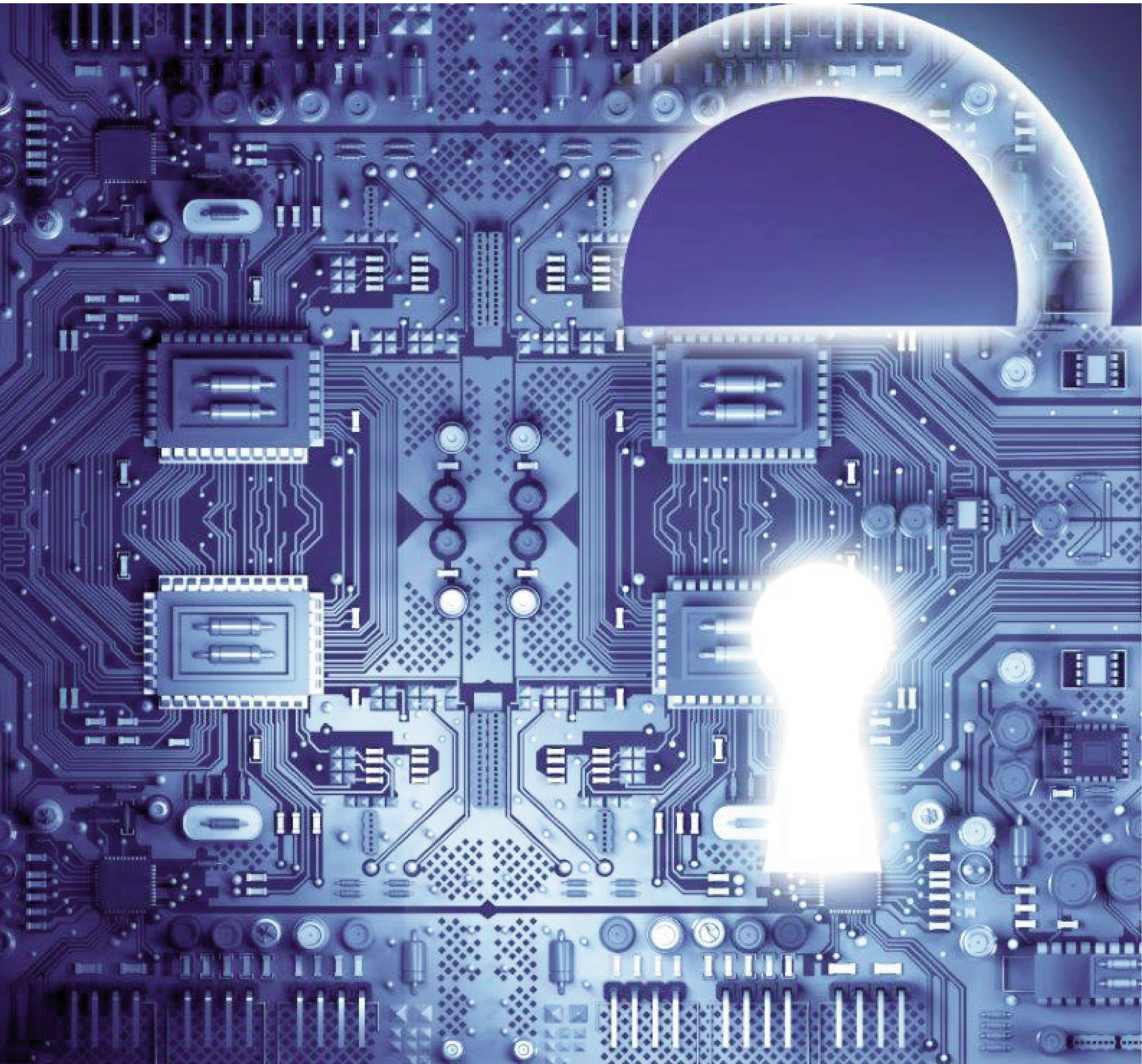
BANK OF ENGLAND

CBEST

# CBEST Intelligence-Led Testing

## CBEST Services Assessment Guide

Version 2.0



# Contents

# Executive summary

Firms participating in a CBEST assessment need to carefully select specialist service providers who can provide an appropriate level of professional support for conducting the assessment.

