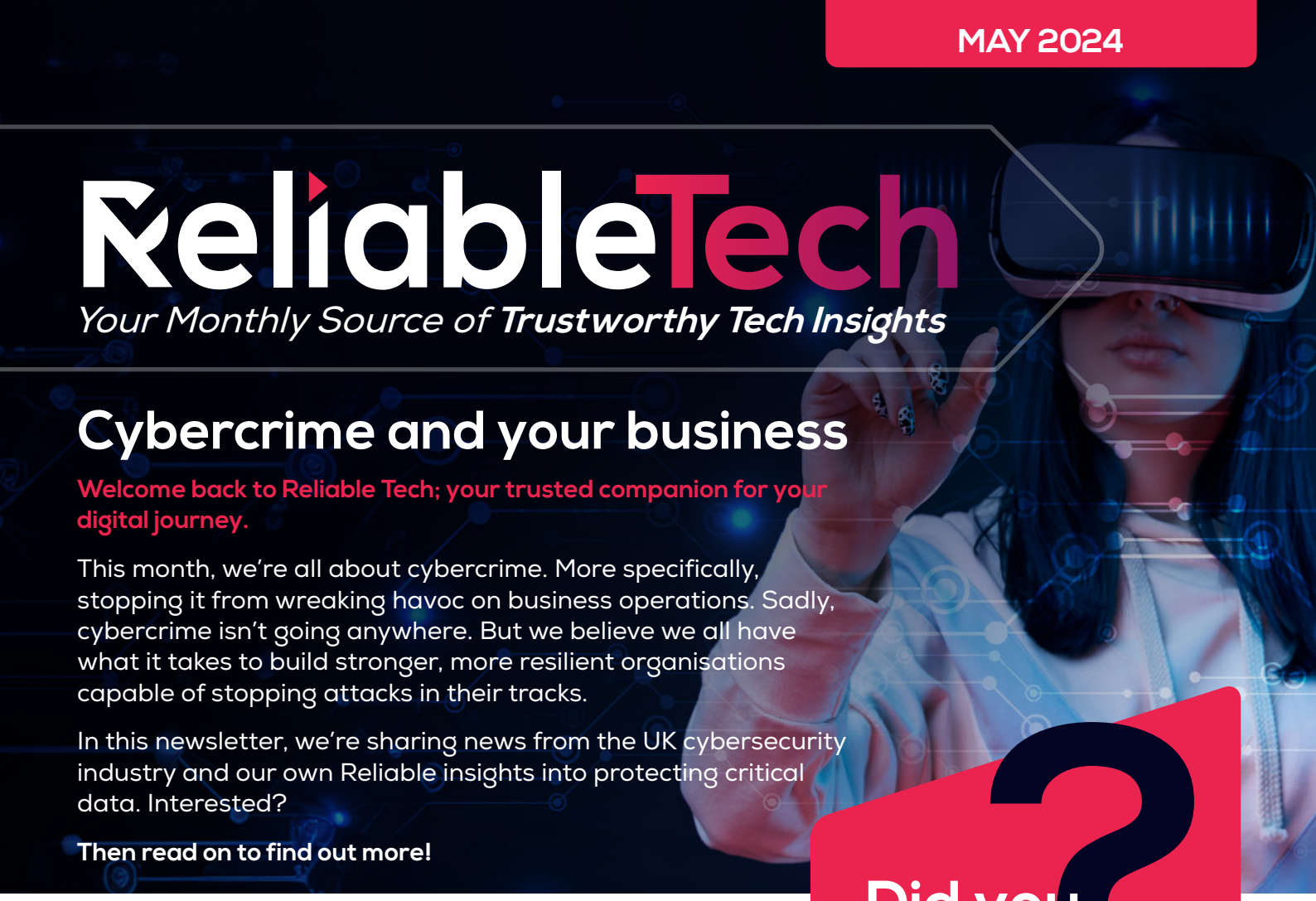
MAY 2024

ReliableTech

*Your Monthly Source of **Trustworthy Tech Insights***



Cybercrime and your business

Welcome back to Reliable Tech; your trusted companion for your digital journey.

