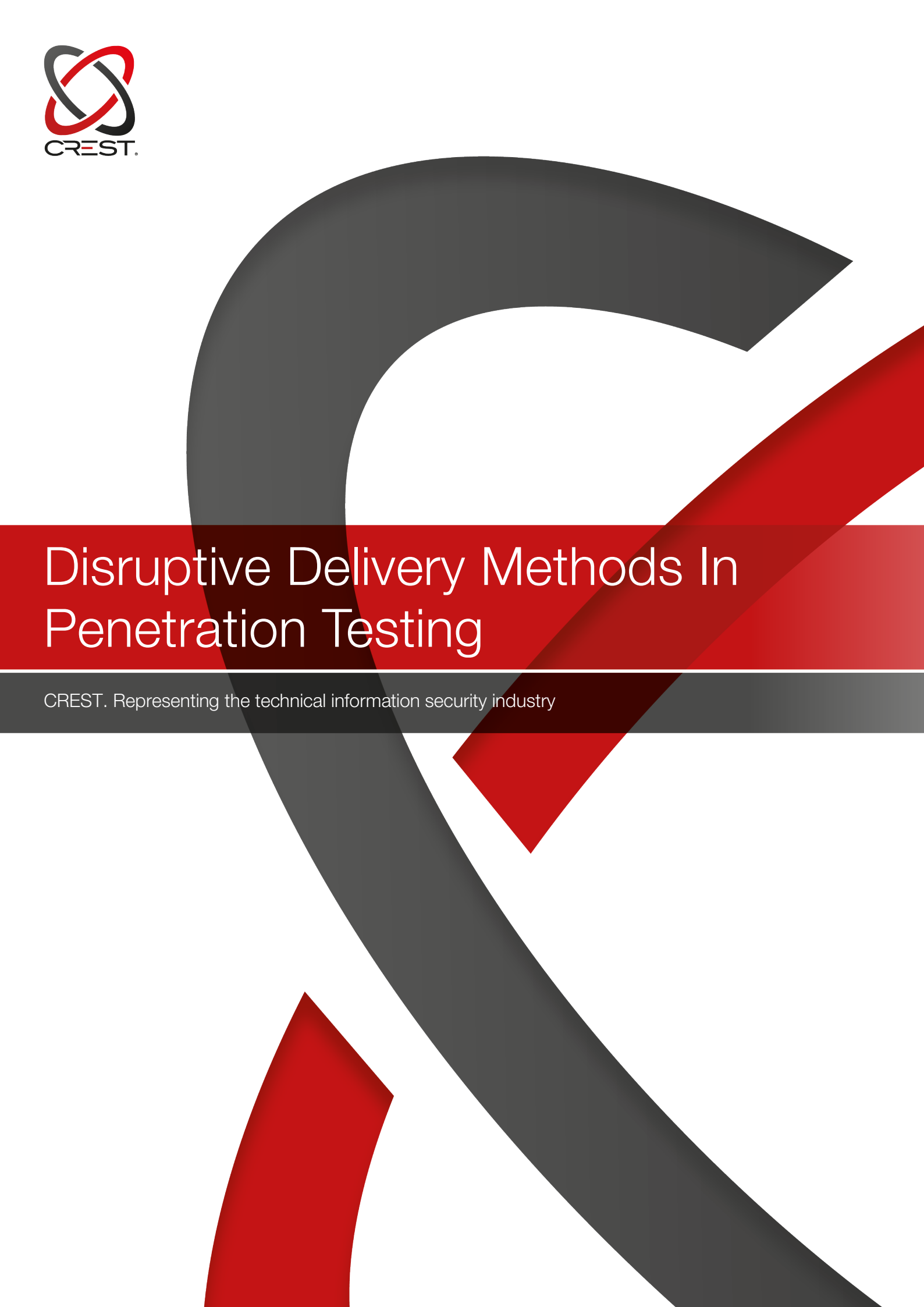

Disruptive Delivery Methods In Penetration Testing

CREST. Representing the technical information security industry

Disruptive Delivery Methods In Penetration Testing

For some time, CREST has been looking into the impact of disruptive delivery methods on penetration testing services. In particular, CREST has been trying to understand the implications these methods have on the buying communities, existing suppliers of services, individuals delivering services and legal and regulatory requirements in a balanced, considered and collaborative way.