Given this need, the purpose of this guide is to provide background information, in the form of a set of assessment criteria, that CBEST participants can use as they assess prospective service providers approved by the Council for Registered Ethical Security Testers (CREST). It is divided into two parts covering threat intelligence and penetration testing services respectively.

Further details on the higher-level CBEST process within which this assessment activity takes place can be found in the *CBEST Implementation Guide*.

# 1 Introduction

## 1.1 Purpose of this document

The purpose of this guide is to provide background information, in the form of a set of assessment criteria, that CBEST participants can use as they assess prospective service providers approved by the Council for Registered Ethical Security Testers (CREST). For further details on the higher-level CBEST process within which this assessment activity takes place, please refer to the *CBEST Implementation Guide* (CBEST (2016a)).

## 1.2 Terms of reference

Firms participating in a CBEST assessment need to carefully select specialist service providers who can provide an appropriate level of professional support for conducting the assessment.

Both threat intelligence and penetration testing markets feature a wide variety of vendors with competing claims, which generate a significant amount of hype. This is especially so in the commercial threat intelligence market which is relatively immature compared to the penetration testing market.

As a result, the Bank of England, working in collaboration with CREST, the technical information security quality assurance organisation, has developed new accreditation standards for CBEST threat intelligence and penetration testing service providers (hereafter referred to as 'TI provider' and 'PT provider' respectively. These are based on the already stringent quality standards that CREST member companies have to achieve. Details of CREST-approved service providers can be found at www.crest-approved.org.

## 1.3 Structure of this document

The remainder of this document is structured as follows:

- Section 2, *Threat intelligence services assessment*, presents criteria for assessing the quality of prospective providers of CBEST threat intelligence services;
- Section 3, *Penetration testing services assessment*, presents criteria for assessing the quality of prospective providers of CBEST penetration testing services;
- Section 4, *References*, lists sources of information used in the production of this report.

## 1.4 Information sources

Information for this report was gathered from online open sources and discussions with industry professionals. A full set of references appears at the end of this document. Information was also derived from various CBEST meetings and workshops attended by the representatives of the Bank of England, CREST and the Cyber Working Group during the first quarter of 2014. In 2015 the Bank of England Cyber Sector Team commissioned a review and update of this document during which various stakeholders were canvassed for their input.

## 1.5 Legal disclaimer

The information and opinions expressed in this document are for information purposes only. They are not intended to constitute legal or other professional advice, and should not be relied on or treated as a substitute for specific advice relevant to particular circumstances. The sponsors and authors of this document shall accept no responsibility for any errors, omissions or misleading statements in this document, or for any loss that may arise from reliance on the information and opinions expressed within it.

# 2 Threat intelligence services assessment

## 2.1 Introduction

This section presents criteria for assessing the quality of prospective providers of CBEST threat intelligence services.

In comparison to its counterpart in the government and law enforcement sector, threat intelligence in the commercial environment remains a relatively immature discipline and is also the subject of much vendor hype. As the provision and application of threat intelligence services evolve over time, so too will the opportunities to measure and assess services of this type. Since cyber threat intelligence is an emergent discipline, it is likely that TI providers themselves may benefit from the content of this document.

CBEST defines threat intelligence as '*information that provides relevant and sufficient understanding for mitigating the impact of a potentially harmful event*' (CBEST (2016b)). Intelligence encompasses not only the technical details of the attack (indicators of compromise, or the what, when and where) but also understanding and attributing the TTPs behind the attack (the modus operandi or how) and, critically, the attackers themselves (the who and why).

