WIRED for the FUTURE TECHNOLOGY INSIDER

APRIL 2026

Your monthly newsletter, written for humans not geeks

Would your business survive **a serious cyberattack?**

It's not a comfortable question, and it's one many SMB owners assume they never really need to answer.

Cyberattacks feel like something that happens to other people. Big brands. Global companies. Organizations with huge IT teams and budgets.

The reality is very different.

Recent research shows that a worrying number of businesses believe they simply wouldn't survive a major cyber incident.

That might sound dramatic, but it's a fair reflection of how exposed many businesses still are.

Cyberattacks have changed. They're no longer just a hacker guessing a password. Attacks today are faster, more targeted, and often designed to shut a business down completely.

Ransomware, for example, is a type of attack where criminals lock your systems and demand payment to unlock them. If you can't access your data, your systems, or your customer information, normal business stops very quickly.

What's interesting is that most business leaders know the risk is rising. Many openly admit they expect their staff to fall for a phishing attack.

Phishing is when a fake email or message pretends to be legitimate, tricking someone into clicking a link or handing over login details.

That single mistake can be all an attacker needs.

Despite this awareness, the basics are still being missed.

Password reuse is a big one. If someone uses the same password at work and across multiple personal accounts, one breach can quickly turn into many.

Cybercriminals know this, which is why stolen passwords are so valuable.

Basic cyber awareness training is another gap. Many employees have never been shown what to look out for or how to spot common scams.

But it's not all doom and gloom. High-profile attacks have made business owners more alert, especially around newer threats like AI-driven scams and deepfake video calls that pretend to be senior leaders. That growing skepticism is healthy.

The most important thing to understand is that surviving a cyberattack doesn't need expensive tools or complex technology.

Preparation is your best tool.

Simple steps like strong, unique passwords and regular staff training make a real difference.

Do you think your business would survive a serious cyberattack? If you're not sure, we can help you strengthen your defenses. Get in touch.

DID YOU KNOW...

Microsoft wants to be a good neighbor?

AI data centers continue to pop up around the world. It comes as no surprise that some communities are starting to ask questions.

These facilities can place heavy demands on local electricity, water supplies and land, which has raised understandable concerns.

In response, Microsoft has announced a new "Community-First AI Infrastructure Plan". It promises to be a better neighbor by covering infrastructure costs, reducing and replenishing water use, being open with communities, and investing in local jobs, training and services wherever new data centers are built.

The real reason you're struggling with AI

AI has become a regular topic in business conversations.

It comes up in meetings, strategy days and vendor pitches.

Yet for all the talk, many organizations are still struggling to turn AI from an interesting idea into something that genuinely helps people do their jobs.

In many organizations, AI is stuck in a trial phase.

Someone experiments with a tool. A small pilot runs for a few weeks. Then progress slows. The AI works, but businesses struggle to move from experimentation to everyday use. The return on investment everyone expects stays just out of reach.

Uncertainty is usually to blame.

Leaders worry about security, privacy and compliance. They're unsure what data AI tools are allowed to see or how decisions are being made. Others admit they don't yet have a clear business case, so AI becomes something interesting rather than something essential.

Another big factor is confidence.

Many employees are curious about AI, but also nervous. They worry about making mistakes, relying on the wrong answers, or using tools incorrectly.

Without clear guidance, people either avoid AI altogether or use it quietly and inconsistently. That creates risk and limits the benefits.

It's a shame, because when AI is used properly, the gains are very real. Teams can respond to customers faster, spot issues earlier, analyze data more easily and reduce time spent on repetitive admin.

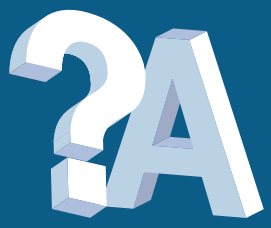
In technical areas, AI can help monitor systems, improve security, and surface problems before they turn into outages. These are practical, everyday improvements that add up quickly.

The businesses seeing progress tend to take a steady, human-first approach. They set clear rules around how AI should be used, what it can and can't do, and where human judgment still matters. They focus on giving staff training and reassurance, not just new tools.

AI becomes a support act, not a replacement.

AI projects don't usually stall because the technology isn't ready. They stall because people aren't.

If you need help giving your team the confidence to use AI effectively, **Get in touch.**



Q: Should we use AI tools in our business, or wait until things settle down?

A: Start now. The key is using approved tools, setting clear rules, and making sure data is protected.

Q: What does zero trust mean?

A: It's a security approach where nothing is trusted by default. Every person and device must prove who they are every time.

Q: Do we need to control which apps staff can install?

A: Yes. Unapproved apps may store data insecurely or create hidden risks. A managed app list keeps everything safer and easier to support.

Microsoft Patch Reveals New AI-Driven Attack

Microsoft's security update highlights how quickly AI is changing the threat landscape. A newly patched Excel vulnerability showed that attackers can combine traditional exploits with AI tools like Copilot to launch "zero-click" attacks, meaning data could be exposed just by previewing a file.

At the same time, Microsoft is rolling out stronger AI-powered defenses, including deeper integration between Copilot and security platforms like Sentinel to improve visibility and automate threat detection.

This is how you can get in touch with us:

CALL: 1-844-572-WFTF (9383) | **EMAIL:** info@wiredforthefuture.com

WEBSITE: wiredforthefuture.com

WIRED for the FUTURE