

4 https://www.snl.com/InteractiveX/Article.aspx?cdid=A-26316576-11566

5 http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/11170888/Could-your-bank-be-the-next-victim-of-a-cyber-attack.html

6 http://www.thebanker.com/World/Cyber-attack-Is-your-bank-safe (registration required)

7 http://www.ft.com/cms/s/0/e6cf88ac-7fa4-11e4-b4f5-00144feabdc0.html#ixzz3PN6FCoRF

8 http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/sabre/

9 http://en.wikipedia.org/wiki/Penetration_test

10 http://www.crest-approved.org/

11 http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx

12 http://www.crest-approved.org/professional-examinations/index.html

FURTHER READING

- http://www.bankofengland.co.uk/financialstability/fscDocuments/cbestimplementationguide.pdf
- http://www.bankofengland.co.uk/financialstability/fsc/Documents/cbestfaq.pdf

NETTITUDE
excellence as standard





NETTITUDE
excellence as standard

UK Head Office

☎ 44 (0)845-5200-085

cbest@nettitude.com

Alternatively email us at **solutions@nettitude.com**