A variety of organisations offer threat intelligence services, the major providers of such services being:

- specialist providers of more technical, machine-oriented threat intelligence;
- specialist providers of more strategic, human-oriented threat intelligence;
- specialist threat intelligence platforms that integrate disparate threat intelligence feeds (technical and/or strategic).

An important step towards raising professional standards is the development of the CREST Certified Threat Intelligence Manager qualification to supplement threat intelligence standards (CREST (2016a)). This tests candidates' knowledge and expertise in leading a team that specialises in producing threat intelligence. Candidates are expected to have a good breadth of knowledge in all areas of threat intelligence and proven experience in operational security and intelligence production. The exam assesses the candidate's ability to conduct engagements that produce threat intelligence in a realistic, legal and safe manner, ensuring the customer is provided with actionable intelligence that can be used to increase security and reduce corporate risk. As a pre-condition for accreditation onto the CBEST scheme, all approved TI providers are required to have personnel qualified in CCTIM.

Most TI providers generate and manage threat intelligence through a standard life cycle of direction, collection, analysis and dissemination. Some choose to conclude the cycle with a review activity that leads to an adjustment in future direction. The following sub-sections consider the factors that will influence the quality of the intelligence product during each of these key phases and concludes with ethical considerations.

## 2.2 Assessment criteria

### 2.2.1 Direction

During the direction phase, TI providers engage with an organisation to obtain useful context for conducting the threat analysis. Information about the current state of the organisation and its information security stance are particularly useful. Although the organisation may not always be able to share the details of sensitive incidents with the TI provider, it should still be possible to learn about the organisation both through engagement with the key stakeholders and through gathering evidence of previous breaches through public sources.

Useful questions to ask a potential TI provider include:

- does it take into account public data about previous incidents that would be relevant to the threats today?
- does it take into account, and keep confidential, private data about previous incidents that would be relevant to the threats today?
- does it look at the short, medium and longer-term goals of the business that might inform the likely interests of a potentially hostile party?
- does it ask for previous risk assessments or risk modelling exercises?

Using questions of this type as input to the intelligence collection process can be very useful in tuning and scoping the threat intelligence process. This is helpful in both determining whether existing threats are still present and characterising the type of threats that the business has faced.

### 2.2.2 Collection

One of the most important parts of the threat intelligence gathering process is collection. This phase of the process provides the raw materials for conducting intelligence analysis. There are a number of factors in the collection process that can directly influence the quality of the output product.

#### Variety of source types

Most collection functions acquire data from a wide variety of data source types. The extent of this variety is a useful indicator of the range of intelligence that a consumer should expect from a TI provider. These can include both web and Internet services, a mixture of public and private forums and a range of media types such as IRC chats, email and video.

#### Breadth of sources

The number of items in any given source type is again a useful means of measuring the likely catchment capability of any collection function. A TI provider that collects across 100,000 unique domains will be expected to generate fewer results overall compared to one that collects across 30 million. That said, the classic 'garbage in, garbage out' rule applies and this must, of course, be balanced against the ability of the TI provider to select domains that are likely to contain content of interest and the likely rate of false positives emanating from that source.

#### Language support

Languages play an important role in selecting an effective TI provider. Cyber threats are a global phenomena and a TI provider that offers no coverage of, for example, Russian and Mandarin Chinese online threats will miss a significant proportion of relevant information. Therefore TI providers with staff who can demonstrate fluency in key foreign languages will offer a considerable advantage. This includes ensuring that the TI provider's technology can ingest, process and manage content in multiple languages.

#### Depth of sources

TI providers collecting intelligence may touch the surface content of a given source but it is also important to know that all the content of a given source can be incorporated when there is an appropriate, and lawful, opportunity to do so. It is therefore worth asking a TI provider whether they can provide the option to acquire data at scale. By acquiring data at scale in this manner it is possible to query the data after retrieval from its original source. This can be useful when the hypothesis, or question, is sensitive in nature.

