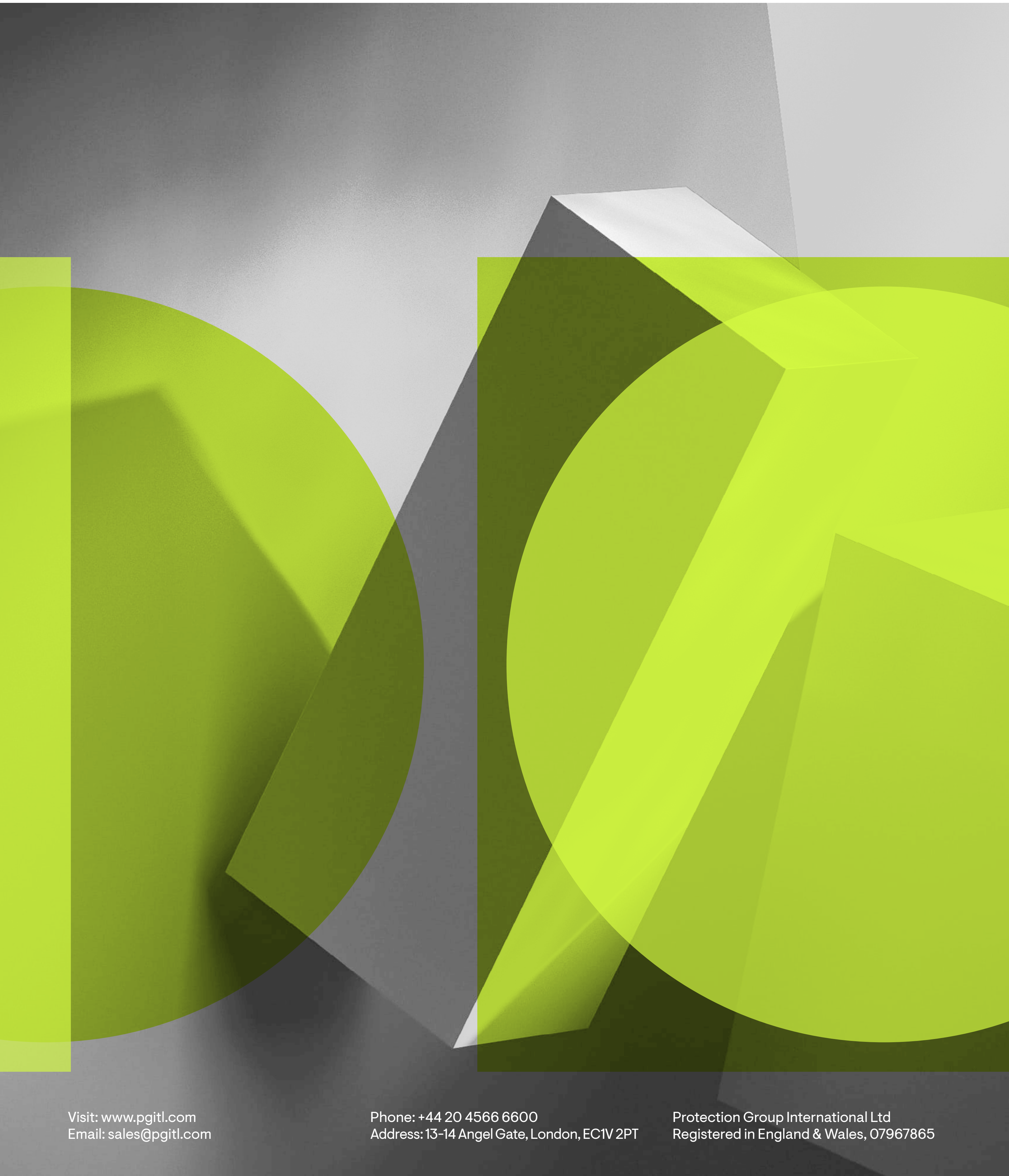
Penetration Testing



Visit: www.pgitl.com
Email: sales@pgitl.com

Phone: +44 20 4566 6600
Address: 13-14 Angel Gate, London, EC1V 2PT

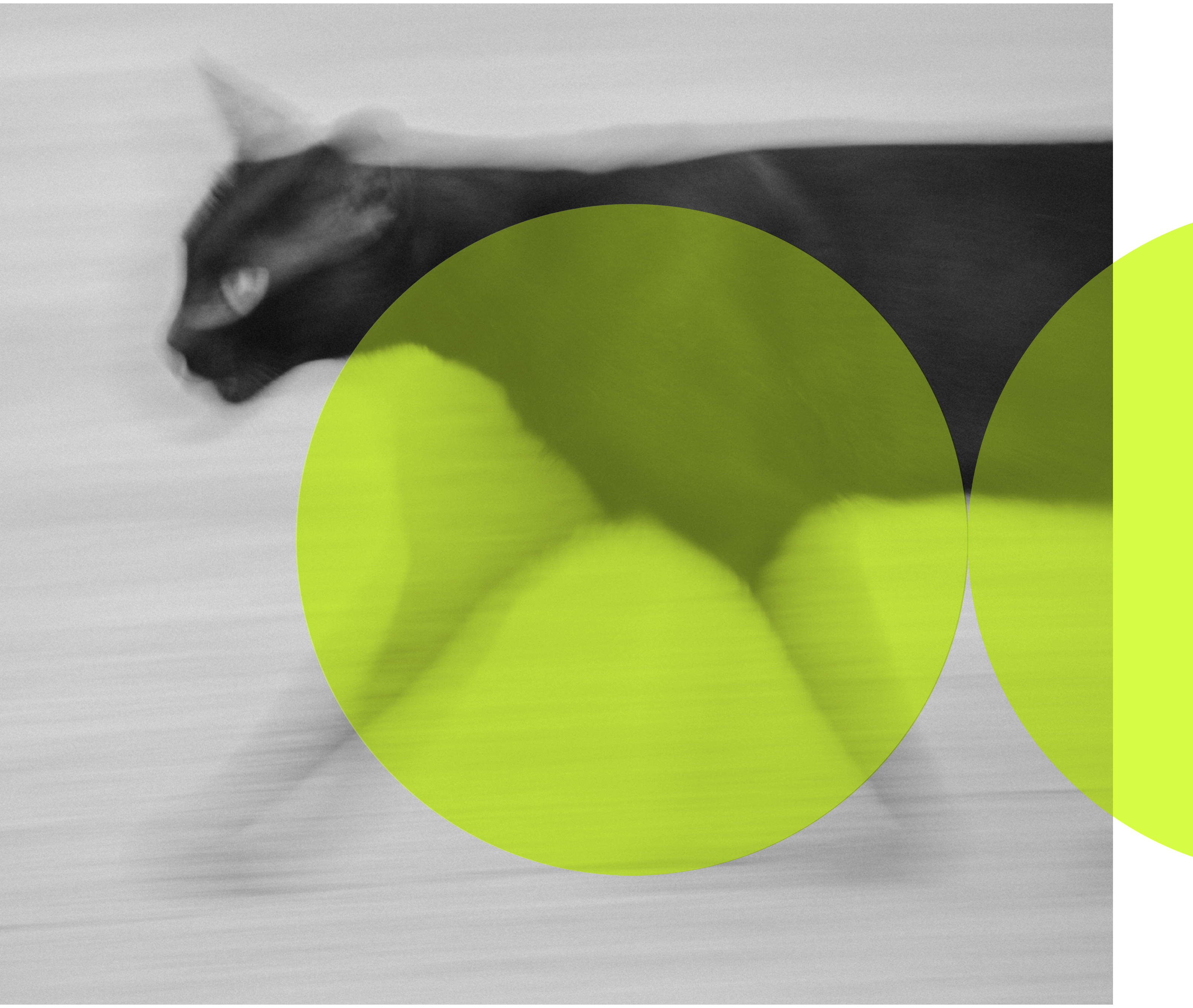
Protection Group International Ltd
Registered in England & Wales, 07967865

Let us find exploitable technical vulnerabilities before someone else does.

No business is immune to cyber-attacks, but there are measures you can take to minimise risk.

Every year, almost half of UK businesses suffer some sort of digital breach. A penetration test is like a practice run to assess if an organisation is secure. During these tests, your team keeps operations running as usual while an external party validates the security of your processes.

At PGI, we've been helping organisations protect their data since 2013. We identify all digital vulnerabilities and advise on the best remediation strategies to prevent malicious attacks.



What is penetration testing?

Penetration testing — also known as pen testing or ethical hacking — covers a range of tests that are designed to identify gaps in IT security that could put your business at risk.

Weaknesses often take the form of:

- Unpatched vulnerabilities in operating systems, applications and firmware
- Incorrect configuration of servers, networks, applications, firmware and operating systems
- Logic flaws in web applications, such as configuration of pricing and user management

Our security experts will conduct the tests either remotely or onsite. Once any issues with your systems and networks have been identified, our consultants will provide expert advice on strengthening your defences.

