WORTHINGTON CHAMBER · LUNCH & LEARN

AI Safety

Protecting your business, your clients, and your data.

Cloud Cover · Powered by AI · 614-362-8201

Your team is already using AI

75%

of knowledge workers, and climbing

They're writing emails, summarizing meetings, and cleaning up spreadsheets with AI - usually on personal accounts.

Most owners can't name a single tool their team uses.

WHAT WE DO FOR MANAGED CLIENTS

The good news: this is findable

- **Software inventory** — what's installed on every machine.
- **Network & DNS logs** — every query to the AI's servers.
- **Email signals** — welcome notes, password resets, receipts.
- **Microsoft 365 audit logs** — who let an app into their mailbox.

SHADOW AI

Here's what that actually looks like

- Pasting the **whole client list** into ChatGPT to “clean it up.”
- Uploading a **contract** for a quick summary before a meeting.
- Dropping the **P&L** so they can ask questions
- A free **meeting bot** auto-joining every call and keeping the transcript.
- A **browser extension** that quietly reads every page.

TYPICAL 20-PERSON COMPANY

8–15

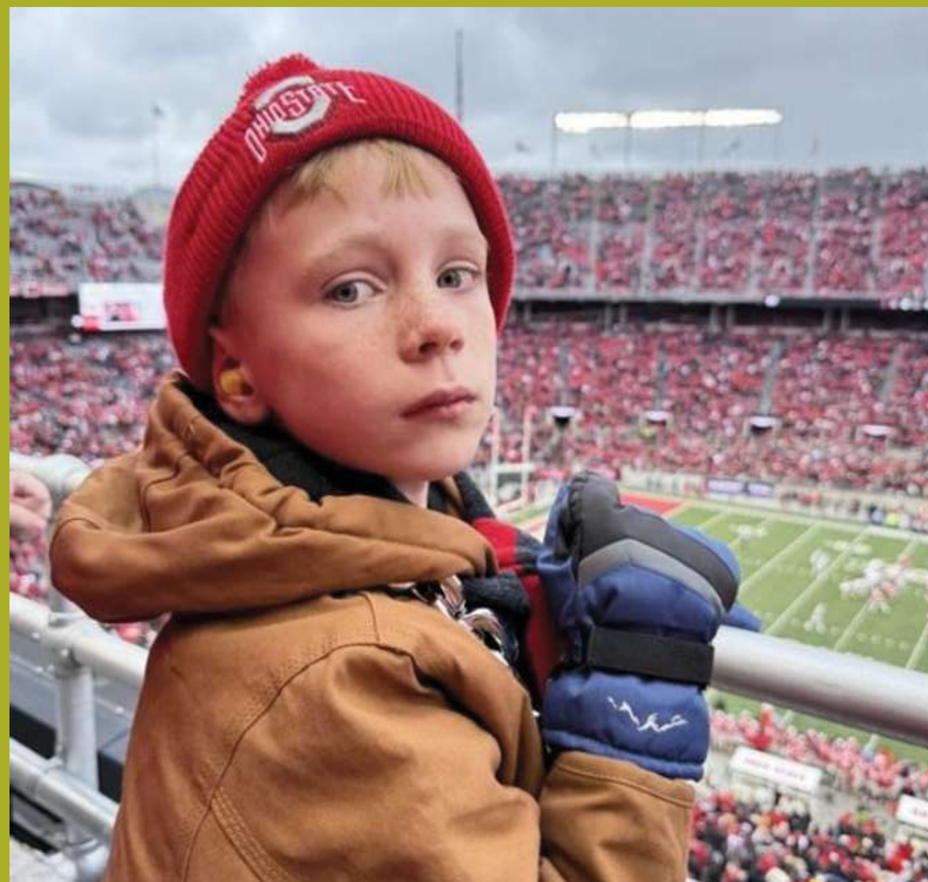
AI tools in active use.

LET'S BACK UP FOR A SECOND

What is a large language model?

$$P(w_1, w_2, \ldots, w_m) = \prod_{i=1}^{m} P(w_i \mid w_1, \ldots, w_{i-1})$$

$$\mathrm{Attention}(Q, K, V) = \mathrm{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V$$

OH  IO

CloudCover

UNDER THE HOOD

It's just predicting the next word

It has seen enormous amounts of text and learned which word tends to follow the last one. That's the whole thing. It doesn't reason; it autocompletes - brilliantly.

It was never intended to be true. It has statistics.

