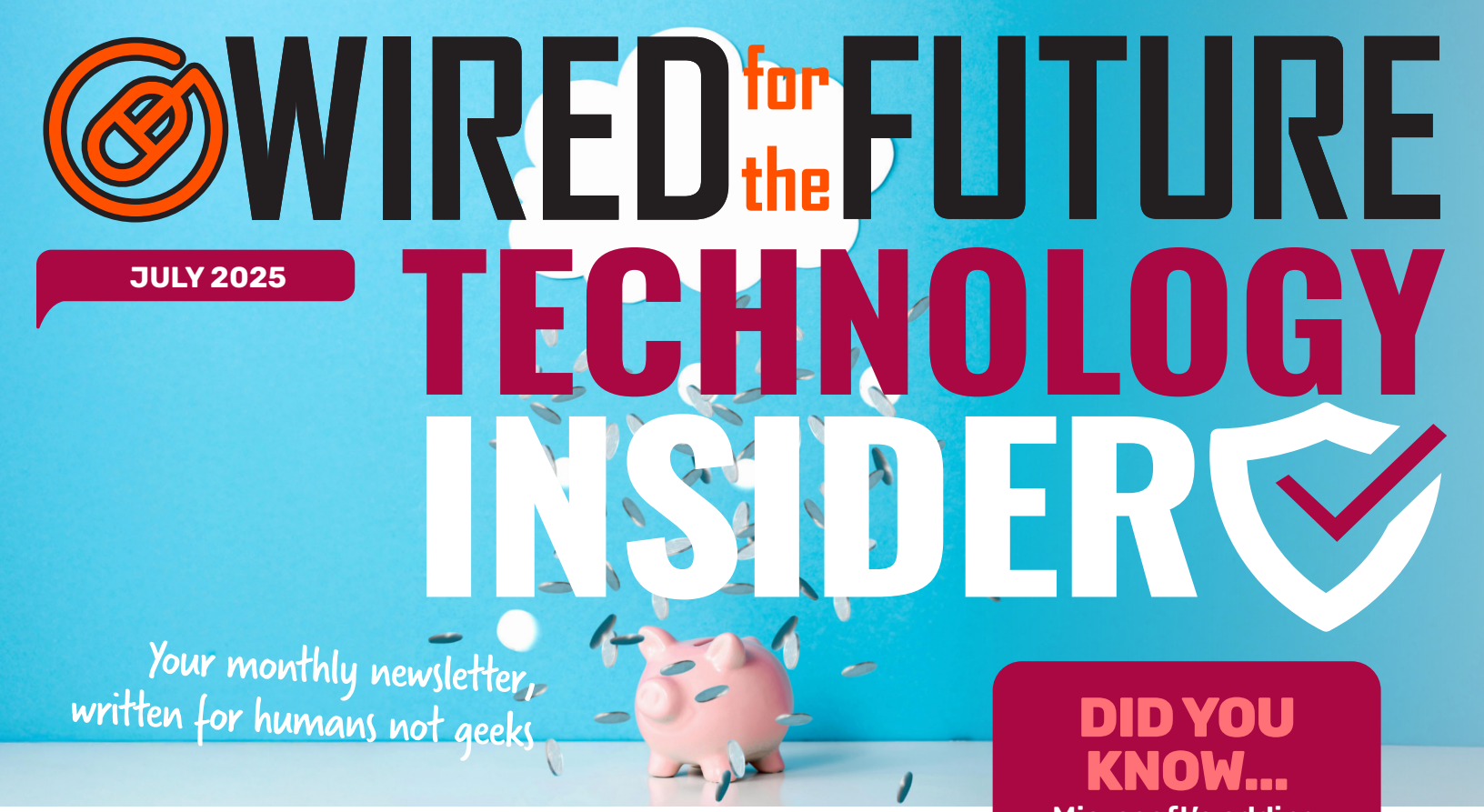
WIRED for the FUTURE

JULY 2025

TECHNOLOGY INSIDER

Your monthly newsletter, written for humans not geeks



Does your business **spend more on cloud storage than you realize?**

Does your business use cloud storage?

That's storing files and data online instead of on your own computers.

There's a good chance you're spending more than you need to be. And the biggest problem isn't how much space you're using… it's the hidden fees.

