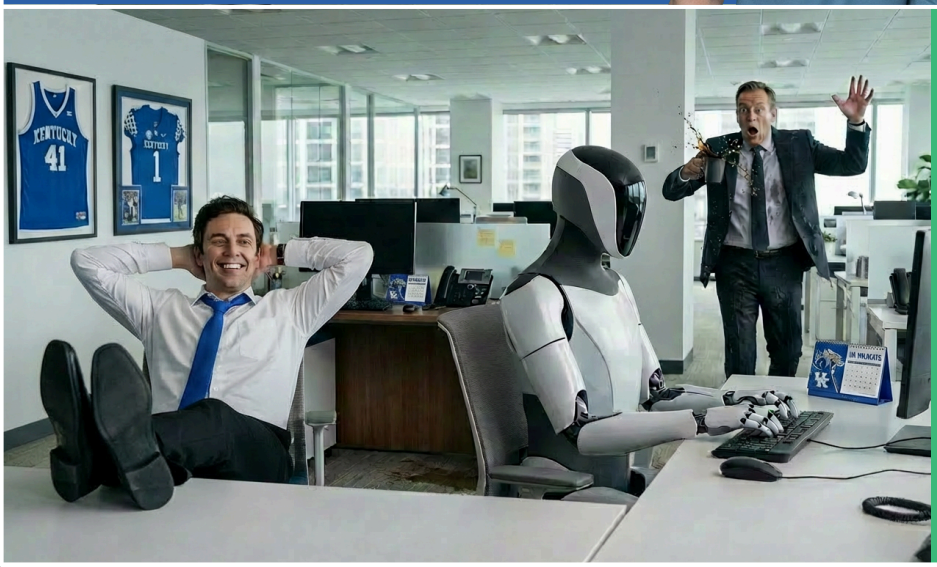
The SimplifIT Advantage

Proven strategies to help leaders make clear technology decisions for measureable business results.



Business leaders depend on technology. SimplifIT allows you to focus on growing your business with secure and compliant IT solutions that are proven to work & keep you safe.

- Craig Willard, COO
- Eric Elder, CTO
- Nick Landers, CMO

SimplifIT MANAGED IT|CYBERSECURITY

A Message From Our Team

As we move deeper into 2026, we're noticing something important: the gap between businesses that plan and businesses that react is widening faster than ever.

The organizations thriving right now aren't the ones with the biggest IT budgets or the newest technology. They're the ones who made IT simple, secure, predictable, and responsive so leadership can focus on growing the business instead of managing technology problems.

This month, we're addressing two realities we're seeing across the region:

First, AI adoption is happening whether leadership approves it or not. That's creating a new risk called "Shadow AI" and most business leaders don't see it until it becomes a security, compliance, or operational problem.

Second, cyber threats are evolving faster than most security stacks can keep up. The tactics that protected you last year aren't enough anymore.

In this issue, we'll show you what Shadow AI actually looks like, how to get the upside of AI without the chaos, and what modern cybersecurity requires in 2026.

If you want clarity on where you stand, and what to do next, we're here to help.

Here's to a strong February!
The Team at SimplifIT

Inside This Issue

A Message From Our Team
PAGE 1

Shadow AI: The Risk Most Leaders Don't See Coming
PAGE 2

Client Spotlight: Curtis Murphy + AI That Saves Money + Strategic Planning
PAGE 3

Modern Cybersecurity in 2026 + Shadow AI Readiness Checklist
PAGE 4

Shadow AI: The Risk Most Leaders Don't See Coming

Most business leaders understand Shadow IT: someone in the organization signs up for a new software tool without telling IT, and suddenly you've got unmanaged accounts, uncontrolled data, and invisible security gaps.

Shadow AI is the same pattern but faster, harder to detect, and higher stakes.

What Shadow AI Actually Is

Shadow AI happens when employees use AI tools—chatbots, meeting recorders, browser extensions, or AI features built into existing software—**to do real business work** without approval, security review, or clear rules about what data can be used.

It typically shows up as:

- Staff copying client emails or contracts into AI tools to draft responses or summaries
- Teams uploading spreadsheets with customer names, pricing, or financial data for analysis
- Departments connecting AI tools directly to email, files, calendar, or CRM systems
- Employees using public AI platforms to rewrite policies, HR documents, or proposals

And it almost always happens with good intentions—people are trying to save time and be more efficient. The problem is that **speed without guardrails creates invisible risk.**

Why Shadow AI Is Dangerous (Real Examples)

1) Data Exposure You Can't Reverse
Once sensitive information leaves your controlled systems, you may not be able to prove where it went, who has access, or how long it's stored. Even data that seems harmless can become harmful when combined with other information.