#### Timeliness of collection

The timeliness of collection will vary from source to source. TI providers must demonstrate understanding that dynamic, high volume data sources such as Twitter are ingested at such a fast rate that the intelligence is relevant at the very moment it is collected. It is also useful to understand the amount of time over which questions can be asked of the source. For example, having the ability to spot malicious tweets over a previous two-year period is more valuable than a six-month period.

#### Types of intelligence

The threat intelligence market contains TI providers who employ a variety of intelligence gathering disciplines. TI providers that use both OSINT (open source intelligence derived overtly from publicly-available sources) and HUMINT (intelligence derived overtly or covertly from human sources) are better able to gather intelligence relating to covert groups such as organised criminals compared to those who use OSINT only. Services that use TECHINT (technical intelligence derived, for example, from signals generated routinely by hardware devices or software applications) are more likely to gather intelligence suitable for system monitoring purposes but which may not be relevant for the purposes of constructing a valid CBEST assessment.

### 2.2.3 Analysis

At the point that collected data is analysed and enriched it is then available for analysis. The CBEST guide *Understanding Cyber Threat Intelligence Operations* (CBEST (2016b)) describes this process in more detail. It is important to ensure that a TI provider employs a range of techniques to ensure the consistency, accuracy and relevance of the information resulting from this phase of the process. For example:

- they should be able to demonstrate that they have implemented systems to remove conformation bias and other cognitive errors where results are curated by an analyst;
- they should have means of confirming facts from more than one source of information by de-duplicating and collating content into a consistent format;
- they should be able to employ data-driven and hypothesis-driven assessment strategies, ie they should be capable of discovering new intelligence by identifying patterns in the collected data and by validating hypothesis.

### 2.2.4 Dissemination

The CBEST guide *Understanding Cyber Threat Intelligence Operations* (CBEST (2016b)) sets out a range of formats, delivery mechanisms and approaches to disseminating information. Organisations should seek quality from the final delivered intelligence product.

The final intelligence product that is disseminated to the consumer should:

- **provide relevant intelligence:** that is, information that provides relevant and sufficient understanding for mitigating the impact of a potentially harmful event, plus relevant guidance, so that a PT provider can use it to construct a realistic test;
- **be in an appropriate format:** intelligence should be concise, clear and consistent, written in plain English and avoiding the use of jargon wherever possible;
- **offer a mechanism for prioritising and comparing results:** intelligence should be graded according to the severity of the threat and the veracity and urgency of intelligence that has been found.

### 2.2.5 Ethical

Threat intelligence in the cyber domain is an emerging capability. There is therefore significant opportunity for TI providers to innovate and, as a result, a considerable variance in the methods and techniques used to acquire, exploit and disseminate it.

Financial services institutions, as regulated entities, are committed to ensuring that they act in a professional and ethical manner. It is therefore essential that, when employing a TI provider, they maintain existing standards of ethics and rigor that run through their supply chains. While financial institutions will implement procurement guidelines to ensure this as a matter of course, it is nonetheless useful to explore ethical considerations that are specific to the CBEST assessment.

#### The CREST Code of Conduct

CBEST will be provided and regulated by the professional standards body CREST (Certified Register of Ethical Security Testers). CREST has a robust code of conduct that encompasses both member companies within the schemes and also individuals who attain qualifications under the scheme (CREST (2016b)).

Even at the inception of the scheme all CBEST members must agree to comply with the CREST code of conduct and will be assessed against it within six months of joining the scheme. All CREST member companies are required to comply with the code of conduct and there is a process to ensure that members adhere to them.