This month, we're all about cybercrime. More specifically, stopping it from wreaking havoc on business operations. Sadly, cybercrime isn't going anywhere. But we believe we all have what it takes to build stronger, more resilient organisations capable of stopping attacks in their tracks.

In this newsletter, we're sharing news from the UK cybersecurity industry and our own Reliable insights into protecting critical data. Interested?

Then read on to find out more!

The rise of ransomware

The National Cyber Security Centre describes ransomware as 'the biggest development in cyber crime'. Why? Because this specific type of malware has evolved to create an even bigger impact on organisations. Looking back just a few years, ransomware was primarily used to encrypt single devices. Now, it's being used to damage entire business networks. And with organisations holding increasing quantities of data, more and more criminals are wanting to get their hands on it.

Ransomware attacks are rising... Is your business strong enough to withstand them?

Find out. Take a health check with us to learn more about your current security posture – and how to improve it.

In The Real World... With risks continually growing, London & Partners wanted to know that they were doing everything they could to protect their organisation, their people, and their data in the digital landscape. We stepped in to help them become Cyber Essentials certified, giving them complete confidence that they were taking all the right measures to keep themselves as safe as possible in the online space.

LONDON & PARTNERS

Read more ›

Did you know...

The Government's latest Cyber Security Breaches survey shows that a third of all businesses experienced a cyber attack over a 12-month period, with the average loss per attack coming in at over £1000. Unfortunately, the number of small businesses stating that cyber protection is a high priority for them is decreasing, with only 68% prioritising protection of their digital assets.

Call: 03333 1111 33 | **Email:** hello@reliablenetworks.co.uk | www.reliablenetworks.co.uk

The importance of a multi-pronged approach

One very common theme that we're seeing among today's businesses is that they pick a single form of protection, and stick with it. It's certainly good to see organisations investing in digital security, but the fact is that focusing on just one area isn't always particularly beneficial. It can mean that while one part of the business is well protected, other areas remain vulnerable. Instead, organisations should be coming at it from all angles, protecting themselves from any threat.

There are two critical ways to boost your security posture that every business should be looking into: attack simulations, and security orchestration, automation, and response (SOAR). Together, these solutions form a strong foundation on which to build a more resilient, protected business.

Speed matters

One of the most important things for every business to understand is that attacks don't just come from nowhere. Of course, it can certainly seem that way when you feel blindsided by criminal activity, but the truth is that there were probably some small, subtle signs that your data was at risk. The key is to be able to spot these signs quickly to prevent threats from turning into real attacks on your business. The faster you're able to react and respond, the more likely you are to thwart potential threats.



KnowBe4

Our recent white paper explores how every business can identify threats faster & more accurately with a world-leading solution: KnowBe4. Download it now from our learning hub.

Eager For More?

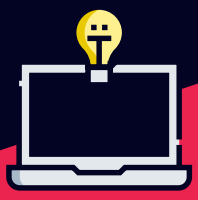
We'll be back next month with the latest edition of Reliable Tech.

Can't wait? want to know more, contact your Reliable Account manager or contact us below

Inspirational quote of the month

"We operate in an uncertain world where adversaries range from the unsophisticated but effective cybercriminals operating in their bedrooms, to the full-throated might of sophisticated hostile states. But whatever the scenario, each of us has a responsibility to address the gaps in our defences".

Lindy Cameron, Managing Director, National Cyber Security Centre



Top Tech Tips

Every month, we ask the Reliable team for their top tech tips to share with businesses.

1. Don't make assumptions

Lots of businesses believe that if their employees can correctly answer questions about cybercrime, then they're well prepared to deal with it. That's not always true. Don't make assumptions that theoretical knowledge can be applied to practical problems. It's better to use interactive methods – like attack simulations – to test how employees would respond if faced with a real threat.

2. Be picky

It's impossible to count all the different cybersecurity solutions that are on the market today. It seems like almost everyone has something to offer. But you can't just put your hand in the bag and pick a solution at random. Unfortunately, some solutions fail to make any impact at all. Where possible, be selective and choose solutions from world leaders and proven industry experts.