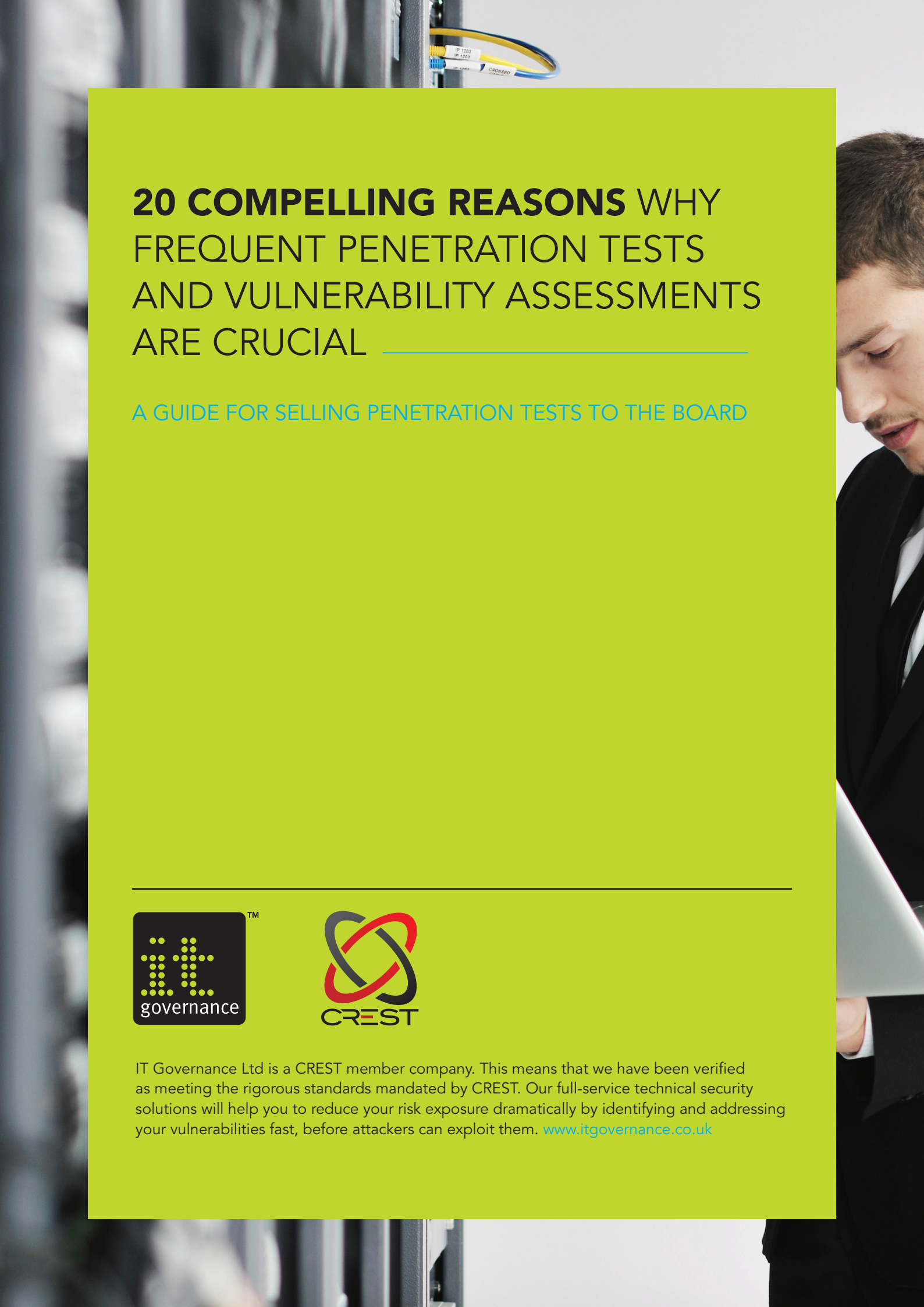