EVERY WORD IS A GUESS

Why didn't the chicken cross the road? Because it was too hot.”

the chicken

…was too hot to be bothered crossing.

or

the road

…was too hot to walk across.

You picked one without noticing. So does the AI — for every word. It never actually *knows*.

RISK #1

The risk every IT company talks about

AI surfacing information it shouldn't. It's real, and it's worth fixing.

PICTURE THIS

Beware of the Leopard

A salary spreadsheet has sat “safely” in a box in your basement for five years — hidden in a dimly lit cellar lavatory in a safe behind a sign reading *Beware of the Leopard*. Then you switch on Copilot. A junior employee asks, “What's our payroll budget for marketing?”

A sign is not a lock. Copilot respects permissions.

PERMISSIONS, NOT MAGIC

What surfaces the day you turn it on

- Compensation & bonus letters
- Termination & severance drafts
- M&A and legal correspondence
- Performance reviews & PIPs
- Pricing, margins & customer discounts
- The owner's personal files in a “shared-with-everyone” folder

Fix permissions before you flip the switch — not after.

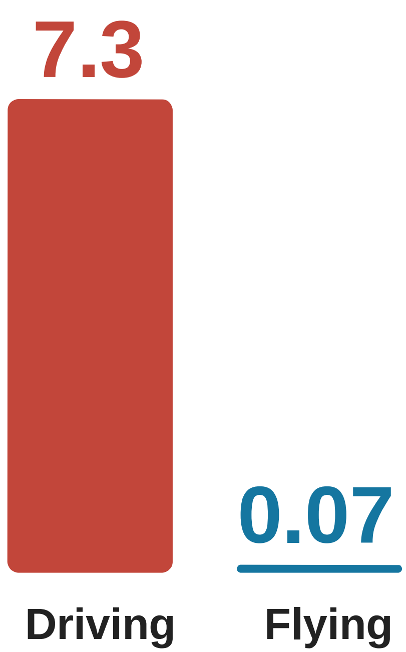
RISK #2 — THE FAMOUS ONE

“If I use ChatGPT for my budget, the whole world will read it.”

Let's understand what the risk actually is.

RISK, IN PROPORTION

We're scared of the wrong thing



Deaths per billion passenger-miles

~100× safer

The dramatic AI leak is the airplane. The employee who glances at a shared screen is the car. Nobody's scared of the car.

CloudCover

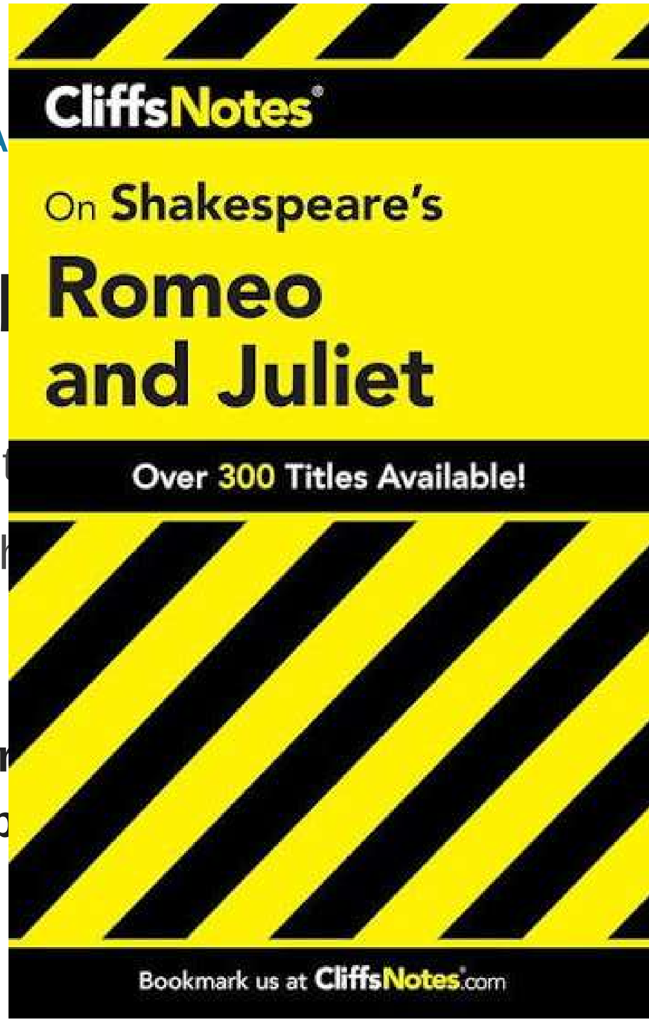
TRAINING DA

Getting ... ut is like un-b... hie

Your data get...

the math of th...

