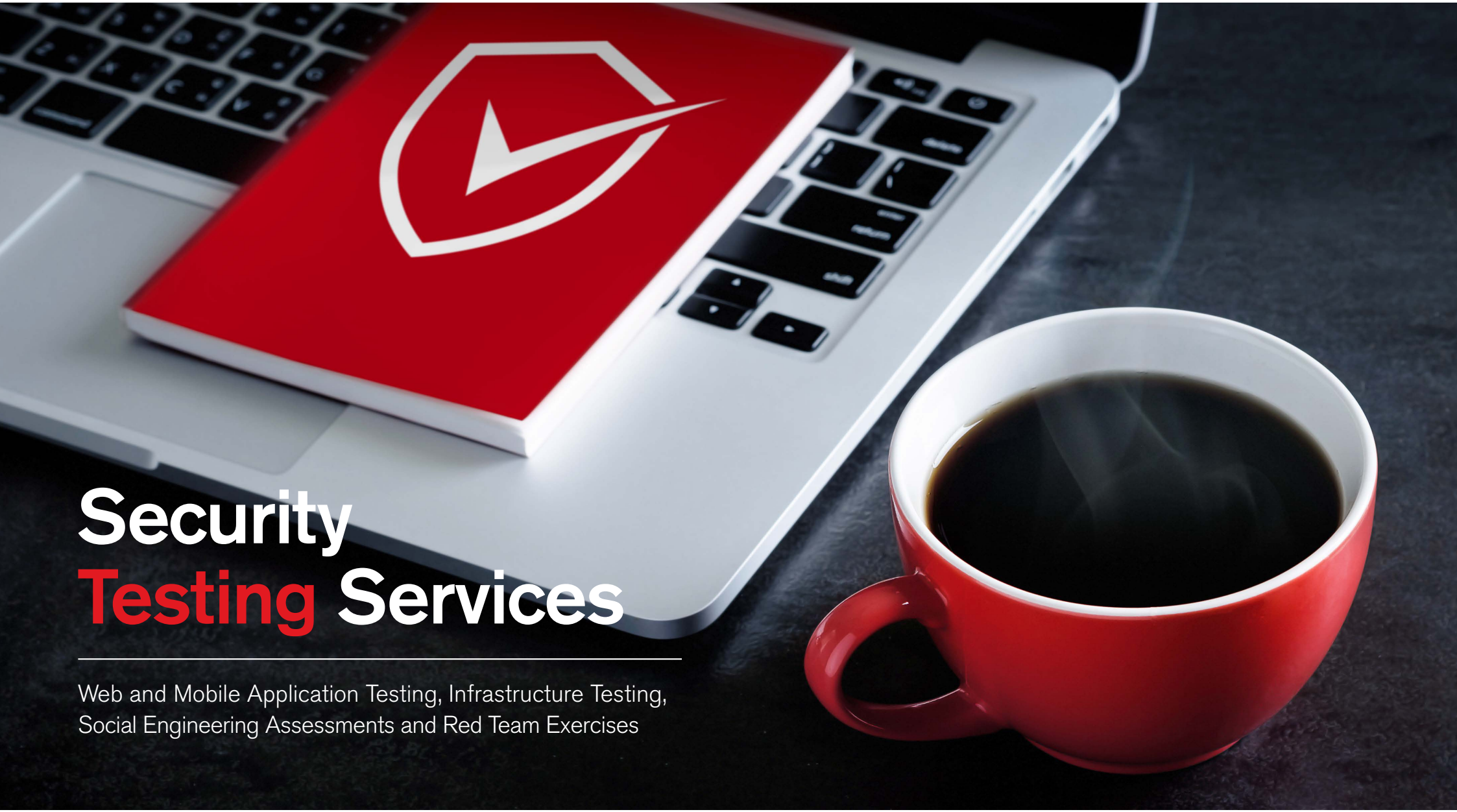


Security Testing Services

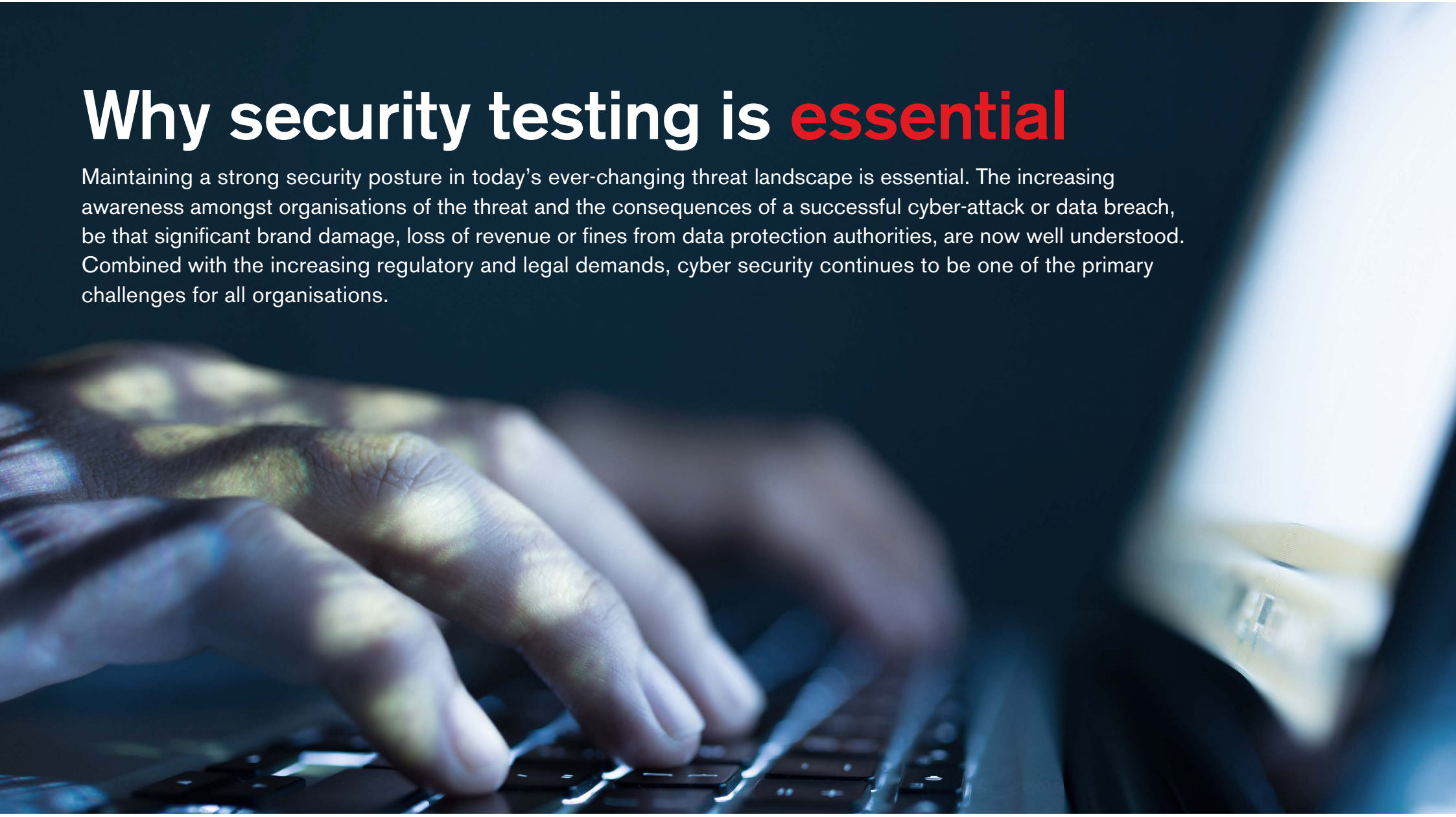
Web and Mobile Application Testing, Infrastructure Testing,
Social Engineering Assessments and Red Team Exercises

claranet cyber security

sec-1

Why security testing is essential

Maintaining a strong security posture in today's ever-changing threat landscape is essential. The increasing awareness amongst organisations of the threat and the consequences of a successful cyber-attack or data breach, be that significant brand damage, loss of revenue or fines from data protection authorities, are now well understood. Combined with the increasing regulatory and legal demands, cyber security continues to be one of the primary challenges for all organisations.



claranet cyber security

sec-1

Visibility of the threats to help you prioritise

A clear and logical strategy of security testing against key targets within your organisation can provide the threat visibility needed in order to make changes, deploy defensive technology and train staff in a way that will make the job of a malicious attacker much harder and reduce the chances of a security breach.