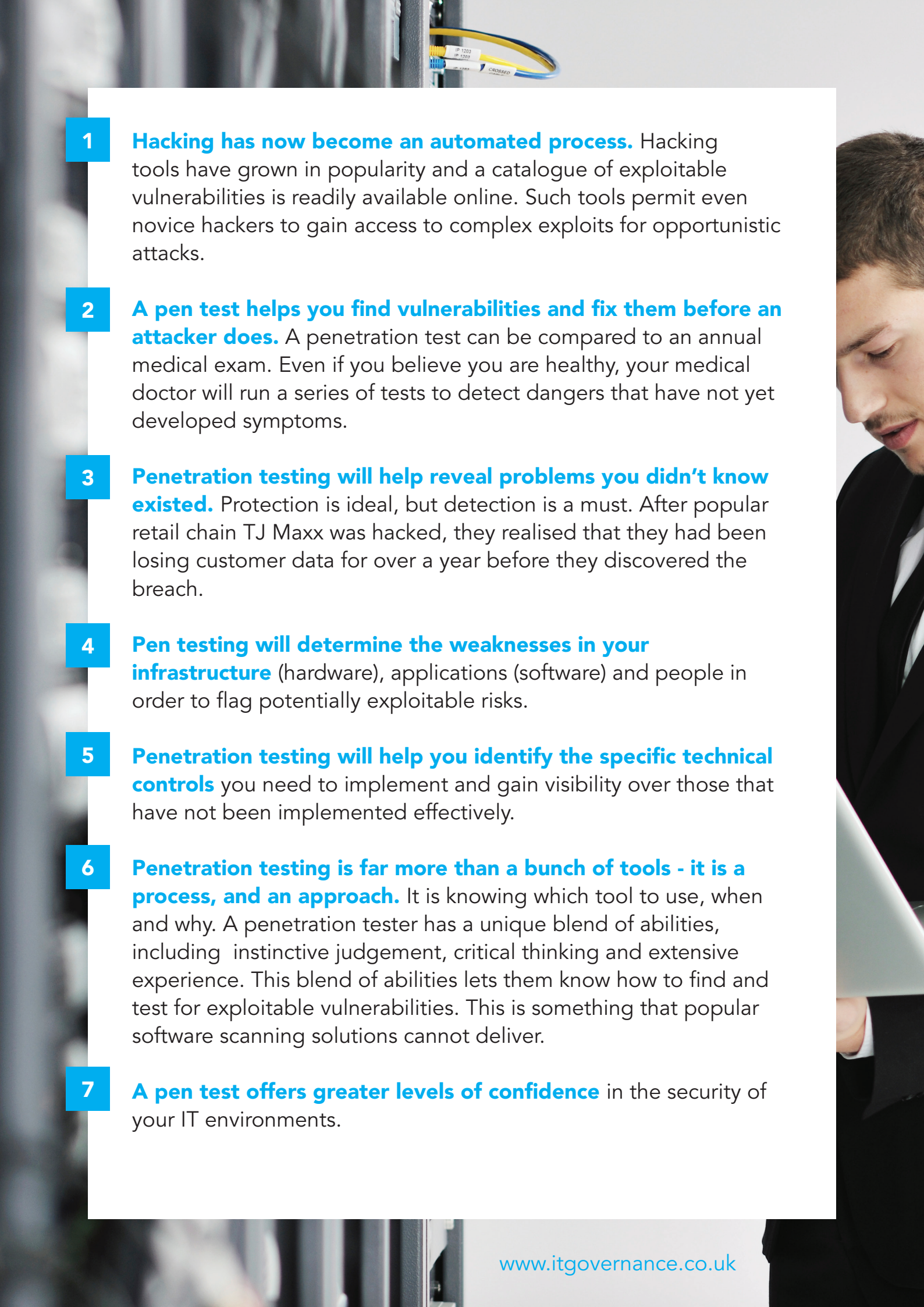