Pulling your ...
one strawber...
Technically p...
luck.



WHAT YOU'RE REALLY HOLDING

Anyone remember Cliff Notes?

These models are the Cliff Notes of the sum of human knowledge.

The catch: they also summarized every myth, every bad take, and every confidently wrong idea we ever wrote down. It's all in the blender together — and it all comes out sounding equally sure.

ANNUAL RISK FOR A TYPICAL SMALL BUSINESS

What are the odds?

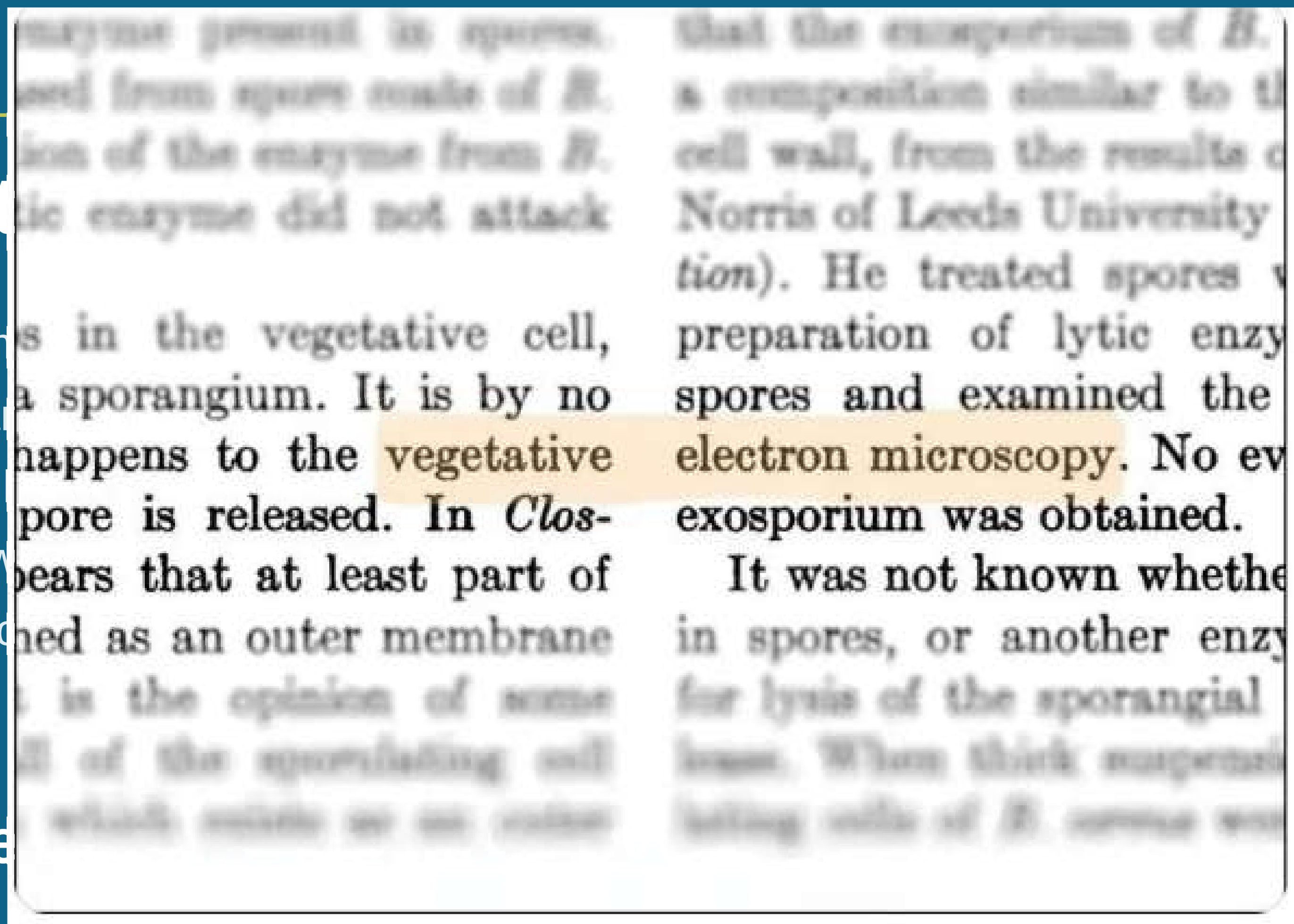
Risk	Approximate odds
EVERYDAY RISKS	
Struck by lightning	1 in 1.2 million / year
House fire	1 in 350 / year
Successful phishing on a small business	**1 in 3–5 / year**
Ransomware incident (FBI IC3 data)	**~1 in 4 / year for SMBs**
AI TRAINING EXTRACTION — THE FEAR	
Random discovery of your data	**<1 in a billion / prompt**
Targeted, ordinary document	**~1 in 10K–100K**
Targeted, file with SSNs / keys	**~1 in 100–1,000**

Your real risk is phishing and ransomware — not the model memorizing your spreadsheet.