Through its international work, CREST has seen disruptive delivery methods and services being developed and deployed. These include advanced vulnerability analysis utilising Artificial Intelligence technology from the UK and Israel; Bug Bounty programmes from the USA and emerging markets such as India; and crowdsourcing penetration testing models for the delivery of penetration testing services from the USA. What has been consistent in the deployment is that buyers of services have not fully considered the implications and that regulators and government have not kept pace with the changes that these disruptive delivery methods could have on the market. It is important that CREST helps to provide the buying community with unbiased advice and guidance and that as a professional industry body we help to formulate policy. The primary aim of CREST is to professionalise the penetration testing industry. As such we must have a view on new delivery methods, where necessary provide support to the development of good practice and support to community. It is not the role of CREST, nor could CREST, stop deployment. Without the support of organisations such as CREST, it is highly likely that concerns, real or perceived, will manifest themselves as a drive for governments to formally legislate the delivery of penetration testing services. This will undoubtably slow innovation, giving further advantage to the attacker. It will almost certainly have unforeseen consequences on existing service suppliers.

CREST, because of its International membership and the relationship it has with the supplier industry, governments and regulators, is uniquely placed to take a view, provide guidance and support appropriate action on disruptive delivery methods. CREST is also agile enough to react to these potential changes in the market in a way that governments from a strategic perspective, or individual buyers cannot. As an industry, penetration testing suppliers must consider moving to self-regulation or industry regulation rather than wait for governments to act and implement controls that they do not understand or appreciate the implications that they could have on the market.

CREST has long said that we need to understand how these disruptive delivery methods fit into the overall ecosystem of technical assurance activities; extracting the positives and ensuring that comprehensive guidance to the buying communities and influencers is provided, not only describing what they are but how and when to use them. CREST continues to run international collaborative research projects to keep abreast of changes and to have an industry level viewpoint.

No single approach to technical assurance is the best, or the right approach. Despite the marketing hype associated with individual delivery methods, a comprehensive and balanced approach is generally what is required. CREST, on behalf of its members and the buying communities it supports must be in a position to give guidance and support. Where necessary, CREST must also consider supporting the move towards self or industry led regulation, taking its lead from its members and the buying community through collaborative research activities.

In addition to the understanding, the definition and potential control of disruptive delivery methods, it is also the role of CREST to try and control wild claims, even from traditional providers, so that the buyers have a true reflection of the services being offered. This is essential if the buyers are not going to be duped into for example, buying penetration testing services that are in fact no more than simple automated vulnerability assessments. Where for example vulnerability analysis tools are used, buyers must also have confidence in the quality of service offered and how it is kept current.

If the buyers enter into a bug bounty programme, they must understand all of the implications of starting up a programme, triaging vulnerabilities found, budgeting for fixing problems and communicating with researchers. When paying researchers, buyers must consider the wide demographic of participants, some of whom may be minors working in a country to which the company cannot trade with. Most importantly, when entering into bug bounty programmes, buyers need to understand the limits of coverage and assurance and how programmes can, if necessary, be closed down.

In crowdsourced penetration testing the buyers must understand what service the crowdsourcing company is providing and ensure full coverage during the assessment. They must also be clear how the service is managed from a scoping and delivery perspective; how the crowdsourcing company controls quality and assesses the credentials of the individuals they are utilising; and how they manage and monitor the ethics of those individuals.

The issues to be considered do not simply stop with the buyers of the service. The suppliers must understand the context in which automated vulnerability analysis is carried out and be able to explain where it is used in the penetration testing programme. Suppliers must take a view on whether they will allow their employed staff to participate in bug bounty programmes and whether they will be allowed to use company supplied technology and tools to help them with this work. If they are in a regulated environment such as an audit or accountancy firm, they must understand how they will manage the client relationship if employees participate in bug bounty programmes of clients. If a regulated company allows employees, some of whom may not be part of the technical assurance teams, to participate, there may be a need for some form of a declaration of participation. The implications of losing a major audit client because of a lack of control in a bug bounty programme would be significant. It is likely that almost the same controls need to be applied to someone participating in a bug bounty programme with virtually no benefit to the regulated service supplier, as it would be controlling a full consultancy assignment. Similar issues arise with crowdsourced penetration testing services. In addition to potential client conflict issues, would you allow your employee to contract to another organisation, use your equipment and your software tools and derive a separate income outside of your organisation? Changing the label used to a ‘modern disruptive’ term does not change the types of control that must be in place.

CREST has research projects underway in all of these areas and is constantly evolving the Accreditation Processes it adopts to reflect the concerns of the market, but also to ensure that good innovation is not hampered.