# **20 COMPELLING REASONS** WHY FREQUENT PENETRATION TESTS AND VULNERABILITY ASSESSMENTS ARE CRUCIAL

## A GUIDE FOR SELLING PENETRATION TESTS TO THE BOARD

IT Governance Ltd is a CREST member company. This means that we have been verified as meeting the rigorous standards mandated by CREST. Our full-service technical security solutions will help you to reduce your risk exposure dramatically by identifying and addressing your vulnerabilities fast, before attackers can exploit them. www.itgovernance.co.uk



1. **Hacking has now become an automated process.** Hacking tools have grown in popularity and a catalogue of exploitable vulnerabilities is readily available online. Such tools permit even novice hackers to gain access to complex exploits for opportunistic attacks.

2. **A pen test helps you find vulnerabilities and fix them before an attacker does.** A penetration test can be compared to an annual medical exam. Even if you believe you are healthy, your medical doctor will run a series of tests to detect dangers that have not yet developed symptoms.

3. **Penetration testing will help reveal problems you didn't know existed.** Protection is ideal, but detection is a must. After popular retail chain TJ Maxx was hacked, they realised that they had been losing customer data for over a year before they discovered the breach.

4. **Pen testing will determine the weaknesses in your infrastructure** (hardware), applications (software) and people in order to flag potentially exploitable risks.

5. **Penetration testing will help you identify the specific technical controls** you need to implement and gain visibility over those that have not been implemented effectively.

6. **Penetration testing is far more than a bunch of tools - it is a process, and an approach.** It is knowing which tool to use, when and why. A penetration tester has a unique blend of abilities, including instinctive judgement, critical thinking and extensive experience. This blend of abilities lets them know how to find and test for exploitable vulnerabilities. This is something that popular software scanning solutions cannot deliver.

7. **A pen test offers greater levels of confidence** in the security of your IT environments.

8 **Frequent penetration testing helps to maintain consistent, ongoing security.** New vulnerabilities appear every month, making you vulnerable to new opportunistic attacks.

9 **Security consists of protection, detection and response** - and you need all three to have good cyber security. Cyber security is founded on a cyber security risk assessment, of which penetration testing is a key component.

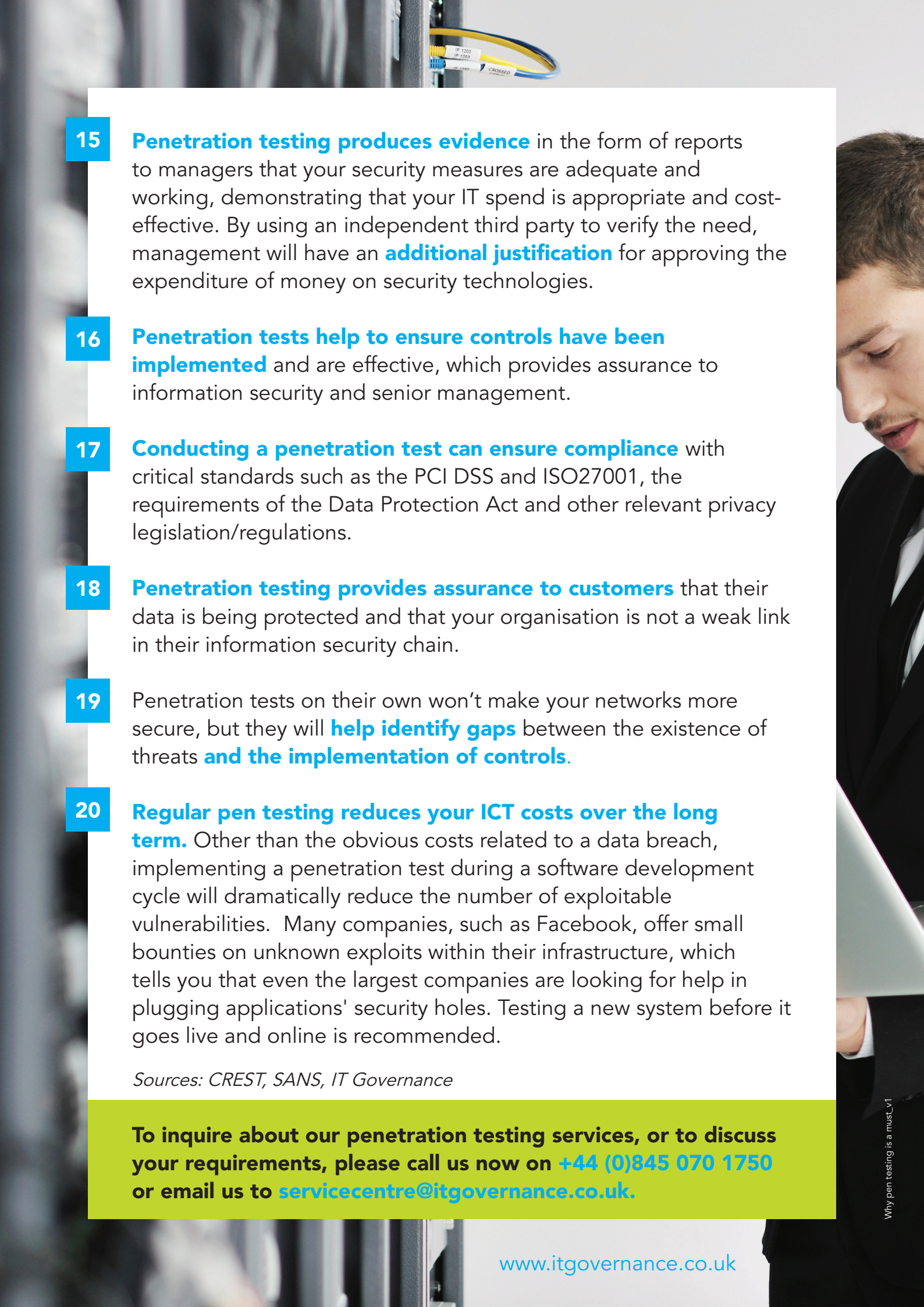
10 **Internal penetration testing can reveal procedural failings in your organisation,** such as insecure services being used for administration, password policies being weakly enforced or a patching policy not being applied properly. This can lead to a massive opportunities for infiltration by attackers.

