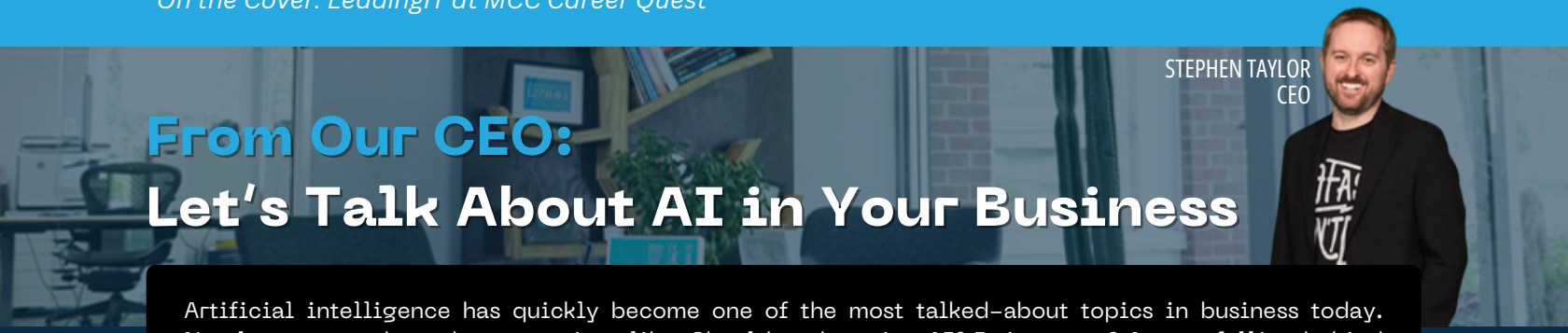
LeadingIT

May 2026

The NetWork

IN THIS EDITION:



STEPHEN TAYLOR
CEO

From Our CEO:
Let's Talk About AI in Your Business

Artificial intelligence has quickly become one of the most talked-about topics in business today. Nearly every week, we hear questions like: Should we be using AI? Is it secure? Are we falling behind if we're not?

The reality is, AI does not need to be complicated.

At its core, AI is simply software. It is powerful software, but software nonetheless. It belongs in the same category as the tools your organization already relies on every day, whether that is email, accounting systems, or your CRM. Just like those tools, AI should be evaluated, implemented, and managed with intention.

Choosing the Right AI Tools

Not all AI platforms are created equal. Established platforms like ChatGPT, Claude, Gemini, and Grok are investing heavily in security, privacy, and enterprise-ready features. These tools are built with business use in mind.

At the same time, there are countless lesser-known tools entering the market, many of which lack the safeguards and transparency organizations should expect.

This is no different than any other category of software. Just as businesses standardize on trusted platforms like Microsoft 365 or Google Workspace, the same level of scrutiny should be applied when selecting AI tools.

Understanding the Risks of Free AI

One of the most important considerations when adopting AI is how your data is handled.

Free versions of AI tools often come with trade-offs. In many cases, the data entered into these tools may be used to improve the platform unless specific settings are adjusted. For businesses, this introduces unnecessary risk.

Paid, business-grade AI platforms are designed differently. They typically include stronger data protection and do not use your company's information for training purposes by default.

As a general rule, if a tool is free and internet-based, it is important to understand how your data is being used before integrating it into your operations.

AI Within Your IT Environment

From a technology management perspective, AI does not change the fundamentals of IT. The same best practices still apply:

- Layered cybersecurity protections
- Controlled user access
- Consistent system updates
- Continuous monitoring

AI tools should be incorporated into your environment just like any other application. Organizations should have clear standards around which tools are approved, which are restricted, and how they are used.

Whether it is limiting certain file-sharing platforms, standardizing communication tools, or restricting specific AI applications, these decisions should align with your broader IT and security strategy.

Where AI Delivers Real Value

While the technology itself is important, the true value of AI comes from how it is used. The people within your organization, those who understand your processes, your customers, and your day-to-day operations, are best positioned to identify where AI can make a meaningful impact.