These codes of conduct will provide financial services organisations evidence that ethical conduct is mandatory for companies supporting CBEST participants. Of particular note in the CREST code of conduct are requirements to ensure:

- **honesty:** with regard to compliance with legal obligations, disclosure of information in reports and discussing sub-contractual relationships;
- **prohibition of bribery, corruption and extortion:** to ensure that both the company, individuals and any subcontractors are free from bribery, corruption and extortion of any kind;

- **fair competition:** that TI providers compete fairly within the marketplace and selection of TI providers happens after a free and fair process.

## The OSIRA Code of Conduct

Just as cyber threat intelligence is an emergent field in information systems security, so too are the professional and ethical standards that surround it. Groups such as the Open Source Intelligence and Research Association (OSIRA) are making some early and encouraging progress. This is an international body dedicated to enhancing the knowledge and expertise of Open Source Intelligence practitioners in both the public and private sector (OSIRA (2016)).

OSIRA is a professional body consisting of both technical and academic industry experts as well as experienced OSINT professionals. Notably, its mission statement outlines a code of conduct by which future members should comply and it has a Professional Standards Board. Whilst the group is still at an early operating stage, and membership is yet to be fully determined, the code of ethics cover some important areas in respect of Open Source Intelligence (OSINT).

Because the professional body managing CBEST will be CREST then the code of conduct and ethics of this group will apply to TI providers. However, it is likely that collaboration with industry groups such as OSIRA will be explored.

According to OSIRA, key considerations when gathering intelligence in an ethical manner are:

- adherence to legislation, in particular the requirements to respect individuals' privacy and comply with communications legislation;
- where the client has any kind of Governmental ownership, ensuring that the requirements of the Regulation of Investigatory Powers Act (RIPA) are observed;
- ensuring the intelligence supply chain is free from torture, abuse and respects the human rights (as defined by United Nations and European legislation) of all those who have participated in it.

The key qualities that OSIRA believes its members should exhibit are as follows:

### *Responsibility*

OSIRA members will never promise more than they can deliver and will be honest about the limits of their professional capability. They will always qualify the veracity of their intelligence with absolute integrity. They will maintain independence of thought, product and organisation and declare immediately any potential conflict of interest to employers and fellow members.

### *Professionalism*

OSIRA members will continuously strive to acquire the professional knowledge and skills required to perform their function, recognising that new tools and techniques are evolving rapidly. They will use accredited, systematic and verifiable processes and act in ways that are at all times accountable, legal and ethical. They will strive continuously to deliver timely, relevant and accurate intelligence.

### *Credibility*

OSIRA members will seek to present the highest standards of objectivity in their assessments, advice and conduct. OSIRA members will at all times safeguard company information and intellectual property, recognising the poacher/gamekeeper risks to a client of open source research.

### *Personal example*

OSIRA members will be role models for employees through their professional ability, approach to life and work ethic. They will display selflessness, honesty and integrity at all times. They will show respect for fellow workers and show leadership and openness in their dealings with employers and clients.

In addition to OSIRA, other industry analysts have commented on the need for an ethical code for intelligence officers, for example (Schneier (2009)).

## Ethical standards in human intelligence (HUMINT)

The OSIRA organisation exists to support intelligence conducted over public information sources. However, cyber intelligence often employs person-to-person interactions in order to obtain information. This additionally has some important considerations. If human intelligence (HUMINT) is included in the intelligence product then the purchasing party will need to be confident that the information that they consume is obtained in an ethical manner.

When information is collected from an interaction between individuals, eg through the posting of a message on a message board, this becomes HUMINT. In a number of cases the participants of a conversation with an intelligence officer may not be aware of the identity of the party with whom they are interacting. It is therefore important to ensure that a TI provider who uses HUMINT in the intelligence gathering process adheres to certain standards, in particular:

- ensuring that information is obtained by ethical means — it is unacceptable to use techniques such as blackmail, entrapment and coercion;
- the exchange of stolen goods or services or the proceeds of crime are unacceptable in any form;
- actions must be avoided that could effect the personal safety, security or risk to life of individuals involved in information exchanges;
- actions must be cognisant of the outcome of the civil liberties of the individuals with whom interaction takes place;
- commercial companies are not law enforcement officers and therefore actions that lead to harm of an individual will be treated in the same way as any other form of harm under criminal law.

