The AI Risks No One Warned Your Business About

Table Of Contents

03
Introduction

04
Risk 1: No guardrails, no rules

05
Risk 2: You're losing control of your data

06
Risk 3: Your AI tools might be making things up

07
Risk 4: AI is being used against your business

08
Conclusion

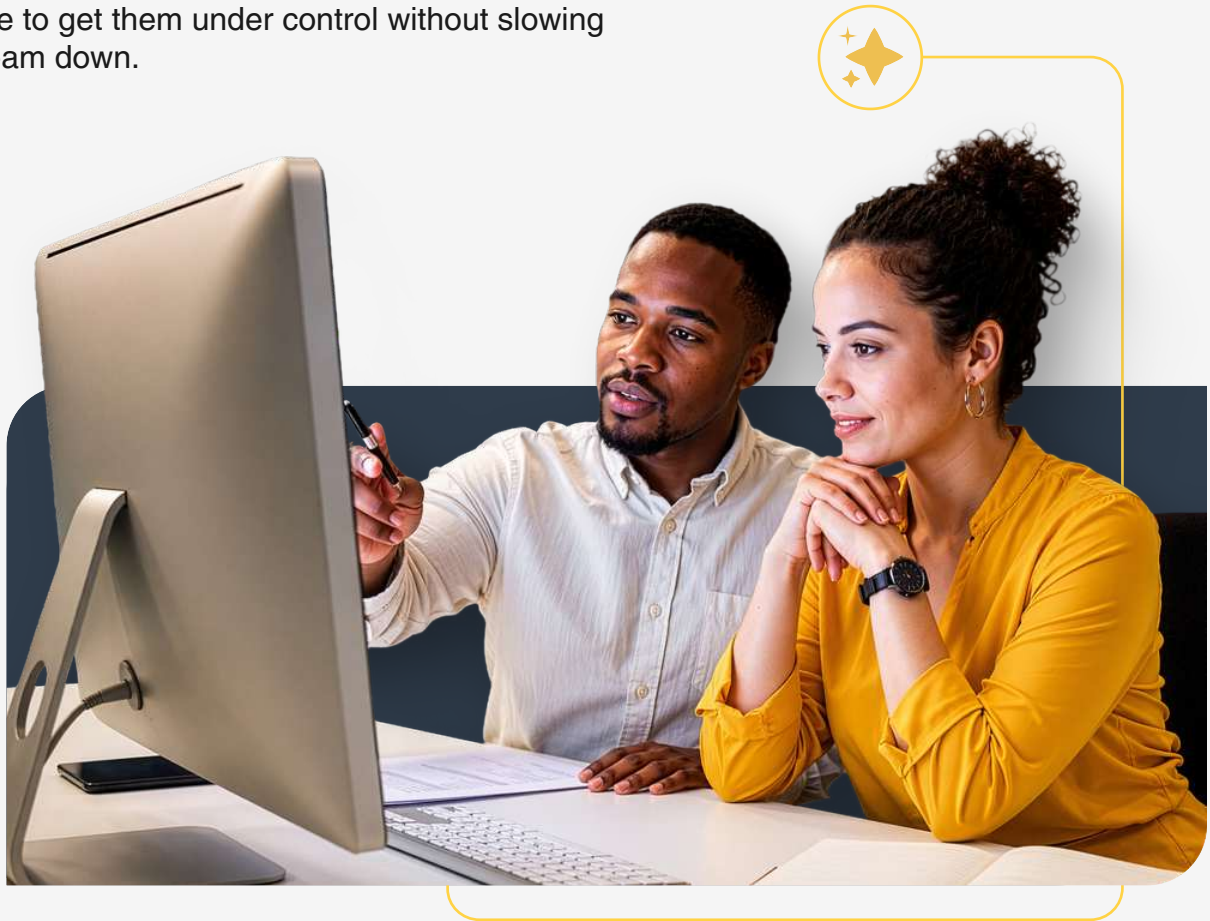
Introduction

Most small business leaders are in similar positions right now. AI tools have entered the chat, your team is using them and no one has stopped to ask what that means for the business.

There's no policy, no oversight and no visibility into what's happening or how decisions are being made with AI-generated information. Everyone is finding their own way and for the most part, it works. Until it doesn't.

When powerful tools enter a business without any structure around them, they create risk. The four risks in this eBook are already present in most businesses. They're just not visible yet.

This eBook uncovers what those risks are, how they show up in everyday work and what you need to put in place to get them under control without slowing your team down.



Risk 1:
No guardrails, no rules

AI tools didn't go through your procurement process. They didn't require IT approval or a company-wide rollout. They're free, browser-based and don't need a purchase order or vendor contract to access. An employee can sign up and start using one in under two minutes, without anyone in leadership knowing it happened.