Why should I have a penetration test?

There are valuable benefits to committing to regular penetration testing, from gaining valuable insights into your setup's integrity to reassuring your clients.

Understand the risks

Our penetration tests provide you with clear data about the level of technical risk emanating from your IT infrastructure and web applications. They also offer the information required to fix gaps in your organisation's IT setup – before they become problematic.

Gain peace of mind

A correctly scoped test means you can feel confident that your networks and applications are as safe and secure as possible, and configured in accordance with best practice.

Demonstrate commitment

Regular testing allows you to demonstrate security to clients and stakeholders your strong and ongoing commitment to IT.

What tests do we offer?

Because vulnerabilities exist in all technology, from hardware to operational processes, we offer a range of CREST-accredited security tests that cover all potential risk areas:

1 Infrastructure testing

Identifies weaknesses across your IT infrastructure that could expose you to risk. This test examines your IT system as a whole — including hardware and software — to assess existing security measures and highlight areas for improvement.

2 Web application testing

Discovers vulnerabilities in your web applications, helping you to minimise the risk of data loss.

3 Wireless testing

Focuses exclusively on identifying and mitigating risks associated with your organisation's wireless network.

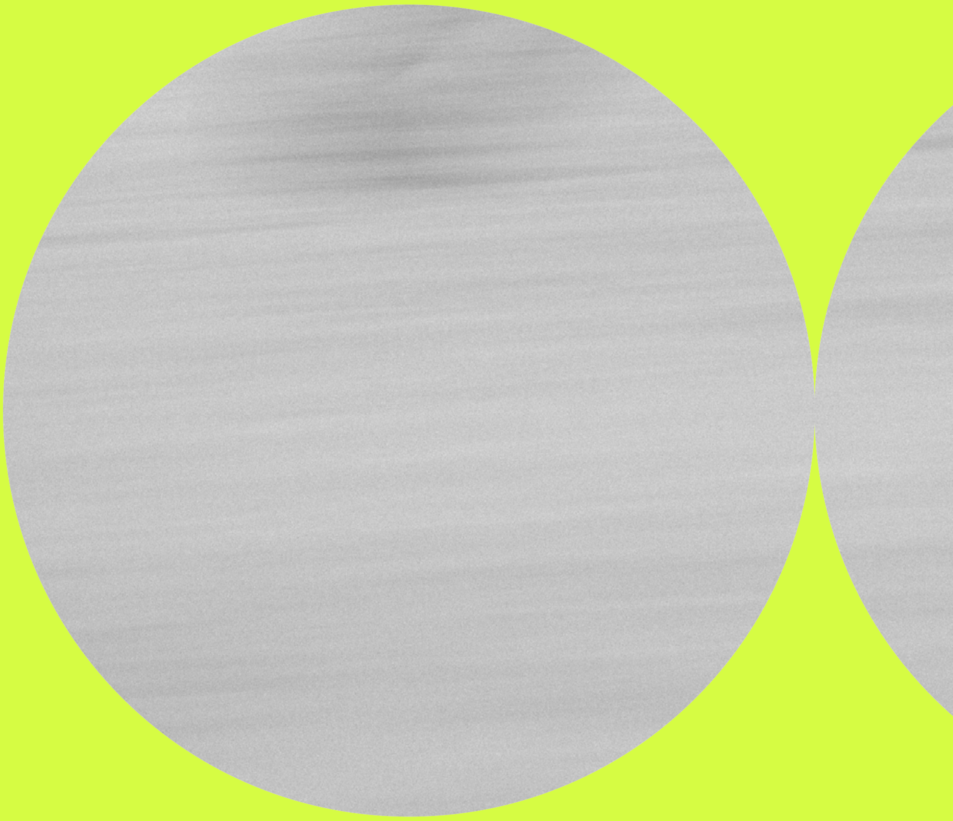
4 Build and configuration review

Assesses operating systems, devices, services and cloud environments to ensure they are in line with security best practices. A good review achieves the ideal balance between security and functionality for a business's critical assets.

5 IT health check

An annual assessment that is required by all public sector organisations on the government's Public Services Network (PSN). The health check examines all aspects of IT security to ensure any weaknesses are identified and managed.

Why choose PGI?



Our team of experts:

Our experienced, multi-disciplinary team appreciates how information security and cyber security intersect, ensuring an in-depth understanding of your needs. An accredited CREST Member, PGI works to the highest industry standards.