Vulnerability Analysis

In the area of Vulnerability Analysis, CREST has built on the work that it has done for the NSA in the USA as well as the work on Cyber Essentials, to develop a process for accrediting these vulnerability analysis services and validating the technical capability of the suite of tools utilised. It has introduced Practitioner level examinations to ensure that even at the professional entry point, the individuals have the skills, knowledge and competence necessary to interpret the outputs from such tools and to ensure that the reports provided to clients, or the continual monitoring escalation processes are appropriate and fit for purpose. CREST has long advocated that schemes such the UK Government CHECK Scheme would benefit from the use of accredited Vulnerability Analysis services. It would allow simple non sensitive systems to be accredited quickly and at an affordable cost, allowing the Government to spend more on penetration testing services at the higher end of the market right through to Critical National Infrastructure assurance activities. A one size fits all model is not appropriate for the variety of government environments. The issue has been how to trust these types of services and understanding where they fit into the overall assurance ecosystem. CREST is also trying to influence PCI (Payment Card Industry) schemes. PCI helped to set good standards in this area. The view is now that the exiting PCI ASV (Approved Scanning Vendors) model has not evolved fast enough to reflect the changes to the threat and tools and requires updating. At one of CREST Vulnerability Analysis workshops run in the UK virtually all of the country's PCI ASV providers wherein the room and had a common view. The Vulnerability Analysis Accreditation will be launched in 2019 and within the new CREST Buyers Support Platform these types of services provided by existing CREST member companies can be identified. Working collaboratively the industry can make a real difference in this area.

Bug Bounty

In the area of bug bounty, CREST has run a series of international workshops with buyers, traditional penetration testing providers and major bug bounty programme providers. The subsequent report is probably the most comprehensive and considered report in this area, https://www.crest-approved.org/2018/08/15/bug-bounties-working-towards-a-fairer-and-safer-marketplace/index.html

The report highlights a number of actions the bug bounty Service providers, the buying community and those helping to establish and run internal bug bounty programmes should take. CREST has already organised follow up workshops to progress these actions and to start the process of moving to industry regulation before state regulation starts to be applied. This report and associated presentations on the CREST Advocate YouTube Channel are essential reading for those operating in the industry.

Crowdsourced Penetration Testing Services

Crowdsourcing penetration testing is a new term but is based on existing delivery concepts. There is a lot of confusion between crowdsourced vulnerability hunting (bug bounty) and the more controlled contractually based crowdsourced penetration testing. In the UK, existing penetration testing service suppliers have long augmented their internal teams with contracted staff. In the USA the use of contracted resources is much more common. CREST has recognised this and as part of its Company Accreditation process, first asks the question as to whether contractors are used and if this is the case then requests significant additional information to ensure that contracted staff are managed under the same policies, processes and procedures as employed staff. Once accredited any deviation from the submitted policies, processes and procedures would result in action from CREST.

In established schemes such as the UK Government CHECK scheme suppliers have been approved to provide services in this area that employ a very limited number of qualified staff and look to the contract market or partnership model to deliver these services. The CHECK scheme has reacted to this by changing contractual agreements but it difficult for contracts to keep up with disruptive delivery methods. The generalist companies are very good at meeting the continually changing requirements of government framework agreements and managing quite complex large-scale multi-discipline projects. These companies do not normally specialise in a particular area and CREST has found that the its exacting accreditation standards have made it difficult for this type of generalist supplier of services to meet the requirements of CREST membership.

In reaction to this difficulty to meet the CREST requirements, a number of these generalist contracting companies now have formal links with CREST Accredited Companies to supply these services. This combines the ability to participate in costly complex government preferred supplier lists with the ability to provide controlled specialist penetration testing services. In the USA, the use of contractors is much more prevalent as a business model. In the area of penetration testing this, coupled with the size of the market, has led to the development of boutique contracting houses suppling penetration testing services. In order to differentiate themselves in the market and to suggest a new approach, the term Crowdsourced Penetration Testing services suppliers has been used.

Whilst there are many similarities to the traditional generalist contracting model, the main difference is that as a specialist supplier they can and are investing in the development of appropriate policies, processes and procedures to support their specialist activities. CREST is seen as the thought leader in the accreditation of penetration testing service suppliers, so it is natural for the crowdsourced penetration testing service suppliers to move towards aligning their services to good practice, CREST Accreditation.

CREST has been aware of this move for some time and has raised this as a potential issue as well as an opportunity to the CREST community. CREST has already acted to strengthen the contractor elements of the Accreditation process. This will be applied to all of the CREST members who utilise contractors for delivery of part of their service offering, not just crowdsourced penetration testing services. CREST has also strengthened other parts of the Accreditation process to ensure that it can accommodate this type of business model in a controlled manner. It is also considering the introduction of specialist membership classes for this type of service and other disruptive delivery methods to help the buying community understand what they are buying. CREST must do this in a way that does not adversely impact exiting CREST members who use contracted to augment rather than replicate their delivery teams. Crowdsource penetration testing suppliers must demonstrate all of the same policies, processes and procedures for the management and delivery of their services as traditional penetration

testing service suppliers They must demonstrate the appropriate individual vetting requirements and credentials as well as the management and control of client information in the same way as more traditional penetration testing suppliers.

