

ReliableTech

Your Monthly Source of Trustworthy Tech Insights

Finding the missing link

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

We're now more than halfway through 2024 (believe it or not!), and I think it's time we all had a bit of a celebration. After all, we've had some really great news over the past few months. The Department for Science, Innovation, and Technology reports that businesses are taking cybersecurity more seriously than ever before. And the National Cyber Security Centre has introduced new guidance on phishing attacks which is already helping businesses significantly reduce their risk.

But while things are definitely looking up, it's important that we don't become complacent.

That's why, this month, I'd like us all to take a closer look at what we're doing to maintain a secure environment. I want us to focus on what we're doing right, as well as being brave enough to put our hands up and say, 'this is where we're letting ourselves down'. I want us all to find our missing link.

By 'missing link', I mean that one thing that's perhaps missing from our security strategies, but could help tie everything together. Having worked with many businesses, I know there are some common practices that often get overlooked, so this month I'll talk you through some of them.

Security awareness training

Your employees may know about the risks present within your industry and business. They may even know the best ways to protect themselves and the data they work with. But would they know what to do if faced with a real threat? That's what's missing from a huge number of cybersecurity strategies. Luckily, security awareness training is a simple way to boost employee risk responses.

Did you know...



95% of cyber attacks are only successful because of human error?

Imagine how much of a positive impact we could have on attack statistics if we prioritised security awareness among employees!

Security awareness training acknowledges the huge role that employees play in whether or not an attack is successful. And it aims to ensure everyone within an organisation understands this role. When employees feel confident enough to identify potential threats, report them, and handle them in the safest, most efficient way, they can make smart decisions to help protect your business.

Managed penetration testing

Many cybersecurity strategies feature penetration testing, and for good reason. With experts acting as cyber criminals and attempting to gain access to your systems, you can easily see where your vulnerabilities lie and seal up entry points before hackers can exploit them. The 'missing link', in this case, is that organisations are opting for traditional pen testing over the managed alternative.

According to the National Cyber Security Centre, 'it's not uncommon for a year or more to pass between penetration tests'. Problem? Absolutely. You may find that your security posture is strong in January. But what about February? July? December? Managed pen testing offers regular assessments, giving you ongoing and up-to-date insight into your strengths and weaknesses.

Cloud services

If you're currently working with an on-premises server and managing a physical IT infrastructure, your 'missing link' could be the cloud. The issue here is that on-prem environments may still appear on the outside to be working well, but as time goes on it's increasingly likely that security vulnerabilities will start rearing their ugly heads.

What happens when vendors stop providing support for your on-prem solutions? What happens when they no longer release updates to patch new vulnerabilities? Shifting to the cloud may seem like a big step, but from a security perspective it's one of the smartest things organisations can do to keep themselves safe... especially in a world where cyber attacks are becoming increasingly sophisticated and harmful.

In the real world...

We worked with London Golf Club to carry out a cloud migration project, shifting from on-prem solutions to cloud-based alternatives. This not only enabled the team to make use of more features and functionality, but also enhanced digital security and data protection, ensuring all employee, member, and guest information remained safe.



[Read more >](#)

Eager For More?

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

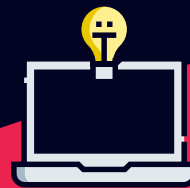
Can't wait? want to know more, contact your Reliable Account manager or contact us below



Powerful quote of the month

"Penetration testing is a great way of finding vulnerabilities in your system before an attacker causes you harm. It's a bit like going to the doctor's for a health check to see if you have things like high or low blood pressure or cholesterol, so they can be treated before these things cause you harm."

Chris Ensor, Deputy Director for Cyber Skills and Growth at the National Cyber Security Centre



Top Tech Tips

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

1. It's OK to admit you're not perfect

We all want to focus on what we're doing well. But honestly, looking at where we're struggling is even more important. It's OK to say 'we need help in this area', and go after what you really need.

2. Don't put all your eggs in one basket

There are many different security solutions out there that all address a different security concern. Try to incorporate a wide variety to give yourself the best protection, rather than homing in on one area.

3. Never settle

Sometimes, a security solution can seem good, but not quite right (for example, standard pen testing). Don't settle for second best. Instead, find what's right for you. If you need help, we're here!