AI is not a replacement for your team. It is a tool that can enhance productivity, improve efficiency, and support better decision-making when applied thoughtfully.

Your IT partner plays a critical role in guiding, securing, and managing these tools. But the direction and impact should always be driven by your business goals and your team's expertise.

Moving Forward with Confidence

AI represents a significant opportunity for businesses willing to approach it strategically. With the right tools, proper safeguards, and a clear understanding of how it fits into your operations, AI can become a powerful advantage, not a risk.

As with any technology, success comes down to alignment. Align your tools with your goals, your security with your standards, and your strategy with the people who make your business run.

When those pieces are in place, AI becomes just another way to move your organization forward.

Why Are Password Changes Required?

Few things are as universally annoying as the "Please update your password" notification. But there's a reason it keeps showing up, and it's worth understanding why.

Everything from your bank account to your business applications lives online. Passwords are the first line of defense against unauthorized access, and even the strongest ones weaken over time. According to a GoodFirms survey, 30% of IT professionals reported experiencing a data breach due to weak passwords. That's not a hypothetical risk. It's happening regularly.

Why Passwords Get Less Secure Over Time

Sticking with one password forever is like leaving your door unlocked because it hasn't been kicked in yet.

Three common threats make old passwords increasingly dangerous:

- **Data breaches:** In 2024 alone, data breaches resulted in over one billion records being exposed. When companies get hacked, stolen passwords often end up on the dark web. If yours hasn't been updated, you could be an easy target.
- **Brute-force attacks:** These attacks use software to guess your password by trying every possible combination. The longer a password stays unchanged, the higher the odds it gets cracked.
- **Phishing:** If you've ever been tricked into entering your password on a fake website, the attacker could keep using that credential until you change it.

How Regular Updates Help

Changing your passwords regularly disrupts even the most persistent attackers. Once you've updated a compromised credential, the old one becomes useless.

Some industries don't just recommend this, they require it. Financial institutions and healthcare providers often mandate password rotations to meet strict compliance standards like HIPAA and PCI. It's not about being annoying. It's about protecting sensitive information.

What a Strong Password Looks Like

When you do update, make sure the new password actually improves your security:

- Make it strong and unique: Use a mix of uppercase and lowercase letters, numbers, and symbols. Avoid predictable patterns like "1234" or names.
- Use a password manager: A reputable password manager stores and organizes your credentials safely, so you don't have to memorize every one.
- Turn on multi-factor authentication (MFA): MFA adds an extra layer of verification. Even if someone steals your password, they still need a second factor to get in.

The Bottom Line

Changing your passwords can feel like a chore, but it's a small step that significantly reduces the chances of your information being compromised. Staying one step ahead is your best defense.

If your organization needs help building stronger password policies or implementing MFA across your systems, contact LeadingIT to get started.

Cybersecurity Best Practices: What Every SMB Actually Needs

"Cybersecurity best practices" gets thrown around so often it starts to lose meaning. What does it actually look like for a business with 25 to 200 employees? It means having a strategy, not just a collection of tools. And it means understanding that the cost of getting this wrong is not abstract.

According to IBM's 2025 Cost of a Data Breach Report, the average data breach now costs $4.44 million globally. For small and mid-sized businesses, those numbers can be existential.

Here are the fundamentals that consistently separate businesses that get breached from those that don't.

Start With an Assessment

Before investing in tools or training, you need to understand your current security posture. A cybersecurity risk assessment identifies where your vulnerabilities are, which assets matter most, and where your defenses have gaps. Without one, you risk spending money on protections that don't address your actual risks.

Train Your People

Human error is involved in 74% of data breaches according to Verizon's DBIR. No technology stack can compensate for employees who can't recognize a phishing email or who reuse passwords across personal and business accounts. Effective training starts during onboarding and continues with regular refreshers and simulated phishing tests throughout the year.

