July 2026

The SimplifIT Advantage

Proven strategies to help leaders make clear technology decisions for measurable 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

This month, we want to cover something that happened in June and caught a lot of attention in the technology world, but didn't get much coverage in business circles: the federal government's decision to ban Claude Fable 5, one of the most advanced AI models available.

The story matters because it highlights risks every business leader should understand when adopting AI. Access to these tools isn't guaranteed. Governance matters before conflicts emerge. And the businesses that benefit from AI are the ones using it through secure, managed environments, not hoping nothing goes wrong.

We are also addressing a question we hear often from business leaders: where is AI actually working right now? Not the hype. Not the speculation. Where is it delivering measurable results for small and medium businesses? This issue answers that question with real data from trusted sources.

Finally, we are covering something showing up in cyber insurance renewals: AI exclusions, sublimits, and new underwriting requirements. If you haven't reviewed your cyber policy recently in the context of AI, there may be gaps you don't know about.

This issue covers the Claude Fable 5 ban and what it means for businesses, the top 10 AI use cases delivering real results for SMBs right now, and how AI is changing cyber liability insurance.

We hope it is valuable. As always, we are here when you need us.

All the best!

The Team at SimplifIT

Inside This Issue

US Government Bans Claude Fable 5: Here's What it Means for Your Business

On June 9, 2026, Anthropic released Claude Fable 5. Three days later, the U.S. Commerce Department shut it down completely.

Not because of a security breach. Because of a national security concern about the model's capabilities.

What Happened on June 12

The Commerce Department issued an export control order prohibiting access to Claude Fable 5 for foreign nationals. Because Anthropic couldn't distinguish foreign nationals from U.S. persons in real time, they shut down the model globally for all customers.

Businesses using Fable 5 for software development, financial analysis, legal document review, and customer support lost access immediately. The work didn't stop. The tool did.

Why This Matters for Your Business

Access to advanced AI isn't guaranteed. Technology your team depends on can be restricted by government policy overnight. This just happened to one of the most widely used AI platforms in the world.

Governance matters before disruption hits. The businesses caught in this shutdown had no warning. The ones with structured AI governance, documented policies, and alternative pathways adjusted and kept moving. The ones without spent days rebuilding workflows under pressure.

The businesses that benefit from advanced AI use it through secure, managed environments. When access changes or regulations shift, businesses with structured AI access can adapt quickly. Businesses running AI tools directly without governance get stuck.

What Strategic Businesses Are Doing Right Now

Build secure AI access infrastructure. If your team is using AI tools, they should be doing it through a managed environment that monitors what data goes in and out. Provide access to advanced AI technology with a secure layer in between. That's what our Secure AI solution delivers.

Document AI usage and governance. Which AI tools are approved? What data can employees share? What happens if someone uses an unapproved tool? If those answers aren't documented, you don't have governance.

Understand industry specific risks. If you handle regulated data in accounting, legal, healthcare, or work with defense contractors, the rules around AI usage are stricter. Your AI strategy needs to account for those constraints before something goes wrong.

Train teams on safe AI usage. Your employees are already using AI tools. The question is whether they're using them safely or feeding client data into public AI systems without understanding the implications.

The Bottom Line

The June 12 ban on Claude Fable 5 is a signal that AI access, governance, and security have moved from optional considerations to business critical infrastructure.

The businesses that will benefit most from AI are the ones treating it seriously today. Building secure access infrastructure. Documenting clear policies. Training teams. Staying ready to move when technology evolves or access gets restricted.

Team Spotlight: Craig Willard
SimplifIT COO

Leadership in IT is one thing. Understanding how people and organizations actually work is another. Craig Willard brings both. As SimplifIT's Chief Operating Officer and founding partner, Craig combines over 15 years of Healthcare Information Technology experience with a rare depth of insight into organizational dynamics. He holds a bachelor's degree in organizational management, a master's in business administration, and is currently completing a doctorate in industrial and organizational psychology. That's not just credentials—it's how he thinks about the work. Most IT leaders focus on systems. Craig focuses on the people using them and the organizations they serve.

Craig's been nationally recognized for leading one of the best hospital IT departments in the country, where he learned that when people's lives depend on technology working flawlessly, there's no room for reactive support or surprise downtime. That standard became SimplifIT's Four Pillars: Simplicity, Security, Predictability, and Responsiveness. His expertise in HIPAA compliance, project management, lifecycle management, and helpdesk operations separates reactive firefighting from proactive strategy. For SimplifIT clients in regulated industries, Craig's leadership translates into IT environments that prevent problems before they happen.

Ask Craig what drives him and the answer is transformation. He doesn't just want systems that work—he wants businesses where leaders never have to think about IT because it's working so well in the background. His leadership philosophy is rooted in making complex technology simple, secure, predictable, and responsive. We're honored to work alongside him every day.

Contact Craig:
Craig@WeSimplifIT.com
502.783.6630.

Top 10 AI Use Cases for Small Businesses

Here's what the data shows about AI applications working today, delivering measurable time savings, cost reductions, and revenue growth for businesses.

1. Data Analysis and Business Intelligence. 62% of SMBs using AI apply it to data analysis. 58% save 20 plus hours monthly on reporting. Payback period: three to six months. Revenue benefit: 15-25% faster decision making.

2. Content Generation and Marketing. 55% use AI for content. Reduces creation time by 60-70%. Cost savings: $500 to $1,500 monthly. Revenue benefit: 10-15% more qualified leads.

3. Customer Service and Chatbots. 46% use AI powered customer tools. Achieves 60-80% first contact resolution. Time saved: 15 to 25 hours weekly. Cost savings: 30% reduction in support costs.

