TECH TALK MONTHLY

YOUR MONTHLY DOSE OF TECH & BUSINESS NEWS

WHAT'S INSIDE?

MONTHLY UPDATE FROM TONY

Do you remember how we used to collaborate on documents in the bad old days? (y'know, about 10 years ago).

I'd write a document and email it to you.

You'd save it, adding "v2" to the filename. Make some changes. And then email it back to me.

I'd save a "v3", make my changes and email it back...

All the while, we both got considerably older and our children sat at home crying, because we were never there any more...

If there's been one benefit to this pandemic, it's that the collaboration tools have got better and more of us are using them.

Whether you use Teams, Slack, Google Docs or one of the many hundreds of pieces of clever software around, you'll be enjoying the benefits while your team are remote working.

I think we'll start to see these software packages integrating more closely with other software you rely on. For example, Outlook reminders now have a "join meeting" button to launch a Teams video call.

Microsoft is already well integrated, and it's moving further down this route at speed. Others will follow. The more your various pieces of software are integrated, the less friction there is for you.

I'd always love to talk about your business. You can reach me at sales@ashdownsolutions.co.uk or on 01342 363000.

Kind Regards,

Tony Baulch

Founder & Technical Director

DID YOU KNOW?

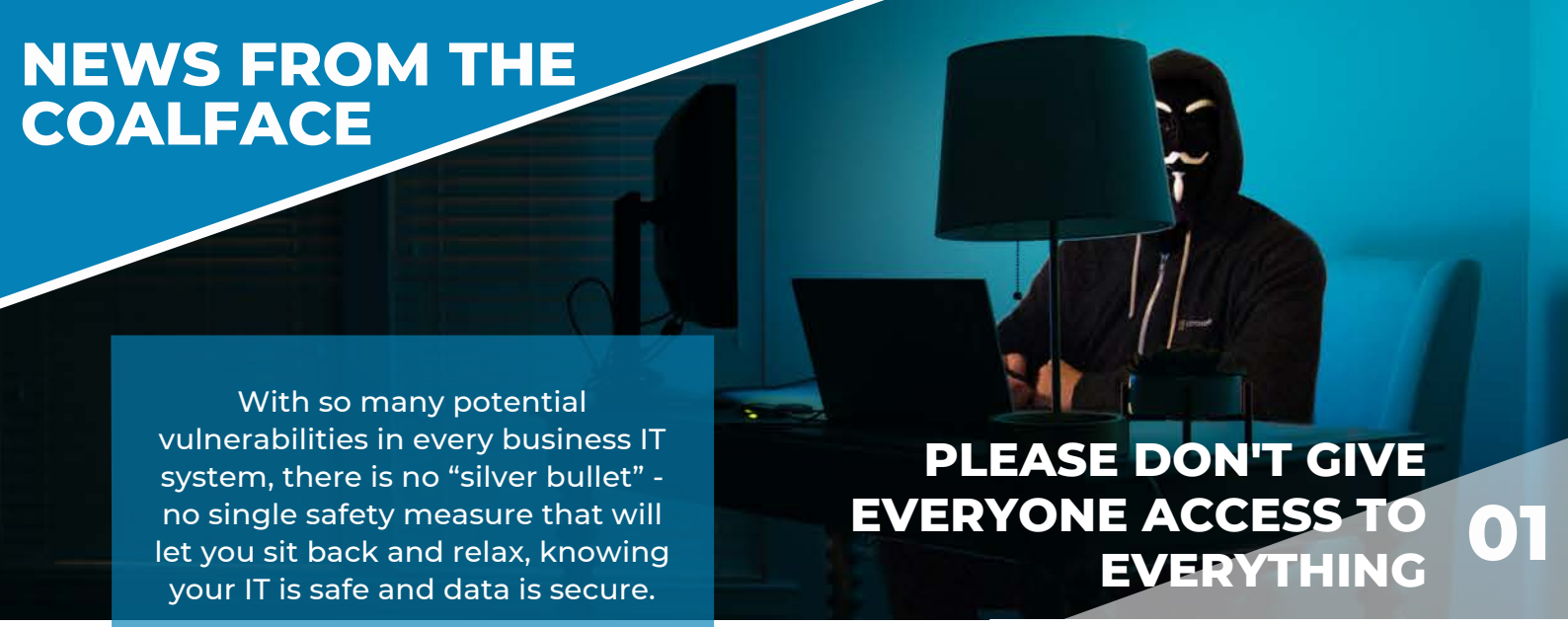
The first chatbot was developed by MIT professor Joseph Weizenbaum in 1966. Called ELIZA, it was driven by a script called DOCTOR and replied to people like a psychotherapist would.