Fix Passwords and Enable MFA

Weak or stolen passwords are involved in more than 80% of hacking-related breaches. Every business account should use strong, unique passwords, and a password manager makes this practical at scale. Multi-factor authentication blocks over 99% of automated attacks according to CISA and should be enabled on every business-critical system.

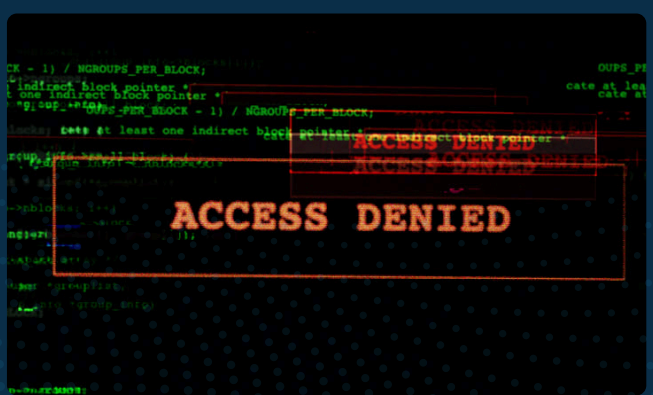
Patch Your Software

Unpatched software remains one of the easiest ways for attackers to get in. Exploited vulnerabilities are the number one root cause of ransomware attacks, responsible for 32% of incidents according to Sophos. Establish a patch management policy with automated tools that keep systems current, and replace end-of-life systems that no longer receive security updates.

Back Up Everything That Matters

Reliable backups are what allow you to recover from a ransomware attack without paying the ransom.

Back up critical data multiple times per day, store backups on separate servers so ransomware can't destroy your production systems and backups simultaneously, maintain geographic redundancy through cloud backups, and test your restores regularly.



Control Who Has Access

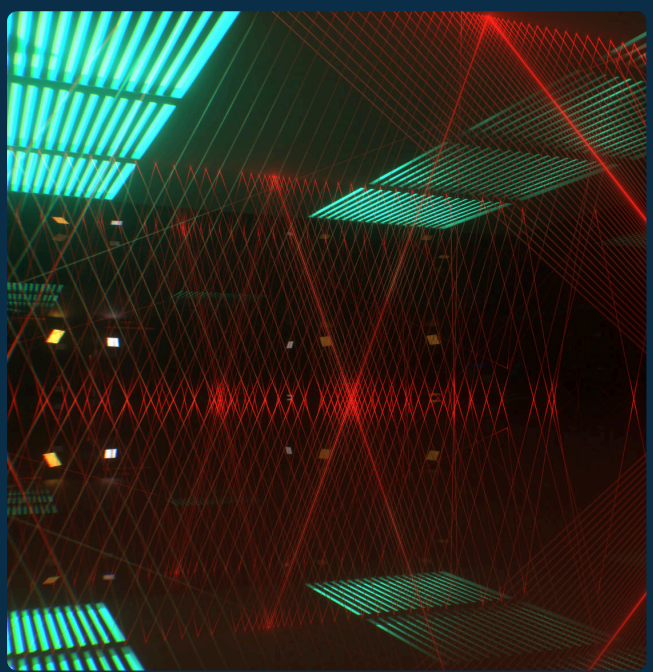
The principle of least privilege means every user should have access only to the systems and data they need for their role.

Tightly control administrative rights, and make sure offboarding triggers an immediate access revocation process covering email, cloud accounts, VPN, and physical access.

Layer Your Defenses

A single security tool is never enough.

Effective cybersecurity requires multiple layers: endpoint detection and response (EDR), managed firewalls, email security with anti-phishing, dark web monitoring, and network logging. Each layer catches what the previous one missed.



The Bottom Line

Cybersecurity isn't a product you buy once. It's an ongoing discipline that touches people, processes, and technology. The businesses that stay protected are the ones that treat it as a core operational priority, not a back-office afterthought.

If you're not sure where your business stands, a risk assessment is the best place to start.

