

# The Upside and *the Fine Print*

A conversation on where AI is paying off inside mid-market companies and private equity firms, and what has to be in place before it scales.



**Harrison Welsh**  
Director of Professional  
Services, Cyberleaf



**Bob Elfanbaum**  
Founder and CEO,  
Kairoi



**Andrew Montgomery**  
CTO and COO,  
Kairoi

## Three ways to look at AI in your business



### Where it pays off

AI is disruptive where revenue is tied to labor hours. The gains show up when you start from a business problem you haven't been able to solve, not from a decision to adopt AI.



### Where it leaks

A tool that isn't configured at the admin level can send your data into the model or out of your control. Note-takers, dragged-in files, and personal accounts are the common paths.



### What holds it together

An inventory of what's running, a signed acceptable use policy, a published list of approved tools, and over time, data that's classified and protected before AI touches it.

## Key Takeaways

- ✓ **AI arrived the way spreadsheets did.** Individuals can run their own analysis without going to IT, and the gains came from people self-directing.
- ✓ **The best tool keeps changing, and people follow it.** The people most invested in doing great work are the ones most likely to bring in their own.
- ✓ **Your note-taker sits in your most sensitive conversations.** A tool joins the meeting, listens, and touches everything discussed in the room.
- ✓ **Banning it backfires.** A ban pushes people onto personal accounts and phones, outside every protection you have.
- ✓ **Saved time is not value.** One company freed up real hours with AI and never converted them into revenue or margin.
- ✓ **Nobody agrees on who owns AI.** It usually lands with IT, who often lack the business context to decide what's worth building.

## One thing to do Monday morning

### Harrison Welsh

Build an AI inventory with IT. Pull a software list and check it for AI tools and AI features someone switched on.

### Bob Elfanbaum

Start at your biggest business problem and scope down. Solve a piece of it you can measure.

### Andrew Montgomery

Find something your team does consistently and can measure consistently.

## Start with an Inventory

You can't govern what you haven't found.

- **Pull the software list.** Most environments have a way to extract what's installed and in use.
- **Check it against AI.** Standalone tools, plus existing software with AI features someone switched on.
- **Decide what stays.** Block what isn't approved. Protective DNS is one way to do it.
- **Publish an acceptable use policy.** Have people sign it. Be specific about what can't go into a tool, including personal information and sensitive financial data.
- **Publish the approved tool list.** And let it grow. The list isn't meant to be frozen, it's meant to be known.

This applies to off-the-shelf tools like Claude, ChatGPT, Copilot, and Perplexity. Custom agents are different.

## Before You Let a Tool Touch Your Data

| What To Check             | Why It Matters                                                                        |
|---------------------------|---------------------------------------------------------------------------------------|
| Where your data is stored | Which cloud it lands in, and under what terms.                                        |
| Subprocessors             | Whoever your vendor uses also touches your data.                                      |
| Admin configuration       | Enterprise versions let you stop content from reaching the model. Verify the setting. |
| Logging and retention     | Enterprise plans generally offer compliance APIs for both.                            |

## Who Should Own It

The one place the panel disagreed.

### Harrison

It often lands with internal IT or an outsourced provider, since they set up the guardrails. Some firms have a director of AI for the business use cases. One PE firm built an AI steering committee with a written charter: IT, director of AI, CFO, CEO, and legal counsel.

### Bob

IT alone doesn't work. The team with the technical depth often lacks the business context, and the partner who understands the business can't evaluate the technology. The answer is a multidisciplinary group.

## The Longer Project

Securing the data underneath the tools is the piece that doesn't fit in thirty days. On Microsoft 365 that means classification, retention, and loss prevention, which takes real tuning before it's useful. Once it's running, it tells you when sensitive information is going somewhere it shouldn't. Microsoft isn't the only path.

### Ready to Get Started?

Book time with our team to talk through where your organization stands, whether that's an AI inventory, a governance gap, or the data work underneath it.

[Book 30-Minutes with a Security Practitioner](#)

Cyberleaf

[www.cyberleaf.io](http://www.cyberleaf.io) | [info@cyberleaf.io](mailto:info@cyberleaf.io)

Kairoi

[www.kairoi.io](http://www.kairoi.io) | [info@kairoi.io](mailto:info@kairoi.io)