He was shocked by how many people opened their hearts to ELIZA. His secretary even asked him to leave the room when she was speaking with it...

Ashdown Solutions Limited

East Grinstead
West Sussex
RH19 4LZ
www.ashdownsolutions.co.uk
01342 363000

NEWS FROM THE COALFACE



PLEASE DON'T GIVE EVERYONE ACCESS TO EVERYTHING

01

With so many potential vulnerabilities in every business IT system, there is no “silver bullet” - no single safety measure that will let you sit back and relax, knowing your IT is safe and data is secure.

Most of the risks are ongoing and constantly changing. They need an active approach to stop your business falling victim to a data breach or malicious cyber-attack.

It would take a lot more space than is available in this newsletter to talk about all the risks you face.

So instead, we can talk about two of the most important things you can do to stay safe.

MAKE SURE YOUR TEAM ONLY HAS ACCESS TO THE DATA IT NEEDS

Keep an eye on who has access to what, and whether they need it.

The more people have access to sensitive data, the more potential routes there for the wrong people to get access to it.

If you give everybody access to everything, all it will take is for one account to become compromised. And before you know it criminals armed with malware will have access to your systems.

Just as important as this is how you manage the IT accounts of people who leave the business or change jobs internally. For example, if an employee switches from accounting to a management job in a completely different part of the business, they probably won’t need to keep access to all the data they needed for their last role.

Failing to adjust permissions only adds to your level of risk.

When people leave your business, you must immediately restrict their access to your systems and data. Implement appropriate policies and processes to reduce the risk of something slipping through the net.

KEEP YOUR DEVICES SECURE

Another important thing to watch out for is how frequently you’re installing updates on devices. This includes tablets and phones as well as computers.

They must all be kept updated with the latest security patches. Because all it takes is one weak link for your whole business to potentially be compromised.

Make sure that you replace old devices that are no longer getting updates, or can’t support the latest versions of software.

And of course, it’s also important to make sure that all devices are backed up in real time. Plus encrypted turning the data into unreadable garbage if the wrong person gets hold of your device.

02 TURN YOUR BIGGEST CYBER-SECURITY THREAT INTO YOUR BEST LINE OF DEFENSE

Your employees are your number one cyber-security threat. A sad fact, but true.

They're often the main gateway through which hackers try to worm their way into your business. After all, it only takes one click on one wrong link in an email, for cyber-criminals to get in.

But your staff can also be your best protection against threats.

Turning your team from a security risk into your most important line of defense isn't as difficult as you may think.

The most important step is to train them all properly. Cyber-security training, whether it's delivered through an e-learning module or face-to-face session, should be a compulsory part of their onboarding process – with ongoing training and refreshers.

Building a culture of awareness and vigilance is one of the best things you can do to protect your business.

For example, educating staff on the risks of opening suspicious email attachments will make them pause and think twice before opening emails they're not 100% sure about. It can also be useful to share details about attempted attacks so they can see the risks are real, ongoing, and what they look like.

It's also a good idea to write a formal information security policy that all employees need to read and sign. This should set out, in clear and direct terms:

- Best practice
- What needs to be avoided
- And the procedures employees need to follow to reduce data security risks.

Your policy should also explain what actions people need to take if they suspect there's been a cyber-security incident.

It's key to act fast and make the right people aware the moment anything suspicious happens. Steps can then be taken to reduce the risk of a serious incident developing by fixing gaps in your systems, or making other employees aware of an emerging threat.

This can be especially important if criminals are targeting individuals by impersonating somebody known to the business, like a senior manager or a major supplier. Attacks like this have a nasty habit of hitting several people at the same time with similar techniques.