If the contracting entity is a government entity then the appropriate legislation concerning the Regulation of Investigatory Powers Act must be followed. A separate consultation and discussion is recommended on this topic.

### Ethical standards in technical intelligence (TECHINT)

The CREST group has already established a mature understanding of the ethical and legal considerations for conducting security tests. These tests typically require a professional security tester to manipulate and probe the technology platforms of a financial services institution. There are a number of legal considerations associated with this, in particular, the legal considerations relating the to Computer Misuse Act, Telecommunications Act and Data Protection Act under UK law.

In gathering information that is relevant to threats through the use and exploitation of technology there are some further areas that require consideration. Criminals commonly exploit computers and infrastructure that is owned and managed by innocent third parties. Criminal operatives and groups will exploit weaknesses in the defences of a computer and take control of the systems resources to carry out a particular activity.

Recently the information security industry has explored the area of 'active defence' where threat intelligence companies may launch a counter-attack against an online actor from a legal jurisdiction where there are no laws that govern online behaviour or from a location where no extradition agreement agrees with the target's location. In the case of a CBEST assessment these types of test have significant and complex legal considerations and for this reason it is recommended that intelligence involving elements of active defence is not included in the material of a TI provider. A discussion of some of these issues is included in (Vihul *et al* (2012)).

Information must be gathered using approaches that respect the United Kingdom's legislative framework. The existing CREST membership requirements will ensure that member companies adhere to these requirements.

## 2.2.6 Collaborative working

Successful CBEST assessments are underpinned by a collaborative, transparent and flexible working approach observed by both TI and PT providers. A TI provider must demonstrate a willingness to work in this way, sharing its deliverables (once approved by the CBEST participant) with its penetration testing counterpart for review and comment.

The TI provider should also demonstrate a willingness to work with the PT service provider during the handover stage when threat scenarios are transformed into a cohesive and tractable Penetration Test Plan.

# 3 Penetration testing services assessment

## 3.1 Introduction

This section presents criteria for assessing the quality of prospective providers of CBEST penetration testing services. More detailed guidance can be found in the CREST guidance document *Penetration Testing Services Procurement Guide v1.0* (CREST (2016c)).

A penetration test involves the use of a variety of manual and automated techniques to simulate an attack on an organisation's information security arrangements — either from malicious outsiders or the organisation's own staff.

Undertaking a series of penetration tests help test an organisation's security arrangements and identify improvements. When carried out and reported properly, a penetration test can reveal nearly all of an organisation's technical security weaknesses and provide it with the information and support required to remove or reduce those vulnerabilities. In CBEST, traditional penetration testing is enhanced — ie made more proactive, realistic and evidence-based — by the input of high quality threat intelligence that has been collected and analysed by a CREST-accredited TI provider and quality-assured by GCHQ.

A variety of organisations offer penetration testing services, the major providers of such services being:

- specialist penetration testing firms — who may have specialist research and testing capabilities;
- information security consultancies and integrators with penetration testing teams — who may have wider links to information security strategy and integration with security management standards;
- systems integrators and outsourcing service providers with penetration testing teams — who may have detailed understanding of an organisation's technical environment and knowledge of attacks on similar outsourced organisations;
- regulated professional services firms, including the 'Big 4' accountancy firms, with penetration testing teams — who may be more heavily regulated with links to wider audit and compliance requirements.

CREST offers CREST Certified Simulated Attack Manager (CCSAM), and CREST Certified Simulated Attack Specialist (CCSAS) qualifications to supplement existing penetration testing standards (CREST (2016d); (CREST (2016e)). As a pre-condition for accreditation onto the CBEST scheme, all approved PT providers are required to have personnel qualified in both CCSAM and CCSAS for Penetration Testing.

