VOLUME 65
MARCH 2026

Tech Talk

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE:

We love technology and we love helping people.

Give me a call today for a quick (non-salesy) chat to find out whether my team and I can help you better secure your data and get more out of your existing Technology!

Mark Giles

BEYOND CHATBOTS: PREPARING YOUR SMALL BUSINESS FOR "AGENTIC AI" IN 2026

AI chatbots can answer questions. But now picture an AI that goes further, updating your CRM, booking appointments, and sending emails automatically. This isn't some far-off future. It's where things are headed in 2026 and beyond, as AI shifts from reactive to proactive, autonomous agents.

This next wave of AI is called "Agentic AI." It describes AI that can set a goal, figure out the steps, use the right tools, and get the job done on its own. For a small business, that could mean an AI that takes an invoice from inbox to paid, or one that runs your whole social media presence. The upside is massive efficiency, but it also means you need to be prepared. When AI gets more powerful, having the right controls matter.

What Makes an AI "Agentic"?

A research article on the evolution and architecture of AI agents explains the big shift like this: AI is moving from tools that wait for instructions to systems that work toward goals on their own. Instead of just helping with tasks, AI starts doing the work, making it possible to hand off whole processes and collaborate with it like a teammate.

The 2026 Opportunity for Your Business

For small businesses, this is about real leverage. Agentic AI can work around the clock, clear out repetitive bottlenecks, and cut down errors in routine processes. That means things like personalizing customer experiences at scale or even adjusting supply chains in real time become possible.

And this isn't about replacing your team. It's about leveling them up. AI takes the busywork so your people can focus on strategy, creativity, tough problems, and relationships, the things humans do best. Your role shifts too, from doing everything yourself to guiding and supervising your AI.

What You Need Before You Launch Agentic AI

Before you hand over your processes to an AI agent, you need to make sure those processes are rock solid. The reasoning is simple: AI will amplify whatever it touches, order or chaos, with equal efficiency. That's why preparation is key. Start with this checklist:

1. **Clean and Organize Your Data:** AI agents make decisions based on the data you give them. Garbage in means not just garbage out; it can lead to major errors. Audit your critical sources.
2. **Document Workflows Clearly:** If a human can't follow a process step by step, an AI won't be able to either. Map out each workflow in detail before you

Building Your Governance Framework

Just like with human team members, delegating to an AI agent requires oversight. That means setting up clear guardrails by asking a few key questions:

- What decisions can the AI agent make on its own?
- When does it need human approval or guidance?
- What are its spending limits if it handles finances?
- Which data sources is it allowed to access?

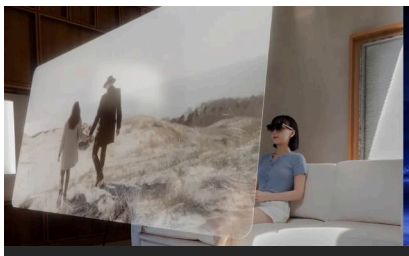
Answering these questions lets you build a framework that becomes your company's rulebook for its "digital employees."

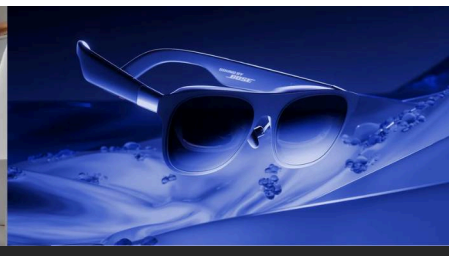
Security is another critical piece. Every AI agent needs strict access controls, following the principle of least privilege. Regular audits of agent activity are now a non-negotiable part of good IT hygiene.

Embracing the Role of Strategic Supervisor

Agentic AI is a true force multiplier, but it depends on clean data and well-defined processes. It rewards careful preparation and punishes the hasty. By focusing on data integrity and process clarity now, you position your business not just to adapt, but to lead.

Contact us today for a technology consultation on AI integration. We can help you audit workflows and create a roadmap for reliable, effective adoption.





XREAL 1S AR GLASSES

XREAL 1S packs a stunning micro-OLED display, a wider 52-degree field of view, and crisp 1200p resolution into a comfortable, sunglasses-style frame built for everyday use.

With plug-and-play support for phones, laptops, consoles, and handheld gaming devices, you can enjoy a massive virtual screen anywhere. It delivers smooth 120Hz visuals, Bose-tuned speakers, and simple on-device controls, making it effortless to switch between gaming, streaming, or productivity on the go.

THE HYBRID STRATEGY: WHY "CLOUD-ONLY" MIGHT BE A MISTAKE

Since cloud computing became mainstream, promising agility, simplicity, offloaded maintenance, and scalability, the message was clear: "Move everything to the cloud." But once the initial migration wave settled, the challenges became apparent. Some workloads thrive in the cloud, while others become slower, or more expensive. The smart strategy for 2026 is a pragmatic hybrid cloud approach.

A hybrid cloud strategy blends public cloud services like AWS, Azure, and Google Cloud with private infrastructure, whether that's a private cloud in a colocation facility or on-premise servers. The goal isn't to avoid the cloud, it's to use it wisely.

This approach recognizes that one size does not fit all. It gives you the flexibility to place each workload where it performs best, considering cost, performance, security, and regulatory requirements. Treating hybrid as a temporary solution is a mistake, as it is increasingly becoming the standard model for resilient operations.

The Hidden Costs of a Cloud-Only Strategy

Relying on a single model can create blind spots. The cloud's operational expense (OpEx) model is fantastic for variable workloads. but for predictable, steady-state applications, it can cost more over time than a capital investment (CapEx) in on-premise equipment. Data egress fees, the cost of moving data out of the cloud, can lead to surprise bills and create a form of "lock-in."