The risk doesn't live in the AI itself, but in the absence of a shared standard for how it's used. Right now, it's likely someone on your team is drafting client proposals with it, someone else is summarizing confidential meeting notes, and another person is pasting customer data into it to pull together a report. They're all utilizing AI differently because they haven't been told otherwise.

Without a policy, every person on your team is making individual judgment calls about what's appropriate. Those judgment calls won't always align with each other, with your brand standards or with your legal obligations. And because no one is tracking how AI is being used, you won't know there's a problem until one surfaces.

How to get control

- Start by finding out which AI tools your team is using and what they're using them for. The answer to that question will tell you exactly where your exposure is.
- From there, put a written policy in place. It doesn't need to be long, but it needs to cover which tools are approved, what kind of information should never go into an AI tool and who is responsible for reviewing AI-generated content before it goes out.
- Once the policy is finalized, make sure every employee sees it and understands it applies to them.

Risk 2:
You're losing control of your data

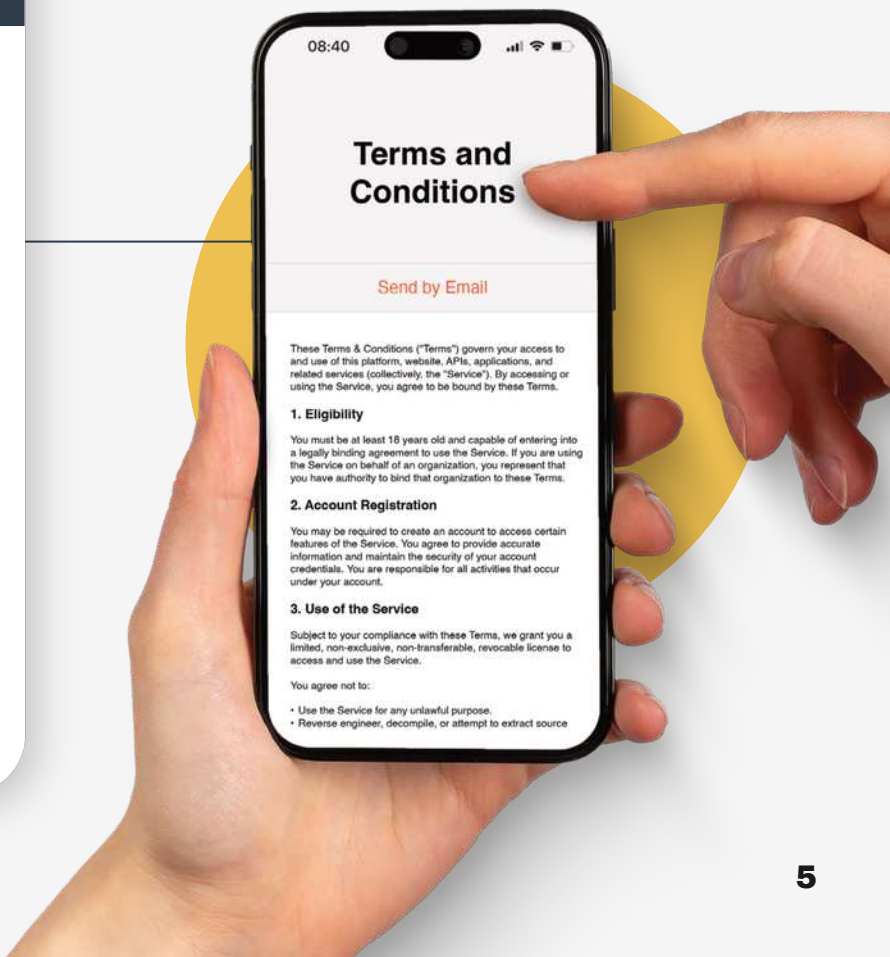
When your team uses an AI tool, they're not using a closed, internal system. They're sending information to a third-party platform with its own terms of service, data retention policies, and in some cases, its own right to use that content to train future models. Most people on your team have never read those terms and wouldn't know what to look for if they did.

The exposure happens at two levels. The first is behavioral, with employees inputting client information, financial data or internal strategy into a tool that lives outside your business's walls. The second is structural. Even if your team is being careful, the platforms they're using may be storing, analyzing or learning from everything they submit. You have no control over what happens to that data once it leaves the browser.

Sensitive information can get out through the routine, well-intentioned work of employees who had no idea they were creating a risk. That's what makes this one hard to catch.

How to get control

- Pull the terms of service for every AI tool your team is using. Look specifically for language around data retention and model training. What you find will tell you which tools are safe to keep and which ones need to go.
- From there, clearly define which information is entirely off-limits to AI tools. Client data, financial records, internal communications, anything you would not hand to a third-party vendor without a signed agreement.
- Add that boundary to the same policy you put in place for Risk 1. If it isn't written down, it isn't a rule.