11 By implementing a regular penetration testing regime, you can **continually measure and improve the security performance of your systems and networks,** ensuring that your assets and information are appropriately protected at all times. Maintaining a secure network requires constant vigilance.

12 **Non-technical executive management reports** provided by IT Governance's penetration testing teams will **help senior managers understand the recommendations** outlined in the testing overview. Meanwhile, the detailed technical feedback included in the technical reports will be immediately actionable by your IT/ security team, **saving you time and costs.**

13 **Penetration testing provides a second set of eyes.** Using an independent, external provider to test the security of a critical system is good security practice.

14 **Penetration testing gives security personnel a chance to recognise and respond to a network attack.** Testing the monitoring and incident handling teams can show if they are able to figure out what is going on and how effective their response is.



15 **Penetration testing produces evidence** in the form of reports to managers that your security measures are adequate and working, demonstrating that your IT spend is appropriate and cost-effective. By using an independent third party to verify the need, management will have an **additional justification** for approving the expenditure of money on security technologies.

16 **Penetration tests help to ensure controls have been implemented** and are effective, which provides assurance to information security and senior management.

17 **Conducting a penetration test can ensure compliance** with critical standards such as the PCI DSS and ISO27001, the requirements of the Data Protection Act and other relevant privacy legislation/regulations.

18 **Penetration testing provides assurance to customers** that their data is being protected and that your organisation is not a weak link in their information security chain.

19 Penetration tests on their own won't make your networks more secure, but they will **help identify gaps** between the existence of threats **and the implementation of controls**.

20 **Regular pen testing reduces your ICT costs over the long term.** Other than the obvious costs related to a data breach, implementing a penetration test during a software development cycle will dramatically reduce the number of exploitable vulnerabilities. Many companies, such as Facebook, offer small bounties on unknown exploits within their infrastructure, which tells you that even the largest companies are looking for help in plugging applications' security holes. Testing a new system before it goes live and online is recommended.

*Sources: CREST, SANS, IT Governance*

**To inquire about our penetration testing services, or to discuss your requirements, please call us now on +44 (0)845 070 1750 or email us to servicecentre@itgovernance.co.uk.**