Selecting the right type of attack simulation and the right targets to bring into the scope of the exercise is difficult. With 17 years' experience in penetration testing, Claranet Cyber Security can offer a comprehensive, global breadth of service. We make our work together engaging and personal, we are known for being practical, to the point and relationship-orientated.

claranet cyber security

sec-1

Web Application Testing

Available to hackers 24x7 and brim-full of data, web applications present a tempting target for hackers. Our penetration testing relies on the manual exploitation of vulnerabilities so you get the assessment of business risk that only an expert tester can provide. We combine this with the use of the best automated tools. All assessments are followed by a comprehensive report, with both non-technical and technical descriptions, alongside recommendations for remediation.

We provide visibility of risks including:

- **Unauthorised access past authentication controls to escalate privileges**
- **Introduction of malicious code**
- **Manipulation of the application's function**
- **Defacing of the website or causing disruption**
- **Gaining access to the hosting infrastructure**

In addition to our point-in-time web application testing services we also offer continuous security testing and Security Operations Centre (SOC) services to keep you protected around the clock. Please ask for details.

claranet cyber security

sec-1

Mobile Application Testing

With the huge proliferation of mobile applications comes the need for robust security testing to validate that mobile applications are defending systems and data to the same level as the standard web application.

The aim of the exercise is to validate that the mobile application is coded securely, preventing attackers from subverting authentication controls, escalating privileges, introducing malicious code or manipulating the application's functionality in order to achieve their goals. Any failure to mask and/or store sensitive information correctly could lead to leakage and its use by applications other than the intended.

Mobile application testing validates:

- **The encryption of data both in transit and at rest**
- **Web services**
- **Information disclosure through local data storage**
- **APIs cached data such as application backgrounds**

claranet cyber security

sec-1

Infrastructure Testing

The principal aim of infrastructure testing is to highlight where vulnerabilities exist in computer systems that could provide unauthorised access or serve as an entry point into private areas of the network and to sensitive data.

Infrastructure testing applies in many areas including internal, perimeter, and cloud. It also applies to many technology areas from PCs and laptops to smart phones and Wi-Fi networking. From a hacker's perspective each area represents an opportunity to attack, opportunities that can be minimised by reviewing your security in the same way you would your buildings or physical assets.

Infrastructure testing can be deployed as a stand-alone exercise to provide a comprehensive view of the vulnerabilities and associated exploits or can be used as an element in a wider simulated attack including web application, social engineering and physical access assessments.

Social Engineering Assessments

Social Engineering is becoming one of the most effective means of gaining access to secure systems and sensitive information. What is more, the attacker requires little to no technical knowledge. Preventing an attack of this nature requires a very different set of defences to traditional cyber security defences.

Raising employee awareness

Your best defensive strategy against social engineering is to raise employee awareness and to educate on good practices. A social engineering assessment from Claranet Cyber Security allows you to see how susceptible your staff might be when presented with an attempt by an attacker to trick them. The results of social engineering assessments can be used to direct training, create data handling guidelines and security policies.

Typical social engineering engagements include:

- **Phishing & spear phishing campaigns** - tricking users via email
- **Physical entry** - gaining unauthorised access to buildings
- **Baiting** - tempting users into plugging in USB drives...
- **Staff impersonation -** in order to obtain information or access remotely

claranet cyber security

sec-1

claranet cyber security

sec-1

Red Team Exercises

A Red Team exercise is an all-out attempt to achieve the defined objectives by any methods available, and usually includes internal and external penetration testing, compromising wireless networks, physical access and other social engineering techniques.

Red Team exercises are performed using a black-box testing approach where no prior information about the target organisation is given. During a Red Team engagement, the defending side is unware of the exercise and is expected to respond as it would during a genuine attack.

Red Team common objectives

- **Foothold:** Standard user access (shell/GUI) gainedfrom outside
- **Privilege Escalation:** Administrative user privileges gained
- **Defence Evasion:** Evade external/internal security alerting systems
- **Persistence:** Remote access is not being dependent on a single user account or a single device
- **Lateral Movement:** Traversal to multiple points on a network
- **Full Compromise:** Domain/Enterprise Admin account or equivalent compromised
- **Collection:** Action on objectives
- **Exfiltration:** Data exfiltration

claranet cyber security

sec-1

Our accreditations

Claranet Cyber Security continually invests in hiring the most experienced, highly trained teams in the industry. A core part of delivering the best service is our commitment to being fully accredited across all the major standards in IT security. These include:

claranet cyber security

sec-1

For more information about our **Security Testing Services** please call:

01924 284 240

claranet cyber security

sec-1

claranet®
cyber security