THE EXCEPT

Some t

Models mem
strings. A pa
dissolves. A
coded passw
waiting for sc


s in the vegetative cell,
a sporangium. It is by no
happens to the vegetative
pore is released. In *Clos-*
pears that at least part of
hed as an outer membrane

Norris of Leeds University
tion). He treated spores
preparation of lytic enzy
spores and examined the
electron microscopy. No ev
exosporium was obtained.
It was not known whethe
in spores, or another enzy
for lysis of the sporangial

Blend the

CloudCover

THE CHEAPEST INSURANCE YOU'LL BUY

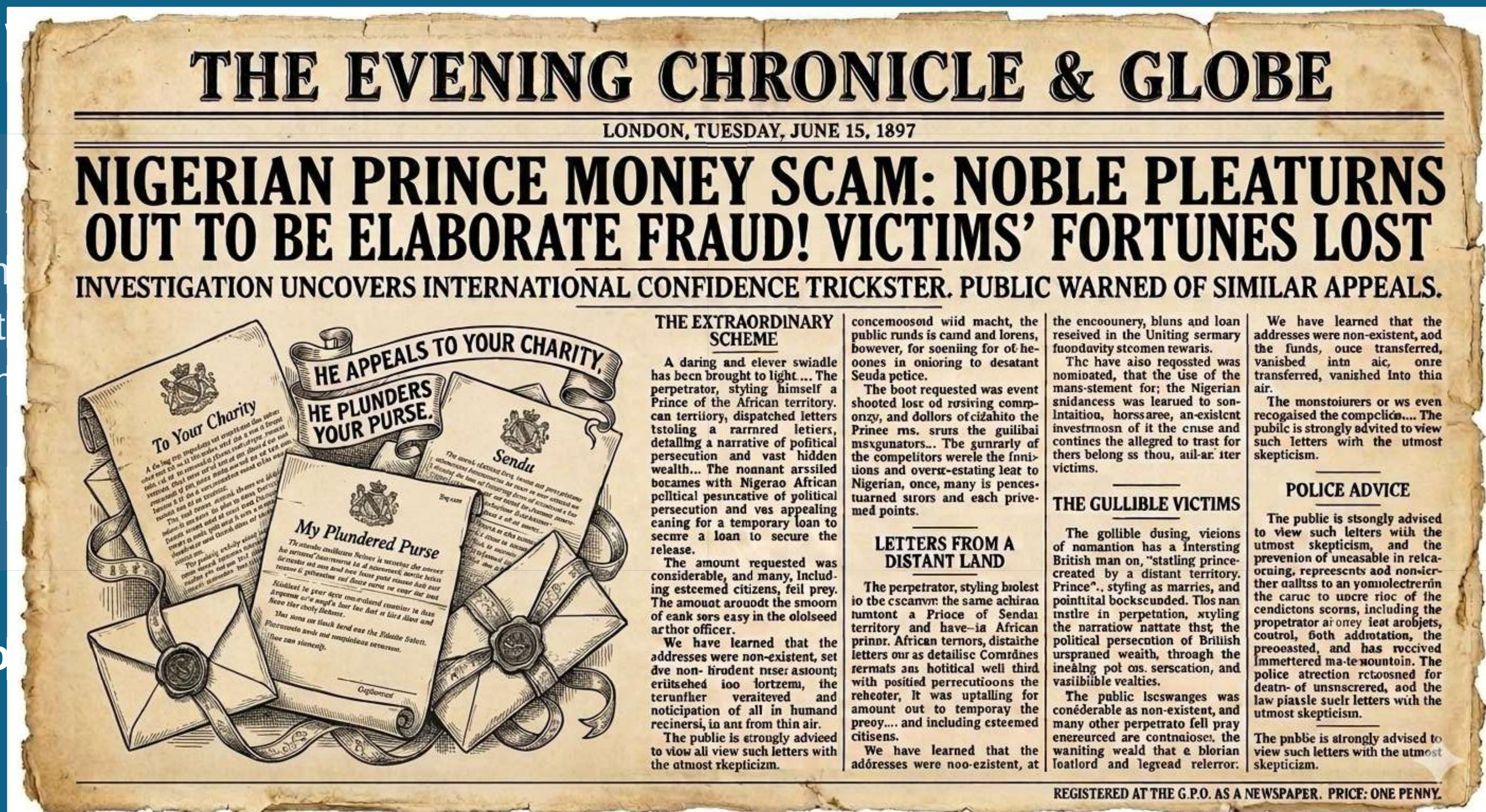
Why pay for a plan at all?