One of the main culprits is something called egress fees. These are charges you pay when you want to move your data away from your current cloud provider or access it in certain ways. In simple terms, you're being charged just to use your own data. It's like paying a fee every time you open your own storage cupboard.

These costs add up quickly. And they're making it harder for businesses to stay within budget.

Recent research found that almost half of what a company pays for cloud storage goes toward these fees… NOT the actual storage itself.

And the result?

Most businesses end up overspending on their cloud storage plans. Only a small percentage manage to stay under budget.

This pricing model makes it tricky to switch providers even if better or more affordable options are available. That's why so many businesses stick with their current provider. Not because it's the best choice, but because it's too expensive to move.

To keep costs under control, many businesses are now choosing a hybrid approach to storage. That means using a mix of cloud services and local, on-site storage (like servers or hard drives you own). It gives you more flexibility. And it can help you avoid some of those expensive cloud fees.

The key takeaway?

Cloud storage isn't always as straightforward – or as affordable – as it seems. If you haven't taken a close look at your cloud costs lately, it's worth reviewing them.

Understanding where your money is going can help you make smarter decisions and avoid paying for things you don't need.

Not sure where to start? We can help you make sense of it all and keep your storage spending in check. Get in touch.

DID YOU KNOW...

Microsoft's adding a new way to block risky devices

Microsoft's testing a new safety feature in its Defender for Endpoint security software.

It's designed to spot and block devices that are connected to your network but haven't been set up properly or aren't being protected. These "undiscovered" devices are a big risk because hackers can use them to get into your systems without being noticed.

The new feature automatically blocks any data going to or from these devices. Kind of like cutting off a suspicious stranger before they can cause any trouble. If a device gets blocked by mistake, there'll be a button to undo it.

The feature isn't live yet, but it'll be available soon for supported Windows devices.

The real cost of a security breach (it's not just about money)

We hear about security breaches all the time. But it's easy to think, "That won't happen to us."

Unfortunately, the truth is… it could.

And if it does, the costs to your business go far beyond fixing a few systems or paying a fine.

Cyberattacks have become more frequent, more sophisticated, and more damaging.

As more businesses move their data online, rely on cloud services, and encourage remote work, their networks become easier to target.

And attackers know it.

When a business suffers a breach (where someone gains unauthorized access to your data) the immediate impact might include lost revenue, a damaged reputation, or a big regulatory penalty.

But the real damage often appears over time.

Take this in: The average cost of a serious security breach is now estimated at nearly $600 million. That includes everything from fixing systems, legal fees, lost business, and customer support. It's a huge jump from just a year ago, and it shows no signs of slowing down.

But it doesn't stop at finances.

Businesses that are breached often see a drop in customer trust. People may take their business elsewhere, unsure if their data is safe. In some cases, the business's value drops as investors lose confidence. Even applying for funding or planning future growth becomes harder.

It gets worse in sectors like healthcare or finance, where a breach can delay operations, expose personal records, and cause real harm to people. That kind of disruption can ripple far beyond just the business itself.

The bad news is: Cyberthreats aren't going away.

The good news?

There's a lot you can do to reduce the risk. A strong security setup, smart employee training, and a plan for how to respond to an attack can make all the difference.

If you're not sure how protected your business is, don't wait for something to go wrong.
Let us help, starting with a security audit. Get in touch.

Q: What's the difference between backing up my data and syncing it?

A: Syncing keeps files up to date across devices. Backup means creating a separate copy in case something goes wrong. You need both to stay safe.

Q: We use Microsoft 365. Does that mean we're automatically protected from cyberthreats?

A: Not quite. Microsoft 365 has some great built-in tools, but you still need extra security layers like backup, security software, and staff training.

Q: How do I know if our Wi-Fi is secure enough?

A: Make sure you're using a strong password, up-to-date hardware, and modern encryption like WPA3. And ALWAYS change the default router settings.

NEW TO MICROSOFT

New spell check feature for Teams

Tired of making embarrassing typos in Teams messages?

Microsoft's rolling out an improved spell check for Teams that highlights mistakes as you type and suggests quick fixes. Just like in Word.

You can choose a correction, ignore it, or add your own words to the dictionary. It also supports switching between up to three languages (though we don't yet know which ones).

It's available now on Windows and Mac.

This is how you can get in touch with us:

CALL: 416.572.3805 | **EMAIL:** info@wiredforthefuture.com
WEBSITE: wiredforthefuture.com

WIRED for the FUTURE