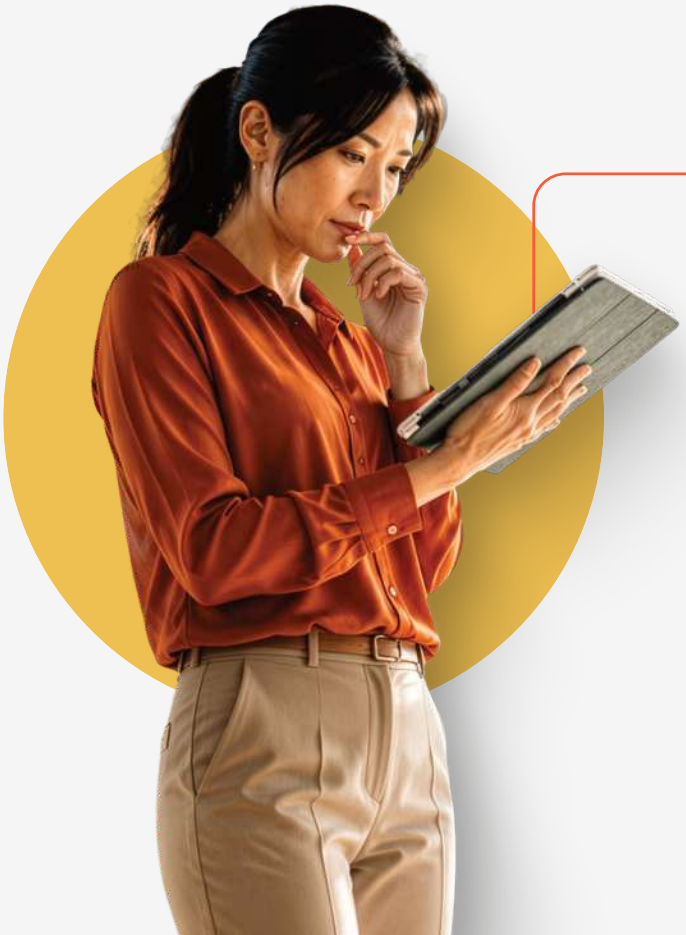


Risk 3:
Your AI tools might be making things up

AI tools are built to generate responses that sound authoritative and complete. They don't pause to question their own output or signal when they're uncertain. They produce an answer that looks polished and credible, regardless of whether it's true.

The technical term for this is hallucination. An AI tool can cite a statistic that doesn't exist, reference a law that was never passed or summarize a document in a way that changes the meaning entirely. It won't tell you it did any of that. The output will look the same as it always does.

For a small business, the consequences are real. Wrong information can leave your business every time someone sends out AI-generated content without checking it first, and it almost always ends up in front of a client. That's a credibility problem at best and a liability issue at worst.



How to get control

- Establish a clear review standard for AI-generated content before it leaves your business. Anything that contains statistics, legal or financial information, or factual claims about your industry needs to be verified against a credible source before it goes out.
- The person sending the content is responsible for what it says and so is the business it represents. AI output is a starting point and your policy needs to clearly reflect that expectation.

Risk 4:
AI is being used against your business

While the first three risks concern decisions made within your business, this one comes from the outside and is getting harder to defend against.

AI has given cybercriminals a significant upgrade. Phishing emails used to have tells. Poor grammar, a generic greeting or a request that felt slightly off were enough for a cautious employee to pause. AI has removed most of those signals.

Fraudulent emails read like professional correspondence, fake invoices arrive properly formatted and voice scams can convincingly replicate someone your employee knows. The instincts your team developed to catch these threats are being used against outdated versions of them.

This is a costly problem for any business that doesn't have dedicated security staff reviewing communications. It only takes one person clicking the wrong link or approving a fraudulent payment to create a situation that is very difficult to recover from.

How to get control

- Your cybersecurity awareness training needs to reflect what attacks look like today. If your team hasn't been trained in the past twelve months, what they know is already out of date.
- Beyond training, put simple verification processes in place for high-risk actions. Any request to change payment details, transfer funds or share sensitive information should require a secondary confirmation through a separate channel before anyone acts on it. A quick phone call to verify a request is still one of the most effective ways to stop a fraudulent transaction before it happens.

Introduction

The four risks in this eBook aren't hypothetical. They're playing out right now in businesses that have adopted AI without a policy, oversight or visibility into how it's being used across the organization. The longer there is no structure around it, the more exposure builds.

A clear policy, defined boundaries, a review standard for outgoing content and an updated approach to the threats coming from outside your business will go a long way toward protecting what you've built.

Most leaders already sense that something needs to change, but knowing where to start is the hardest part. That's where we come in.

We help business leaders understand how AI is being used inside their business, where unnecessary risk is being created and what guardrails need to be in place so teams can use AI safely and consistently.

You've read the risks. Now let's do something about them.

Schedule a 10-minute discovery call with us today.

TECH SEVEN PARTNERS