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

A Message From Our Team

It's March Madness which is a great time to take stock. Q1 is wrapping up, and if you're like most of the business leaders we work with, the first quarter brought its share of surprises — new tools, new threats, and a few decisions that got delayed longer than they should have.

This month's issue is built around two themes we keep hearing from business leaders: how to actually get results from AI, and how to make sure your fundamentals are solid enough to support everything you're building on top of them.

On the AI side, we're cutting through the noise. Not theory. Not predictions. Actual numbers, real use cases, and a checklist your team can act on today. On the cybersecurity side, we're going back to basics, because in our experience, most breaches don't happen because someone missed a cutting-edge threat. They happen because a foundational control was missing or ignored.

We're also rolling out AI Workshops this month — short, hands-on sessions with real use cases your team can take back and put to work the same day. No hype. Just practical examples you can use immediately.

As always, if something in this issue raises a question or sparks an idea, reach out. That's exactly what we're here for.

Here's to a strong finish to Q1!
The Team at SimplifIT

Inside This Issue

What Separates the Businesses Winning at AI From Everyone Else

It's not the technology. It's not the budget. Here's what it actually comes down to.

By now, most business owners have heard the promise of AI: save time, cut costs, grow faster. And by now, most have tried something, a free tool here, a quick experiment there, only to feel like the big results they keep reading about are somehow out of reach.

Here's the thing: the gap between businesses genuinely winning with AI and the ones still dabbling isn't about technology. It's not about budget, industry, or company size. According to research from Harvard Business Review and McKinsey, who have surveyed hundreds of companies across dozens of industries, the difference almost always comes down to the same handful of factors. And every single one of them is something a small or mid-sized business can do.

The Research Is Clear: Most Companies Are Using AI. Few Are Using It Well.

78% of enterprises are now using AI in some capacity, up from less than a third just two years ago (Fullview, 2025). 62% of companies have scaled to more than two AI use cases (Bain & Company, 2025). Top performers are generating $3.70 for every $1 invested in AI, while the bottom half are seeing minimal returns (Fullview, 2025). Same technology. Completely different outcomes. So what's the difference?

1) They Start With Business Problems, Not AI Tools

The most common mistake businesses make is choosing a tool first and then trying to figure out what to do with it. The companies seeing real returns do the opposite. They start by identifying their most expensive, most repetitive, most time-consuming problems, and then find the AI application that solves them. The tool is the last decision, not the first.

This sounds obvious. Most businesses still don't do it.

What this looks like in practice: Before adopting any AI tool, ask: "What is the single task in our business that consumes the most time relative to the value it creates?" Start there.

2) They Treat Data Like Infrastructure

You can have the best AI tool in the world, and if it's working with messy, incomplete, or unstructured data, the results will be mediocre at best. McKinsey's 2025 State of AI report found that data infrastructure and talent strategy are the two factors most closely correlated with AI success, more than technology choice, more than vendor selection.

The businesses winning at AI have done the foundational work: they know what data they have, where it lives, how it's organized, and how to connect it to the tools that need it.

What this looks like in practice: Before expanding your AI footprint, ask: "If an AI tool needed to answer questions about our business, where would it find the information, and is that information clean, current, and accessible?"
.

3) They Have Someone Who Owns It

This one shows up in almost every study, and it mirrors exactly what we see with our clients. The businesses that fail at AI treat it like a technology project, something IT handles, or something that just sort of happens. The businesses that succeed treat it like a business initiative, with a clear owner, a clear goal, and a clear timeline.

That owner doesn't have to be a technical expert. They need to be curious, committed, and trusted by the team. HBR calls this "governance." We call it having a champion. Either way, without it, even the best AI investments stall.

What this looks like in practice: Before your next AI initiative, ask: "Who is the person in our business who owns this, not just IT, but someone whose success is tied to making AI work?"

4) They Invest in Their People, Not Just Their Tools

A 2025 Forbes report found that one of the top barriers to AI adoption is employee resistance and lack of training, not technology limitations, not cost, not vendor availability. People.

The winning companies aren't just buying AI tools. They're training their teams to use them, creating cultures where experimentation is encouraged, and making AI fluency a core part of how the business operates. Companies that invest in AI training report productivity gains of 26–55% compared to those that deploy tools without training (Fullview, 2025).

What this looks like in practice: Budget for training alongside technology. If you spend $500/month on AI tools and $0 on helping your team use them, you're leaving most of the value on the table.

