AN INTRODUCTION TO CYBER SECURITY

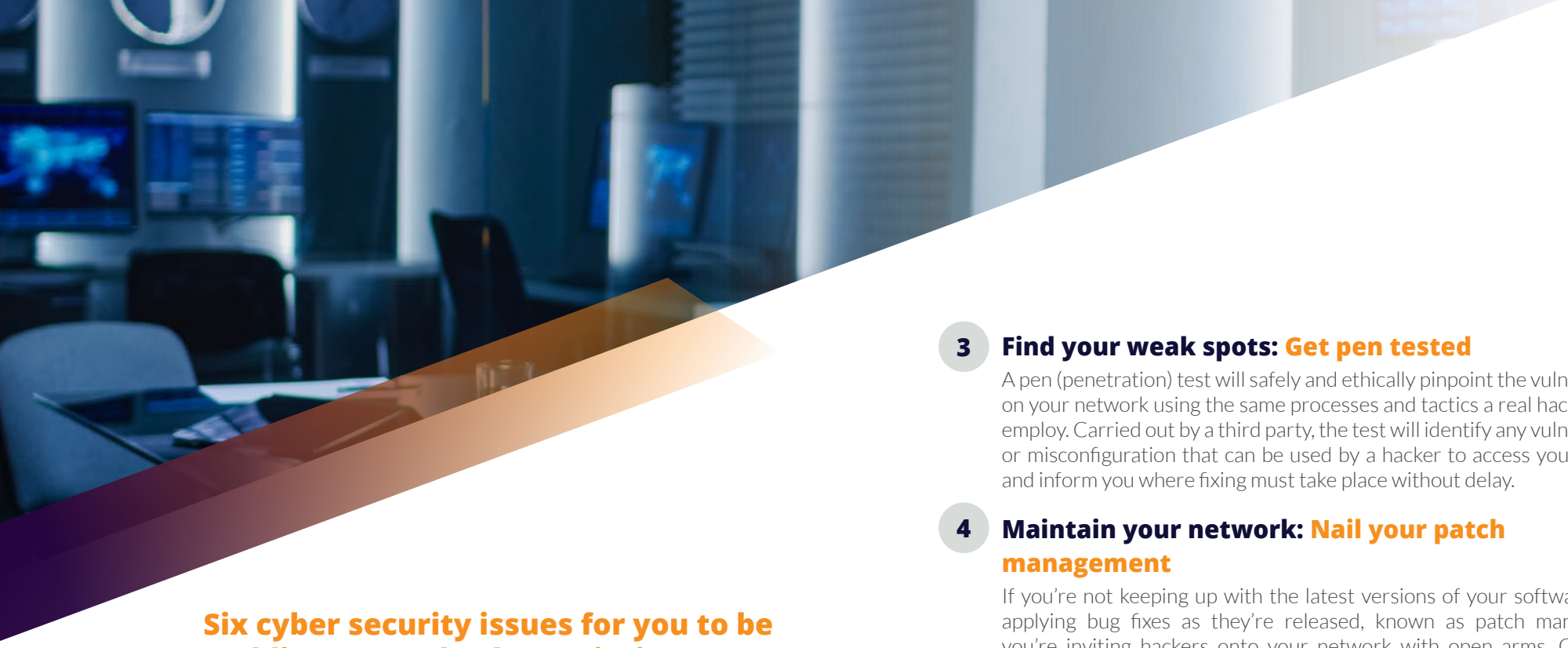
Six cyber security issues you should be considering...

It is a bygone age when passwords were enough to protect your systems and data. As cyber attackers' methods become more and more sophisticated, so must your ways of protecting your business.

This point takes on even more pertinence following the UK's pandemic-induced shift to home working, which has decentralised the workplace like never before. In the scramble to get employees working from home, IT teams have found themselves under enormous pressure, resulting in masses of new IT technology being rolled out, sometimes without proper security protocols in place.

With this in mind, it is essential for you to clue yourself up on the cyber security issues that are most important right now, and gain some understanding about what you need to be doing about them.

CyberGuard Technologies



Six cyber security issues for you to be tackling as an absolute priority:

1 Stay alert: Regularly scan for vulnerabilities

Vulnerability scanning and security monitoring go hand-in-hand and must be built into your workload. Being alert to suspicious behaviour and spotting vulnerabilities on your network is absolutely key to a secure IT network, and it provides the first step in understanding the threat an attacker or employee can potentially pose to your network or data.

2 Control user access: Set up multi-factor authentication

Stringent protocols around user access are a must. First, you must be sure that someone accessing your infrastructure is who they say they are (authentication), secondly you must determine that they are permitted to access the data they are requesting (authorisation). Multi-factor authentication is acknowledged as best practice for all companies these days and forms the backbone of a rigorous access system that sets permissions appropriate for users' roles.

3 Find your weak spots: Get pen tested

A pen (penetration) test will safely and ethically pinpoint the vulnerabilities on your network using the same processes and tactics a real hacker would employ. Carried out by a third party, the test will identify any vulnerabilities or misconfiguration that can be used by a hacker to access your systems and inform you where fixing must take place without delay.

4 Maintain your network: Nail your patch management

If you're not keeping up with the latest versions of your software or not applying bug fixes as they're released, known as patch management, you're inviting hackers onto your network with open arms. Creating a comprehensive patch management plan – or outsourcing it to a third party – will ensure holes in your security are being plugged quickly after they appear.

5 Identify human weakness: Train your staff

It may be uncomfortable to read, but your staff really are the biggest threat to your business' information systems and cyber security. Alarmingly, your organisation could be breached by a phishing attack in just a few minutes. Employees must be taught what to look out for, thus reducing the chance of being duped into giving away precious information such as usernames or passwords to those with malicious intent.

6 Cover all bases: Endpoint security across the board

These days, employees are likely to use a myriad of devices to carry out their work - laptops, mobiles, desktops and tablets - and some of these may be employee-owned. This makes organisations' threat surfaces, and the associated risks, vast. Unsecure file transfers and failure to download security updates are just some of the ways malware or spyware infiltration can occur. Managing the monitoring and endpoint security of a disparate network is challenging but essential to avoid data breaches.

What is cyber security?

Cyber security is the application of tools and controls to protect IT infrastructures and the data, systems, devices and programmes within them. It is the aim of cyber security to prevent unauthorised access to IT infrastructures and reduce the chance of theft or damage.

Need expert help?

Effectively managing your response to these cyber security issues inhouse is undoubtedly a tall order for most businesses. However, choosing to ignore the threat of cyber-crime is not an option for those who understand that data and a secure IT infrastructure is the lifeblood of businesses nowadays.

CyberGuard Technologies (an independent company within the OGL Group) can provide the very latest in cyber security services and lead your proactive approach to cyber-crime on your behalf.

Why take it seriously?

- The costs of cyber security breaches are rising
- Cyber criminals are increasingly sophisticated
- Cyber-crime can damage your reputation
- Cyber security is a critical, board-level issue

YOUR TRUSTED CYBER SECURITY PARTNER

Speak to us about protecting your organisation

Our team of cyber experts can operate as an extension to your business, leading your cyber security proactively and ensuring your business has taken the vital steps needed to protect its assets.

security@cg-tech.co.uk
01299 873800

CyberGuard Technologies