## 3.2. Assessment criteria

### 3.2.1 Reputation, history and ethics

Two of the most important criteria for a buyer of penetration testing services to consider are the reputation (and history) of the PT provider and the ethical conduct it both adopts and enforces.

A reputable PT provider will have achieved suitable professional accreditation (such as CREST) and be a member of current, relevant professional and industry bodies.

It will also have processes in place for agreeing scope and obtaining permissions for the type of work to be conducted, where it will take place and what information and systems will be accessed.

Useful questions to ask a potential penetration testing provider include:

- Can you provide evidence of a solid reputation, history and ethics (eg a full trading history, good feedback from both clients and providers a reliable financial record and a strong history of performance)?
- Do you take part in specialised industry events (such as those run by CREST or OWASP chapters)?

- Are you able to demonstrate exploits or vulnerabilities you have found in other similar environments?
- Can you provide independent feedback on the quality of work performed and conduct of staff involved?
- Do you adhere to a formal code of conduct overseen by an independent industry body?

### 3.2.2 Service quality and value-for-money

The penetration testing market is subject to a degree of vendor hype that can be difficult to penetrate. It can therefore be a challenge to find the right quality of service at the right price.

Providers should be able to produce insightful, practical and easy to read reports, engaging with senior management in business terms, resolving issues with IT service providers and addressing global risk management issues.

A quality provider will not only deliver a highly effective testing process but will also differentiate itself by the quality of the customer services it provides, effectively providing a professional services wrapper around the test.

Useful questions to ask a potential penetration testing provider include:

- Can you show that you provide high quality services, including the methodologies, tools, techniques and sources of information you will use as part of the testing process?
- How do you perform rigorous and effective penetration tests to ensure that a wide range of system attacks is simulated?
- Can you describe your proven testing methodology that is tailored for particular types of environment (eg infrastructure, web applications and mobile computing)?
- Can you demonstrate your organisation's penetration testing capabilities (eg by making a presentation, showing examples of similar projects you have undertaken) and providing a sample report?
- Do you have independently-reviewed quality assurance processes that apply to each test being undertaken in order to ensure client requirements are being met in a secure, productive manner?

### 3.2.3 Research and development capability

One of the biggest selling points for some penetration testing providers is the quality and depth of their technical research and development (R&D) capability.

Some providers will constantly develop specific methodologies to address different environments, such as infrastructure, web application, wireless, mobile, etc.

A good, technically-competent provider is likely to carry out about 70% manual testing (essentially simulated hacking) and 30% using automated tools.

Useful questions to ask a potential penetration testing provider include:

- Do you have an active, continuous and relevant research and development capability?
- Have you produced research papers, published vulnerabilities or won awards in the industry?
- Do you perform sufficient research and development to be able to identify all significant vulnerabilities?
- How do you carry out specially tailored, manual tests to help detect unknown vulnerabilities, rather than just using a standard set of tools?

### 3.2.4 Staff competence

Staff employed by a penetration testing provider should have deep, technical capabilities in the specific areas that are relevant to your target environment (eg web application, infrastructure, mobile or vendor-specific).

CREST provides accreditation in different technical areas, such as CREST web application testers and CREST infrastructure testers. There are also specific examinations in areas such as wireless testing.

Useful questions to ask a potential penetration testing provider include:

- What qualifications do your testing staff hold in the various areas in which tests may be required (such as web application testing)?
- How do your testers identify 'root cause' findings, strategically analyse findings in business terms, help develop security improvement strategies and recommend countermeasures to both address vulnerabilities and prevent them recurring?
- Can you specify named individuals who will be responsible for managing and conducting the test, their experience of the environment within the scope, their qualifications and the exact role each individual will perform?

### 3.2.5 Security and risk management

It is important that the penetration testing provider is itself secure and has a positive approach to both security and risk. A competent provider should be able to provide assurances that the security and risks associated with your critical systems and confidential information (together with any other business risks) are being adequately addressed.