2) Compliance Violations That Don't Feel Like Violations

- **HIPAA environments**: If any part of your workflow touches protected health information (PHI), using non-approved AI tools can create immediate exposure, especially without Business Associate Agreements (BAAs) or documented controls.
- **CMMC environments**: Defense contractors handling Controlled Unclassified Information (CUI) face strict requirements under NIST 800-171 and CMMC. Using unapproved AI tools with CUI, even for summaries or drafts, can trigger non-compliance findings, contract loss, and loss of certification status.
- **Financial Environments**: Financial institutions must protect customer information under GLBA and meet FFIEC cybersecurity requirements. Using unapproved AI tools with account data, loan information, or personally identifiable financial information creates vendor management gaps, data security violations, and examination findings that can lead to enforcement actions and reputational damage.
- **FTC privacy expectations**: Organizations that promise to protect customer data but route it through unvetted AI tools create a gap that can become legal liability—not just a technical issue.

3) AI Hallucinations Becoming Business Decisions
AI tools can generate answers that sound professional and confident but are completely wrong. When that output becomes a deliverable, policy, contract clause, or HR decision, the cost shows up later as rework, disputes, errors, or legal exposure.

4) Access Sprawl and Permanent Back Doors
Many AI tools request OAuth permissions—access to email, calendar, files, or CRM data. One employee clicking "approve" can create long-term access that doesn't get removed when people change roles or leave the organization.

The Goal Isn't to Ban AI—It's to Secure Speed

The solution isn't locking down every tool and slowing your team. It's giving employees **an approved, secure path** to use AI safely so they get speed and efficiency without creating risk.

Want to know where Shadow AI is already happening in your organization and what to do about it? **Contact us at 502.783.6630** for a Shadow AI Risk Review. No pressure. Just facts and a clear plan.

Cyber Star: Curtis Murphy
A Cyber Star at Bluegrass Community Action Partnership

Every once in a while, we get to work with someone who raises the bar, not just for their organization, but for the people around them.

*That's **Curtis Murphy at Bluegrass Community Action Partnership (BGCAP).***

Curtis is the kind of IT leader every organization hopes to have because he does three things exceptionally well:

1) He helps build layered security
Curtis has been instrumental in implementing a layered cybersecurity strategy at BGCAP. He thinks in systems, not quick fixes. That mindset matters because modern threats don't show up as one obvious problem—they show up as patterns. Layered security is how you catch patterns early.

2) He's a constant learner.
Cybersecurity doesn't stand still. Neither does Curtis. He stays current on best practices, evolving threats, and what "good" looks like in the real world, then turns that knowledge into action inside his organization.

3) He serves with professionalism and a willingness to help.
Curtis shows up for his organization, his team, and his industry peers. He's steady, responsive, and thoughtful—exactly what you want when the pressure is high and decisions matter.

We're grateful for the partnership with Curtis and the team at BGCAP. This is what proactive IT leadership looks like.

***About BGCAP:** Blue Grass Community Action Partnership serves Anderson, Boyle, Franklin, Garrard, Jessamine, Lincoln, Mercer, Scott, and Woodford Counties. Their organization is dedicated to providing a comprehensive range of essential services designed to combat poverty and promote self-sufficiency. These services encompass Head Start, Daycare, LIHEAP for home energy and utility assistance, home weatherization, education and employment assistance, financial coaching, housing counseling, Kynect, medical and affordable public transportation through BGCAP Transit. Additionally, they offer senior services such as congregate and home-delivered meals, home care, senior employment, Foster Grandparent program, and Senior Companionship.*

10 Ways AI Saves Money (Without Adding Chaos)

Most AI conversations get stuck in hype. The businesses seeing real ROI are using AI for something simpler: **removing low-value work and reducing rework.**

Here are 10 proven ways AI saves time and money:

1. Customer service deflection - answer routine questions instantly

2. Sales follow-up automation - draft emails, sequences, and call recaps faster

3. Proposal generation - create first drafts in minutes instead of hours

4. Pre-sales research - summarize prospects and competitors before meetings

5. Meeting notes + action items - stop losing decisions to someone's notebook

6. Internal knowledge base - turn SOPs into searchable instant answers

7. Invoice explanation - summarize charges, flag anomalies, reduce back-and-forth

8. HR admin support - draft job descriptions, interview guides, onboarding content

9. Training content - create role-based refreshers, quizzes, and documentation

10. Compliance acceleration - generate policy templates and evidence check

5 Copy/Paste AI Prompts That Save Time and Reduce Rework

Use these in an approved/secure AI tool—especially when handling sensitive data.

Prompt 1: Customer Service Response
"Draft a friendly, professional reply to this common customer question: [insert question]? Give me: (1) a short answer, (2) a longer explanation, and (3) 3 follow-up questions I should ask if the customer is still stuck. Tone: calm and helpful."

Prompt 2: Proposal First Draft
"Create a one-page scope of work for [project]. Include: objectives, assumptions, deliverables, timeline, and what's out of scope. Make it clear and non-technical. Ask 5 clarification questions at the end."

Prompt 3: Meeting Summary
"Summarize these meeting notes into: key decisions, risks, action items (with owners), and deadlines. Then write a follow-up email I can send to attendees."

Prompt 4: SOP Creation
"Create a step-by-step SOP for this process: [describe process]. Include: prerequisites, steps, common mistakes, and a checklist. Keep it simple enough for a new hire."