4. Financial Management and Accounting. Adoption jumped from 37% to 58% in one year. 66% save $500 to $2,000 monthly. Invoice processing automation reduces manual work by 80%.

5. Sales and Customer Insights. 45% use AI for predictive revenue trends. Shows 20-30% faster sales cycles. Time saved: 10 to 15 hours weekly per rep. Revenue benefit: 15-25% increase in conversion rates.

6. Recruitment and Talent Acquisition. 19% use AI for recruitment. Resume screening time reduced 70%. Time to hire drops 30-40%. Cost savings: $3,000 to $8,000 per hire.

7. Supply Chain and Inventory. Demand forecasting reduces forecast error 20-50%. Cost savings: 20-30% reduction in carrying costs. Revenue benefit: 15 to 24% increase. Return on investment: 150-300% within two years.

8. Predictive Maintenance. Delivers 50% reduction in downtime, 31% lower maintenance costs. Return on investment: 385%. Cost savings: $50,000 to $200,000 annually depending on asset base.

9. Business Process Automation. 83% agree automation is key to efficiency. Saves 20 plus hours monthly per employee. Cost savings: 30% reduction in operating costs for automated workflows.

10. Competitive Intelligence. 73% say AI improved competitiveness. Growing businesses are 1.8 times more likely to invest in AI. Time saved: 8 to 12 hours weekly on market research.

What the Data Shows

58% of U.S. small businesses use generative AI in 2025, up from 40% in 2024. 91% report revenue increases. 90% say operations are more efficient. 60% save $500 to $2,000 monthly. Businesses with AI are two times more likely to achieve year over year growth.

Average return on investment: 5.8 times within 14 months. But only 34% are truly transforming operations. The businesses winning aren't just buying tools. They're rethinking workflows and designing processes.

Security Is Non Negotiable

Regardless of which use cases you implement, security must be built in from day one. Every AI strategy requires a secure layer between your team and the tools. Monitor what data goes in and out. Document which tools are approved. Train teams on safe usage. Security isn't optional. It's the foundation that determines whether AI becomes a competitive advantage or a liability. Public-facing LLMs should not be used for most business cases.

What This Means

Start with a problem, not a technology. Focus on payback. Most see results within 90 days. Full payback requires six to twelve months. Expect process redesign. 80% of the value comes from redesigning workflows, not the technology itself. Measure results. If it's working, expand. If not, adjust.

The Bottom Line

AI is delivering measurable results across growing businesses. The question isn't whether AI works. The question is whether you're solving a real problem, whether your team is ready, and whether you're building secure infrastructure that protects your business as it scales.

Organizations need an approved, secure path to use AI safely so they get speed and efficiency without creating risk. You don't have to ban it, but you do need to secure it.

SimplifIT
MANAGED IT | CYBERSECURITY

102 Enterprise Drive
Suite A
Frankfort, KY 40601

502.783.6630

WeSimplifIT.com

How AI is Changing Cyber Liability Insurance

What You Need to Know About AI and Cyber Insurance

If your business uses AI tools, you may have cyber insurance coverage gaps you don't know about.

What Changed in 2025-2026

Major insurers including Berkshire Hathaway, Chubb, Travelers, QBE, and Beazley introduced AI exclusions and sublimits to policies. Over 80% of state regulatory requests for AI exclusions were approved.

Effective January 1, 2026, Insurance Services Office introduced new endorsements excluding or modifying coverage for generative AI related claims.

U.S. cyber insurance premiums grew 11% in 2025. Higher rates reflect AI risks according to Gallagher's 2026 market outlook.

Why Insurers Are Concerned

Coalition's 2026 report found AI enabled email attacks represented 58% of all claims. Phishing emails surged 856% due to AI assistance.

Over 200 active legal cases involving AI emerged in 2025, centering on data bias, intellectual property infringement, and privacy liability.

New Requirements

Cyber insurance now requires documented AI governance frameworks. Organizations implementing ISO/IEC 42001 or NIST AI Risk Management Framework receive improved terms. Organizations without AI governance face premium increases or denial of coverage.

What You Need to Do

Contact your insurance agent. Ask specifically about AI exclusions, sublimits, and what governance frameworks they expect. Get everything in writing. Contact us if you need assistance.

Traditional cyber policies written before 2025 are becoming obsolete. The gap between how businesses use AI and how insurers cover it is where uninsured losses happen.

Cyber Insurance Readiness Checklist

Is your cyber insurance renewing soon?

Whether you are just looking to check a box, ensure that you can get coverage for cyber liability insurance, or improve the security of your organization, this checklist will help you prepare.

Check each common requirement and rate your cyber insurance readiness:

- ☐ Email security is enabled in your email system (DKIM, DMARC, SPF)
- ☐ DNS filtering or web filtering is in place to block malicious web content
- ☐ Advanced Anti-malware/spyware/ransomware software is deployed on all systems
- ☐ User installed programs are limited to only pre-approved applications
- ☐ User training is in place to educate against threats like phishing and ransomware weekly or monthly
- ☐ Perimeter traffic is monitored
- ☐ Internal network traffic is monitored
- ☐ Multi-factor authentication is in place for users
- ☐ All Systems are backed up daily to an offsite or cloud location with the ability to restore
- ☐ Disaster recovery and incident response plans are in place, reviewed and tested annually
- ☐ All available important and critical patches are installed within 7 business days across systems and software
- ☐ Managed Detection and Response (MDR) is installed on all computers and servers
- ☐ Documented AI Governance is in place

Rate your Cyber Insurance Readiness: ____ / 13

If you need to address any of these requirements, contact us now to start planning for your next renewal. We suggest reviewing this list before you submit your application.

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