Performance can also suffer. Applications that require ultra-low latency or constant, high-bandwidth communication may lag if they're forced into a cloud data center far away. A hybrid approach lets you keep latency-sensitive workloads close to home for optimal performance.

The Strategic Benefits of a Hybrid Cloud Model

First, a hybrid cloud strategy is all about balancing resilience and flexibility. For example, during peak periods like a holiday sales rush, you can take advantage of the public cloud's scalability and then scale back to your private infrastructure when demand drops. This approach can significantly reduce costs.

Second, hybrid cloud helps meet data sovereignty and strict compliance requirements. You can keep sensitive or regulated data on infrastructure you control while running analytics or other workloads in the cloud. This setup is often essential for healthcare, government, finance, and legal sectors, where data must remain within a specific legal jurisdiction.

The Path to a Future-Proof IT Architecture

Adopting a hybrid mindset creates a future-proof IT architecture. It reduces the risk of vendor lock-in, preserves capital, and provides a built-in safety net. The cloud landscape will keep evolving, and a hybrid foundation lets you adopt new services without a full rip-and-replace.

The goal for 2026 is intelligent placement, not blind migration. Your infrastructure should be as dynamic and strategic as your business plan, and a blended approach can make that happen.

Reach out today for help designing the hybrid cloud model that best fits your business goals.

ZERO-TRUST FOR SMALL BUSINESS: NO LONGER JUST FOR TECH GIANTS

Think about your office building. You probably have a locked front door, security staff, and maybe even biometric checks. But once someone is inside, can they wander into the supply closet, the file room, or the CFO's office? In a traditional network, digital access works the same way, a single login often grants broad access to everything. The Zero Trust security model challenges this approach, treating trust itself as a vulnerability.

For years, Zero Trust seemed too complex or expensive for smaller teams. But the landscape has changed. Today, it is a practical, scalable defense, essential for any organization. It's about verifying every access attempt, no matter where it comes from. It's less about building taller walls and more about placing checkpoints at every door.

Transform Your Security Posture

Adopting Zero Trust isn't just a technical change, it's a cultural one. It shifts the mindset from broad trust to continuous monitoring and validation. Your teams may initially find the extra steps frustrating, but explaining clearly why these measures protect both their work and the company will help them embrace the approach. The goal is to foster a culture of ongoing governance that keeps Zero Trust effective and sustainable.

Your Actionable Path Forward

Start with an audit to map where your critical data flows and who has access to it. While doing so, enforce MFA across the board, segment your network beginning with the highest-value assets, and take full advantage of the security features included in your cloud subscriptions.

Achieving Zero Trust is a continuous journey, not a one-time project. Make it part of your overall strategy so it can grow with your business and provide a flexible defense in a world where traditional network perimeters are disappearing. Contact us to schedule a Zero Trust readiness assessment for your business.

MANAGING "CLOUD WASTE"

Controlling cloud waste is not just about saving money. Every dollar you save can be reinvested in innovation, stronger security, or your team.

1. Use tagging consistently to make filtering, organizing, and tracking costs easier.
2. Assign every resource to a project, department, and owner.
3. Consider third-party cloud cost optimization tools for deeper insights. They can automatically spot waste, recommend right-sizing actions, and consolidate data into a single dashboard if you're using multiple cloud providers.
4. Automatically schedule non-production environments like development and testing to turn off during nights and weekends.
5. Implement storage lifecycle policies to move old data to lower-cost archival tiers or delete it after a set period.
6. Adjust the size of your servers. If the CPU is used less than 20% of the time, the server is larger than necessary, replace it with a smaller, more affordable option.

IT SECURITY QUESTIONS TO ASK YOUR NEXT VENDOR

- **What security certifications do they hold (like SOC 2 or ISO 27001)?** Reputable certifications provide third-party validation of their security practices.
- **How do they handle and encrypt your data?** Understanding their data lifecycle ensures your sensitive information is protected in transit and at rest.
- **What is their breach notification policy?** A clear policy dictates how quickly you will be informed if a security incident occurs.
- **Do they perform regular penetration testing?** This testing identifies and addresses vulnerabilities before a malicious actor exploits them.
- **How do they manage access for their own employees?** Strict internal access controls prevent unauthorized access to your data by the vendor's staff.

YOUR ESSENTIAL EMPLOYEE OFFBOARDING CHECKLIST

- **Disable network access immediately:** Once an employee leaves, revoke primary login credentials, VPN access, and any remote desktop connections.
- **Reset passwords for shared accounts:** This includes social media accounts, shared email boxes and workspaces.
- **Revoke cloud access:** Remove permissions for Microsoft 365, Google Workspace, Slack, project management tools, and other platforms.
- **Reclaim all company devices:** Have the employee return all company devices and perform secure data wipes before reissuing.
- **Forward emails:** For a smooth transition, forward the employee's email to their manager or replacement for 30 to 90 days, then archive or delete the mailbox.
- **Review and transfer digital assets:** Make sure critical files aren't stored only on personal devices, and transfer ownership of cloud documents and projects.
- **Check access logs:** Review what the employee accessed in the days before leaving. Pay attention to whether sensitive customer data was downloaded and whether it was needed for their work.

TECHNOLOGY TRIVIA

Each month you have a chance to win a $50 Amazon Gift Voucher by being the first person to email us with the answer to our Technology Trivia Question of the Month!

The Question This Month is:

She is considered to be the world's first computer programmer. What is her name?

The first person to email me at mark@phrixus.com with the correct answer gets a $50 Amazon Gift Card!

Last month's answer was *Love Bug*.