5) They Build in Phases, Not All at Once

Bain's research found that the companies scaling AI most successfully are doing it incrementally, proving value in one area, then expanding. They're not trying to transform the entire business at once. This is the Crawl, Walk, Run approach in practice. It reduces risk, builds confidence, and creates internal proof points that make the next phase easier to fund and easier to adopt.

The companies that try to go from zero to full AI integration in one move almost always stall or retreat. The ones that pick one use case, nail it, and build from there almost always expand.

The Bottom Line

The businesses winning at AI right now aren't necessarily the biggest, the best-funded, or the most technical. They're the most intentional. They have a clear problem to solve, clean data to work with, a person who owns the initiative, a team that knows how to use the tools, and a phased plan that builds momentum instead of burning it.

That's not a technology advantage. That's a leadership advantage, and it's available to every business reading this.

Want to build your AI strategy the right way from the start? Book a free AI strategy session with the SimplifIT team and let's map out your 90-day roadmap. Call 502.783.6630 or visit WeSimplifIT.com

The Goal Isn't to Ban AI—It's to Have a Plan

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.

Would you like to strategize about AI for your organization? Join us for our regular AI Strategy Workshops held at our office. **Contact us at 502.783.6630 or email Nick@WeSimplifIT.com for an invitation.**

Cyber Star: Darrall Henderson, PhD

Former President, Kaba Mas | Consultant, Sphere Analytical Solutions

Our partnership with Darrall Henderson began during his tenure as President of Kaba Mas, a premier manufacturer of high-security locking solutions trusted by the Department of Defense and federal agencies worldwide. From the start, it was clear we were working with a leader who understood security not as a product category, but as a strategic imperative. That foundation built a professional relationship grounded in mutual respect and a shared belief that the organizations worth protecting deserve the best.

Darrall's background as a U.S. Army veteran and Colonel in the Army Corps of Engineers shaped how he leads, and how he thinks about security at every level of an organization. He doesn't treat cybersecurity as a line item or a compliance exercise. He integrates it into business operations, culture, and decision-making the same way he approached mission security in the field, with discipline, accountability, and a clear understanding of what's actually at risk.

Today, in his consulting role at Sphere Analytical Solutions, Darrall works with organizations navigating CMMC compliance and NIST 800-171 implementation, some of the most complex and consequential regulatory frameworks in the defense industrial base. He approaches these requirements strategically, helping leadership teams understand not just what the frameworks demand, but how to build the internal structures and evidence that make compliance sustainable. For defense contractors operating in high-security environments, that combination of executive experience, operational credibility, and compliance expertise is exactly the kind of guidance that makes a difference. We're proud to work alongside him.

Back to Basics: The Cybersecurity Fundamentals That Never Fail

In a world of AI-powered threats and zero-day exploits, the biggest wins still come from doing the simple things right.

There's no shortage of advanced threats in 2026. AI-generated phishing. Deepfake impersonation. Ransomware targeting backups before your data. Supply chain attacks through trusted vendors. The threat landscape has genuinely never been more complex.

And yet. When we look at how breaches actually happen, across our clients, across the industry, across the data, the story is remarkably consistent: most attacks succeed not because of sophisticated technology, but because a basic control wasn't in place, wasn't maintained, or wasn't monitored.

You don't need to out-innovate the attacker. You need to close the doors they consistently walk through. Here's what that looks like in practice.

Patch Everything. Actually.

Unpatched software is one of the most reliable entry points attackers use, and it has been for decades. Operating systems, applications, firmware on routers and firewalls, even printers. If it's on your network and connected to the internet, it needs to be current.

Patch management isn't glamorous. It's also not optional. Build a schedule, automate where you can, and review what didn't get updated and understand why.

Multi-Factor Authentication. Everywhere. No Exceptions.

Stolen credentials are behind the majority of unauthorized access events. MFA stops most of them cold. Even if an attacker has your username and password, they can't get in without the second factor.

The list of systems that need MFA is longer than most people think: email, VPN, remote desktop, cloud services, business applications, admin accounts, and financial platforms. "We have MFA on email" is not the same as "we have MFA where it matters."

Backups You Can Actually Restore From

A backup you've never tested is not a backup — it's a hope. Current ransomware strains actively target backup systems first, before locking down primary data. That means your backup strategy needs to account for offline or air-gapped copies, geographic separation, and a tested restoration process your team has actually run before.

If you can't tell someone exactly how long it would take to restore your most critical systems from a complete failure, your backup strategy has a gap.

Least Privilege Access

Every user account, application, and service in your environment should have exactly the access it needs to do its job, and nothing more. This isn't bureaucracy. It's containment. When a credential is compromised, least privilege limits the blast radius. An attacker who gets into an employee's email account shouldn't automatically have access to your financial systems, customer databases, or server infrastructure. Map your access, trim what's unnecessary, and review it regularly.

