TECHNOLOGY INSIDER

Your monthly newsletter, written for humans, not geeks

Here's why you need to automate more, now

Most staff loves automation.

Because it's about automatically creating rules that people and software can follow, and humans don't need to do tedious and repetitive tasks.

Who in your business would be against that?

As well as saving you and your employees valuable time, automation has loads of other benefits for a business.

You should see a productivity boost as people can get more done in the same amount of time. It also increases motivation and improves job satisfaction.

That's because your staff is enjoying their work and feel more listened to as you've made their jobs better, and you will reward that with increased loyalty. In addition, recruitment might be more manageable as your reputation gets a boost.

Another benefit of automating tasks is for your customers. Perhaps they can get a response to a question a lot faster. Or maybe have a better experience when they deal directly with you because you have time to take care of them.

So which tasks within your business could be automated? Yes, even the most straightforward automation can have a tremendous impact on the way your company operates.

DID YOU KNOW... your **executives** might be your weakest link.

When it comes to cyber security, your executive-level managers might be the least vigilant members of your team.

A recent report showed that 49% of execs had requested to bypass security measures on at least one occasion over the past 12 months.

Suppose you're already regularly training your people in cyber security. But, are you including everyone in the business from the top down? It's one of the best ways to ensure all your people know the risks of skipping vital security steps.

Cybercriminals are targeting home and small office routers to steal sensitive data.

Alan Helbush, Where To Start

Yes, this is a smart move by the bad guys, as these devices exist outside of your business's (in most cases) usual security protection. It means they may have additional weaknesses to exploit.

Why?

Because it gives them a landing spot to observe for interesting tidbits and launch an attack from.

How to protect your data?

Ensure you have the proper firewalls installed so incoming and outgoing traffic are monitored, and the devices can be updated (preferably automatically.

Remote workers should insist they use company-provided devices for work-related items is a good idea. Also, using encrypted connections when working, whether in the office or remotely, is extremely important.

TECH FACTS

#1

A typical person spends an average of 6 hours and 55 minutes online, daily

#2

Nearly three quarters of execs believe AI will be a business advantage in the future

INSPIRATIONAL QUOTE OF THE MONTH

"Just because something doesn't do what you planned it to do doesn't mean it's useless."

Thomas Edison, Inventor, and business legend

#3

20% of Google searches are now done by voice

NEW TO MICROSOFT 365

Just Dreaming about Managing your Outlook signature in one place...

You know when you set an email signature in Outlook on one device, but when you use Outlook on the web, the signature isn't there?

It's a frustration that's been around for years. Traditionally the solution has been to use independent software to manage your signatures.

But Microsoft is hard at work changing the way it stores signature settings. It moves them to the cloud, giving you a consistent experience wherever you use Outlook.

This feature will go into testing this month and be available next month... although it's been delayed for a couple of years up to this point, so... watch this space.

IT'S TIME FOR ANOTHER MONTHLY QUIZ!

Winner gets bragging rights for 30 days.

1. How many generations of computer have been invented (so far)?
2. What does CPU stand for?
3. Which company designed the first CPU?
4. What's the name of the information storage used to store short-term running programs and data in a computer?
5. Which company invented the USB port?

The answer are below.

1) Five. The first generation started in 1940 with the vacuum tube. Our current generation is starting to use AI
2) Central Processing Unit
3) Intel
4) RAM (Random Access Memory)
5) It's Intel, again. The first USB-compatible product was a Mac in 1998, followed by USB support for Windows 98 a year later. The rest is history

Who's to blame for a cyber security breach?

We all know how dangerous a cyber security breach can be for a business. And just how many businesses are being breached right now.

In truth, we hate having to write this. We don't want to feel like we're scaring you or being all doom and gloom!

But it's essential that you're fully aware of the risk to your business if you suffer a breach.

Last year, the number of reported data breaches rose 68% compared to 2020.

And while it's a good idea to implement the proper cyber security tools to help reduce the risk of an attack, it's impossible to give your business 100% protection from an attack just using these tools.

Because according to research, 85% of data breaches have been caused by human error.

If that happens, who's to blame for your cyber security breach? Your employee? Or you, the business owner/manager?

It's a difficult question. Sure, your employee is likely the one to have clicked the link or downloaded a bad file that turned out to be malware. They may even have disabled security features to speed up their work.

However, as the business owner/manager, it should be your responsibility to reduce the risk of that happening in the first place.

It starts with training your people regularly to ensure they understand the risks and how to avoid them. But you should also have the right policies to remind your employees of best practices and what happens if they fail to comply.

Employees are your first line of defense against security breaches. But, they can only ever be as good as your cyber security strategy. So, get that in place, and everyone knows:

- What's expected of them?
- How to avoid the risks.
- Put the proper safeguards in place.
- And what to do if things go wrong.

We say, don't worry about who's to blame. Get your ducks in a row, starting with your cyber security strategy.

We can help, get in touch and start the conversation.

Q: I just closed an Office file without saving it. Please tell me I can get it back?

A: You should be able to recover your file, with a bit of luck. If you saved the document once, AutoSave may have done its job. Otherwise, try using AutoRecover or check your temporary files.

Q: I can't open an email attachment

A: First make sure this is a genuine file – phone the sender to check. Then, it's possible you don't have the software the file was created with. Right click the document and select 'Open With' to see if there's another option.

Q: I've had an email telling me an account needs updating. Is it genuine?

A: Don't click any links in the email. If you're even slightly unsure, the safest thing is to visit the website by typing the URL into your web browser.

Business gadget of the month

Using more than one monitor can help make you more productive. But it's not always convenient if you work on a laptop from multiple locations. Enter the Trio from Mobile Pixels Inc.

It's a portable monitor that attaches to the back of your laptop, giving you another screen. Add two Trios, and you have a three-screen setup you can use anywhere.

WHERE TO START
TECHNOLOGY SOLUTIONS

To Set up a 15-minute exploratory video chat , visit
www.WTSci.com/AlanHelbush
or scan this QR code.

How can you get in touch with us:

(844) 727-6448 | hello@WTSci.com | www.WTSci.com

If you like what you see in our newsletter, visit www.WTSci.com/Newsletters for the complete library

Alan's Calendar