RECAP

AI Is In Your Business, Now What?

A conversation on where AI is delivering real value for small and mid-sized businesses, and where it's quietly introducing risk you haven't accounted for yet.

JB **Jeff Buss**
CEO, Cyberleaf

ST **Stephen Tracy**
VP of Technology, Entech

The AI equation: risk, value, and readiness

Risk
AI accelerates how fast attackers find and exploit vulnerabilities sitting in unresolved tech debt. Breach odds for small businesses have roughly doubled in five years.

Value
Real gains show up on defined, repeatable processes with clean data, think reconciliations, not open-ended "chat with AI" experiments on messy inputs.

Readiness
Policies, controls, and clean data have to come before scale. Without that foundation, tools amplify whatever disorder is already there.

Key takeaways

- **The odds have doubled.** Small business breach probability has climbed from roughly 10–15% a year to 35–40%, and AI-accelerated exploitation is a driving factor.
- **Tech debt is a margin call.** Unresolved vulnerabilities that once sat quietly are now found and exploited far faster than before.
- **Real wins need real process.** AI delivers on established, well-defined workflows with clean data. Without that, results are fragmented and unpredictable.
- **Adoption is happening informally.** A live poll found just under a third of attendees have a formal AI policy; more than half said it's happening informally
- **Enterprise accounts only.** Personal ChatGPT or Copilot logins don't protect company data the way a bucketed, secured enterprise account does.
- **Ask the outcome, not the tool.** Most customers don't want AI, they want their problems solved. Some of what they want is automation they already own.

One thing to do Monday morning

Jeff Buss

Get your policies, controls, and data cleanup in place before scaling any AI use. That foundation is what sets up years of return.

Stephen Tracy

Take stock of the AI tools your team is already using informally, and confirm they're running through secured enterprise accounts, not personal ones.

How to Get Started

- **Define the outcome first**. Most organizations don't want AI, they want a problem solved. Get specific about what that problem is before choosing a platform.
- **Run the workshop before the rollout**. A short set of scoping conversations to build the strategy beats buying a tool and experimenting on a live business problem.
- **Get leadership buy-in.** Without it, even well-built use cases stall before they scale.
- **Build in a change management step**. Whatever AI produces has to get integrated back into how the team actually works, and formalized, not just adopted ad hoc.
- **Then implement.** Tool selection comes last, not first.

Pick the Right Tool

Tool	What to Know
Microsoft Copilot	Wrapped in Microsoft's existing security environment, generally a strong default if you're already on Microsoft 365.
Enterprise Claude or ChatGPT	Data stays bucketed and protected under an enterprise account, a materially different setup than a personal login.
Personal Accounts	Not bucketed or secured the same way. Company data typed into a personal account isn't protected like it would be under enterprise.

What a Real Win Looks Like

Real AI wins show up on defined, repeatable processes with clean data, not open-ended experimentation. Two examples from the conversation:

Finance close & reconciliation

A repeatable, well-documented process that used to take significant human time, cut down dramatically once AI had clean inputs to work from.

A narrow, well scoped agent

Think an RFP or grant-writing assistant, built around a defined, clean dataset rather than pulling from public sources or scattered documents.

The bigger picture

At a recent National Cyber Innovation Forum on Capitol Hill, lawmakers discussed a significant structural shift. Historically, major technology revolutions were led by government, with the public interest built into the rollout. AI's rails are being built by Nvidia, Microsoft, Google, Anthropic, and others, companies with commercial incentives driving the pace. Neither point is cause for alarm, but both are context for why getting the foundation right first isn't just caution, it's strategy.

Ready to Get Started?
Book time with our team to talk through where your organization stands, whether that's a governance gap, a tech debt cleanup, or picking the right enterprise tool.

Entech's AI Governance Playbook • Cyberleaf's AI Threat Report

Cyberleaf
www.cyberleaf.io | info@cyberleaf.io

Entech
www.entechus.com | hello@entechus.com