Train Your People, Consistently

Technology controls are only as strong as the people operating them. Phishing simulations, regular security awareness training, and clear incident reporting processes are not one-time events. They're ongoing.

Your employees are your most targeted attack surface. They're also your most effective first line of defense, but only if they know what to look for and what to do when they see it. Make security awareness a repeating calendar event, not a once-a-year checkbox.

Endpoint Protection and Monitoring

Every device that touches your network is a potential entry point. Laptops, desktops, mobile devices, and even smart peripherals need endpoint protection that goes beyond basic antivirus. Modern endpoint detection and response (EDR) tools look for behavioral patterns, not just known signatures, which matters because many of today's attacks use legitimate tools in illegitimate ways.

Protection without monitoring is incomplete. You need to know what's happening on your endpoints, not just have a tool installed and forgotten.

Document It and Review It

Cybersecurity documentation isn't just for auditors. It's for you. Written policies, network diagrams, asset inventories, and incident response plans clarify what you have, establish accountability, and give you something to measure against.

Schedule an annual, or semi-annual, review of your security posture. Not just to check a box, but because your environment, your risks, and the threat landscape all change. Your controls should too.

The Bottom Line

Advanced threats get the headlines. But the organizations that stay secure over the long term are the ones that treat fundamentals as a competitive advantage, not a compliance nuisance.

Patch your systems. Enforce MFA. Test your backups. Limit access. Train your people. Monitor your endpoints. Document your policies and review them.

Do those seven things consistently and you've closed the door on the majority of attacks that are actively targeting businesses just like yours right now.

Want to know where your fundamentals stand? A SimplifIT Cybersecurity Review gives you a clear picture with practical next steps, no scare tactics, no upsell pressure. Call 502.783.6630 to schedule yours.

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

The 5 AI Use Cases With the Fastest Payback

If you're not sure where to start, these five use cases show up consistently across industries as the fastest path to measurable ROI:

Document and Report Generation. Converting notes, recordings, or rough drafts into polished, professional documents. The time savings are immediate and easy to quantify.

Client Communication. Drafting emails, responses, proposals, and follow-ups. AI doesn't replace the relationship, it removes the friction that slows it down.

Internal Knowledge and SOPs. Turning what's in your team's heads into structured, searchable documentation. Faster onboarding, fewer repeated questions, better consistency.

Research and Summarization. Synthesizing information, summarizing long documents, pulling key points from data. Hours of work compressed into minutes.

Your AI Assistant. An AI agent you train on your own workflows, tone, and processes. Once configured, it handles repetitive, manual tasks every day, drafting recurring reports, triaging requests, following up on open items, and more. You stay focused on the work only you can do.

None of these require a complex implementation. All of them deliver measurable value within weeks.

The window where AI is a competitive advantage is closing. It's moving from "early adopter edge" to "table stakes" faster than most people expected.

The businesses that look back in three years and say "AI has been great for us" are the ones making intentional moves right now, not waiting for the perfect moment that never comes.

Not sure where to start? Let's figure it out together. Contact the SimplifIT team to book a free AI strategy session and find out which use cases will move the needle fastest in your business.

Your 8-Point AI Security Checklist

Use this as your starting point before rolling out any AI tool company-wide.

AI adoption is accelerating, and so are the risks that come with it. If your team is already using AI tools, or you're planning to roll them out, the eight controls below are the baseline. Not the finish line, the starting line.

□ **Acceptable Use Policy:** Document what AI tools are approved, what data can and cannot be shared, and the consequences for misuse.

□ **Approved Tool List:** Identify which AI platforms meet your security and compliance requirements.

□ **Data Classification:** Know what data is sensitive, regulated, or confidential before it ends up in an AI prompt.

□ **Vendor Security Review:** Understand how your AI vendor stores, processes, and protects your data.

□ **Employee Training:** Your team needs to know not just how to use AI, but how to use it safely.

□ **Access Controls:** Not every employee needs access to every AI tool or every data source.

□ **Internal Champion:** Designate someone to own AI adoption, governance, and ongoing training.

□ **Review Cadence:** AI tools and risks evolve fast. Schedule quarterly reviews of your policy and tool stack.

This checklist doesn't prevent AI adoption. It makes adoption safe, scalable, and defensible, especially in regulated industries like healthcare, defense, and financial services where the stakes of getting it wrong are highest.

Want help completing this checklist for your organization? That's exactly what our Secure AI Services are designed for. Call 502.783.6630 or visit WeSimplifIT.com.

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