Prompt 5: Compliance Checklist
"Create a compliance evidence checklist for [HIPAA/FTC Safeguards/industry requirement]. Output a table with: control area, evidence to collect, where to find it, owner, and review frequency."

Want AI savings without Shadow AI risk? Our Secure AI Services help you identify the best use cases, deploy them safely, and train your team with guardrails. Call **502.783.6630** to explore what's possible.

Strategic Planning Session: Let's Plan Your 2026 IT Strategy Together

Here's what we know: the businesses that win this year won't be the ones reacting to problems. They'll be the ones planning ahead. That's why we offer Strategic IT Planning Sessions.

What We'll Cover:

✅ Security gaps that need attention before they become incidents ✅ Hardware and software that's due for replacement or upgrade ✅ AI opportunities that could save your team time and money ✅ Compliance requirements (CMMC, cyber insurance, industry standards) ✅ Growth plans and how your IT needs to scale with you ✅ ROI Analysis—direct, measurable impact on your bottom line

Scan The QR Code To Schedule Your Session Today

Simplif IT
MANAGED IT | CYBERSECURITY

102 Enterprise Drive
Suite A
Frankfort, KY 40601

502.783.6630

WeSimplifIT.com

Modern Cybersecurity: What Changed in the Last 12 Months (and Why You Need to Know)

Cyber threats didn't just evolve in the last year—they accelerated. Attackers are faster, smarter, and more patient than ever. They're not breaking down the front door anymore. They're picking the lock, slipping in quietly, and waiting for the perfect moment.

What We're Seeing Right Now

- Token and session attacks designed to bypass MFA protections
- AI-assisted phishing that sounds like real executives, vendors, or partners
- Ransomware targeting backups first, so recovery becomes negotiation
- Stricter compliance requirements from cyber insurance, HIPAA, and FTC expectations
- More scrutiny from partners and regulators who want proof of controls—not just claims

What Proactive Security Looks Like: A Recent Example

Recently, our Managed Detection and Response (MDR) service helped prevent a ransomware incident at a local municipality.

Here's what mattered:

- We identified suspicious behavior early—before systems were locked
- We contained it quickly to stop the spread
- Then we partnered with their IT manager to remediate, close the gap, and strengthen defenses

That's the difference between IT that fixes problems and IT that prevents disruption.

Three Questions Every Leader Should Ask

1. Can your IT show you what's been prevented—not just what's been fixed?
2. If you were breached tomorrow, do you have a documented response plan?
3. Is your security stack evolving as fast as the threats are?

If you hesitated on any of those, that's not a failure—it's a signal that it's time to tighten things up.

Call 502.783.6630 for a Cybersecurity Review. No scare tactics—just a clear picture and practical next steps.

The Hidden Cost of Good Enough IT

Bad IT doesn't always show up as a crisis. Sometimes it just... drains you.

It's the login issue that takes 20 minutes—three times a week. It's the file that won't open when a client is on the phone. It's the software update that breaks something else. It's the quick question that turns into an hour of troubleshooting.

None of these are catastrophic. But together? They steal time, focus, and momentum from your team—every single day.

What to Expect from Modern IT

Modern IT isn't just about uptime. It's about removing friction so your team can focus on the work that matters.

When IT is done right, you stop thinking about IT—and that's exactly the point.

Rate Your Shadow AI Readiness

Shadow AI is already running in your organization—you just can't see it yet. Right now, employees are feeding client data and proprietary information into ChatGPT, Gemini, and other unvetted AI tools. They're solving problems. They're also creating security vulnerabilities, compliance gaps, and data leaks that won't show up until it's too late.

Most leaders discover Shadow AI when something breaks—a compliance audit, a breach, a cyber insurance denial. By then, you're in damage control. This checklist helps you spot the risk early and put guardrails in place without slowing your team down.

Check each requirement and rate your readiness. Visibility is the first step toward control.

- ☐ We have an approved list of AI tools our team is allowed to use
- ☐ We have a clear rule for what data is never allowed in AI tools (client info, credentials, PHI, CUI, etc.)
- ☐ We know which tools have AI features turned on by default in our existing software
- ☐ We can identify new AI tools through SSO/identity reporting (not guessing)
- ☐ We restrict or review OAuth app permissions connected to email/files/CRM
- ☐ We have a process to remove access immediately when employees leave
- ☐ We have written guidance on AI use for sensitive workflows (if applicable)
- ☐ We have written guidance on AI use for customer privacy (data handling, disclosures)
- ☐ We train employees on what AI can't be trusted to do (legal/HR decisions, hallucinations, sensitive advice)
- ☐ We require human review before AI-generated content becomes client-facing
- ☐ We have an internal path for approved AI so teams don't feel forced into Shadow AI
- ☐ We review AI tool usage quarterly as part of our security and compliance process

Rate your Shadow AI Readiness: _____ / 12

If you need help addressing any of these items, contact us now to start planning a more secure and strategic AI strategy.

Do you know another business we can serve? Ask us about our referral program.