Contact LeadingIT or schedule a free cybersecurity consultation to identify your vulnerabilities and build a plan to address them.

What Are the 4 Types of Network Cable? A Quick Guide

Not all network cables are created equal, and the one running through your walls has a direct impact on your speed, reliability, and how well your infrastructure handles growth. Here's a quick breakdown of the four main types and when each one makes sense.

1. Coaxial Cable

Coaxial cables contain a copper conductor surrounded by insulation and metal shielding that blocks external interference. While common in early computer networks, they're now primarily found in cable television and internet connections. Unless you're maintaining a legacy system, coaxial cable likely isn't part of your current network infrastructure.

2. Unshielded Twisted Pair (UTP)

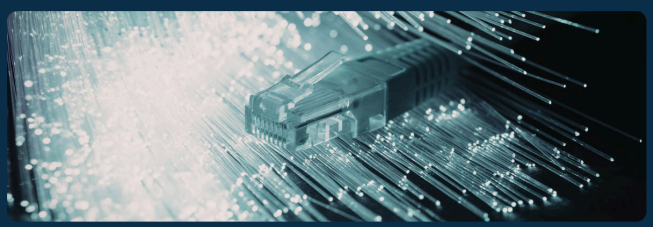
UTP is the workhorse of modern business networks. These cables contain pairs of wires twisted together, and that twisting naturally reduces interference without requiring additional shielding. UTP comes in categories like Cat5e, Cat6, and Cat6A, each supporting different speeds and distances. According to Market Reports World, **Category 6A cables accounted for 40% of global demand** in 2023, reflecting the shift toward higher-performance wired connections.

For most office environments, UTP is the right fit. It balances performance with affordability and handles standard business applications without issue.

3. Shielded Twisted Pair (STP)

STP cables add metal foil or braided shielding around the twisted pairs, providing extra protection against electromagnetic interference. This makes them more expensive than UTP, but essential in environments with heavy electrical equipment, such as manufacturing plants, hospitals, and industrial facilities.

If your office sits next to heavy machinery or you operate in a building with significant electrical interference, STP is worth the investment.



4. Fiber Optic

Fiber optic cables transmit data as light pulses through glass or plastic strands instead of electrical signals through copper. This delivers the fastest speeds and longest transmission distances of any cable type. Fiber comes in two varieties: single-mode for long distances and multi-mode for shorter distances with higher bandwidth.

Fiber is the go-to for data centers, building-to-building connections, and network backbone infrastructure where performance is the top priority. It costs more, but for high-demand environments, nothing else comes close.

How to Choose

The decision comes down to your environment and what your network needs to support:

- Standard office network: UTP (Cat6 or Cat6A) handles most business workloads reliably and affordably
- Industrial or high-interference environment: STP provides the shielding necessary for clean data transmission
- High-performance or long-distance needs: Fiber optic delivers unmatched speed and distance

Proper cabling is one of those infrastructure decisions that's easy to overlook and expensive to fix later. Getting it right from the start saves time, money, and headaches down the road.

If your organization is planning a buildout, office move, or network upgrade, contact LeadingIT to make sure your cabling supports where your business is headed.

$1000 REFERRAL PROGRAM

Do you know an organization that needs unlimited IT and cybersecurity support with an unbeatable guarantee?

You'll earn **$50** for every referral. If they sign up, you'll receive **$1000!**

SCAN TO LEARN MORE

815-788-6041 GOLEADINGIT.COM/REFER

We're excited to welcome Jane Pearre

as LeadingIT's new Director of Operations. As our new Service Delivery leader, Jane brings a strong focus on creating an exceptional customer experience. She is passionate about making support fast, friendly, and reliable every single time.

Jane also cares deeply about building a strong team culture. She believes in empowering people, earning trust, and helping team members do their best work so they can better serve our clients.

We are excited for the leadership, energy, and client-first mindset Jane brings to LeadingIT, and we know our clients and team will feel the positive impact.