During any security assessment it is likely that the test team will encounter sensitive or business-critical data. You will need to be comfortable that you can trust both the provider and every individual tester they provide.

Useful questions to ask a potential penetration testing provider include:

- Do you apply independently-validated security and risk management controls over the testing process, all relevant people involved, key aspects of target systems and any client data affected?
- Can you provide written assurances that the security and risks associated with our critical systems and confidential information (together with any other business risks) will be adequately addressed and compliance requirements met?
- How do you ensure that results of tests are generated, reported, stored, communicated and destroyed in a manner that does not put our organisation at risk?

### 3.2.6 Professional accreditation and complaint process

Penetration testing providers that have been professionally accredited will provide you with confidence that major vulnerabilities have been identified and properly addressed. They will also bring with them a wealth of experience drawn from client work across a range of companies and sectors, allowing lessons learned from one to be transferred to others.

The CREST scheme requires organisations to demonstrate that they have appropriate procedures and controls in place to protect client information and systems.

There can be a big difference between a cheap penetration testing service and one that provides real value for money. For example, many low-cost services may not provide certified, professional staff that can uncover and address significant vulnerabilities or act in an ethical manner according to defined code of conduct. Furthermore, there is typically little recourse in the event of a dispute (eg no independent adjudication and sometimes not even any indemnity insurance).

Useful questions to ask a potential penetration testing provider include:

- Does your organisation hold strong professional accreditation?
- Can you outline the problem reporting and escalation processes that you adopt should there be a problem with the testing?
- Are you supported by a constructive, expert complaint process, with sufficient independence and authority to resolve issues?

### 3.2.7 Collaborative working

Successful CBEST assessments are underpinned by a collaborative, transparent and flexible working approach observed by both threat intelligence and penetration testing service providers. A penetration testing service provider must demonstrate a willingness to work in this way. This includes reviewing and commenting on the intelligence deliverables (once approved by the CBEST participant) as well as transforming threat scenarios into a cohesive and tractable Penetration Test Plan.

# References

**CBEST (2016a)**, 'CBEST Implementation Guide', Bank of England.

**CBEST (2016b)**, 'Understanding Cyber Threat Intelligence Operations', Bank of England.

**CREST (2016a)**, 'CREST Certified Threat Intelligence Manager', available at www.crest-approved.org/professional-qualifications/crest-certified-threat-intelligence-manager/index.html. CREST (GB).

**CREST (2016b)**, 'Code of conduct', available at www.crest-approved.org/crest-member-companies/code-of-conduct/index.html. CREST (GB).

**CREST (2016c)**, 'Penetration Testing Services Procurement Guide v1.0', available at www.crest-approved.org/wp-content/uploads/PenTest-Procurement-Buyers-Guide.pdf. CREST (GB).

**CREST (2016d)**, 'CREST Certified Simulated Attack Manager', available at www.crest-approved.org/professional-qualifications/certified-simulated-attack-manager/index.html. CREST (GB).

**CREST (2016e)**, 'CREST Certified Simulated Attack Specialist', available at www.crest-approved.org/professional-qualifications/certified-simulated-attack-specialist/index.html. CREST (GB).

**OSIRA (2016)**, 'About OSIRA', available at www.osira.net. Open Source Intelligence and Research Association.

**Schneier, B (2009)**, 'An ethical code for intelligence officers', available at www.schneier.com/blog/archives/2009/08/an_ethical_code.html. Schneier on Security.

**Vihul, L, Czosseck, C, Ziolkowski, K, Aasmann, L, Ivanov, I and Bru, S (2012)**, 'Legal implications of countering botnets',available at https://ccdcoe.org/multimedia/legal-implications-countering-botnets.html. NATO Cooperative Cyber Defence Centre of Excellence and the European Network and Information Security Agency (ENISA).