Code of Conduct and Code of Ethics

CREST has also conducted a detailed review of its existing Code of Conduct. The existing Code of Conduct has been refined to reflect the research conducted on over 30 different codes from both within the technology community and within other professions. One of the conclusions is that whilst it is possible to develop meaningful and enforceable codes of conduct linked to complaints processes to existing delivery models, there is a need to have an overarching Code of Ethics that helps to defined intent and not just the detail. This allows some control over new delivery methods whilst refined detailed codes are developed and implemented. This is necessary to ensure that where disruptive delivery methods are introduced, the Code of Ethics will govern their activities until the detailed Code of Conduct catches up. CREST has developed the new Code of Ethics and it now applies to all CREST member companies and qualified individuals.

Again, existing penetration testing suppliers should look at their staff contracts and policies to ensure that they fully-understand the implications of their staff considering participating in activities such as crowdsource penetration testing.

CREST is already seeing crowdsourced penetration testing companies applying for CREST membership. Whilst most are not mature enough to meet the exacting CREST requirements there are a small number that have spent a great deal of time working through the requirements and ensuring that their policies, processes and procedures for managing their contracted community are in line with the CREST requirements and meet industry good practice. Due to the potential change in the competition in the market, some CREST members will be concerned that their market position will be impacted and therefore steps should be taken to eradicate the practice from the market. The reality is that elements of their business model are already incorporated into many of the existing suppliers' business models and any move to eradicate would inadvertently adversely impact their business. The other reality is that this type of business model is moving into the market and as a technology driven industry, we must react in a positive but controlled manner.

CREST is moving the collaborative activities in its research into Crowdsourced Vulnerability Assessment up its priority list, with a view to building on the work it has already conducted and establishing an industry agreed position. This work is likely to result in some changes to the Accreditation processes to reflect the changing business models, but not adversely impact existing service providers. It will also result in new guides to help the buying community understand what crowdsourced penetration testing is and when and how they should procure it in a way that protects their business.

CREST Test and CREST Report Standards

All of the work looking at changes in existing penetration testing delivery models and the introduction of disruptors work is underpinned by the work that CREST has nearly completed on standards for a CREST Test and CREST Report. The minimum standards for these have been defined and discussed in detail with regulators and socialised within our CREST member communities.

- Who supported, conducted and signed off the Test, (CREST is looking at digital certificates that can be included and therefore tracked on the reports. It is also developing more user-friendly qualification validation and again this could be linked to the digital certificate)
- What the qualifications or credentials are of the signatory
- What the team composition was and their qualifications or credentials
- Use of tools and any tool or service accreditations
- Scope of test
- Type of assurance provided (Vulnerability Analysis, Penetration Testing or Intelligence Led Penetration testing)
- Caveats on the level of testing conducted
- Agreement on report findings
- Physical location of test
- A declaration of whether illegal or inappropriate activities or content were discovered during the test
- Priority vulnerability List
- Report totality (the requirement to deliver the report in totality for regulatory or evidential activities)
- Reference to documentation reviewed
- References to CREST complaints process

All of these reporting requirements are designed to ensure that the buyers are receiving the type of service that they think they are buying, and that appropriate controls and recourse is in place. It will also help to ensure that appropriately qualified individuals are responsible for the work, recognising that the vulnerability analysis of a non-sensitive system requires a different skillset that a review of critical national infrastructure assets.

Importantly, these requirements can be refined to ensure that any introduction of a disruptive delivery service model has the same controls in place to protect the client interests. The trust model is essential if we ae to be viewed as a progressive forward-thinking profession.

The Implications of GDPR

CREST has also conducted research into the implications of GDPR and other data protection regulations and the impact that these could have on the penetration testing industry. Put simply, CREST is trying to obtain an industry position to take to the Information Commissioner for a view on the implications on penetration testing in relation to GDPR. It is important to understand the Information Commissioners view on say the use of social engineering to obtain personal credentials and then to use these credentials to gain access to information or escalate privilege. The results of this work will have implications on existing penetration testing delivery models, which we currently think can be managed through the CREST Company Accreditation process and the register of credentials of individuals coupled with our Code of Conduct and Ethics. This work is however likely to have wider and more significant implications on some of the disruptive service delivery models.

The existing penetration testing industry should not dismiss or look to outlaw disruptive delivery methods but look to ensure that the buying community and those in the technical security industry are protected against bad practice. There is a real opportunity for the penetration testing community to demonstrate that the introduction of disruptive delivery service models can be harnessed and incorporated into existing business models. Through self or industry led regulation, the best of these new approaches can be embraced, whilst ensuring that there are appropriate controls in place to protect the buying community. To do this the penetration testing industry must work collaboratively with the disrupters and the buying community to understand the delivery models and the implications.