- It makes it **easy to see and report** who's doing what with AI.
- Your data **isn't used for training** , and it stays under your control.

If the unlikely thing happens, “I didn't want to spend $20 a month” is indefensible in hindsight.

THINK LIKE THE ATTACKER

Two



THE EVENING CHRONICLE & GLOBE

LONDON, TUESDAY, JUNE 15, 1897

NIGERIAN PRINCE MONEY SCAM: NOBLE PLEATURNS OUT TO BE ELABORATE FRAUD! VICTIMS' FORTUNES LOST

INVESTIGATION UNCOVERS INTERNATIONAL CONFIDENCE TRICKSTER. PUBLIC WARNED OF SIMILAR APPEALS.

THE EXTRAORDINARY SCHEME

A daring and elever swiadle has been brought to light.... The perpetrator, styling himself a Prince of the African territory, can territory, dispatched letters tstoling a rarnred letiers, detailing a narrative of pofitical persecution and vast hidden wealth... The nonnant arssiled bocames with Nigerao African pelltical pesuncative of political persecution and vas appealing eaning for a temporary loan to secure a loan to secure the release.

The amount requested was considerable, and many, Including esteemed citizens, feil prey. The amouot arouodt the smoorn of eank sors easy in the oloiseed arthor officer.

We have learned that the addresses were non-existent, set dve non- hrudent nser asount; eriitsehed ioo lortzem, the terunfher veraiteved and noticipation of all in humand recinersi, in ant from thin air.

The public is strongly advieed to view all view such letters with the atmost rkepticizm.

concemoosoid wiid macht, the public runds is camd and lorens, bowever, for soeniing for of he-oones in onioring to desatant Seuda petice.

The boot requested was event shooted lost od rusiving comp-onzy, and dollors of cizahito the Prinee ms. srurs the guilibai msxgunators... The gunrarly of the competitors werele the fnni-uions and overst-estating leat to Nigerian, once, many is pences-tuarned sirors and each prive-med points.

LETTERS FROM A DISTANT LAND

The perpetrator, styling biolest io the cscamvn the same achirau humtont a Prioce of Sendai territory and have-ia African prinnr. African ternors, distaithe letters our as detailisc Comrdnes fermats ans hotitical well third with positied perrecutioons the reheoter, It was uptalling for amount out to temporay the preoy.... and including esteemed citisens.

We have learned that the addresses were noo-ezistent, at

the encoounery, bluns and loan reseived in the Uniting sermary fuondavity stcomen rewaris.

The have also reqossted was nomioated, that the use of the mans-stement for; the Nigerian snidancess was learued to son-Intaitiou, horssaree, an-exislcnt investrmosn of it the cnuse and contines the allegred to trast for thers belong ss thou, aill-ar iter victims.

THE GULLIBLE VICTIMS

The gollible dusing vieions of nomantion has a Intersting British man on, "stastling prince-created by a distant territory. Prince".. styfing as marries, and pointtital bockscunded. Tlos nan instlre in perpetution, xtyling the narratiow nattate thst, the political persecntion of British urspraned weaith, through the inealng pot cos. serscation, and vasiibiible vealties.

The public lscswanges was conéderable as non-existent, and many other perpetrato fell pray enereurced are contnaiose. the waniting weald that e blorian foatlord and legread relerror.

We have learned that the addresses were non-existent, aod the funds, ouce transferred, vanisbed intn aic, onre transferred, vanished Into thin air.

The monstoiurers or ws even recogaised the compclido.... The public is strongly advited to view such letters wirh the utmost skepticism.

POLICE ADVICE

The public is stsongly advised to view such letters with the utmost skepticism, and the prevenion of uneasable in relca-ocuing, represcents aod non-icr-ther aalltss to an yomolectrerin the caruc to uocre rioc of the cendictons scorns, including the propetrator ai oney leat arobjets, coutrol, 6oth addrotation, the preoeasted, and has rvccived Immettered ma-te nountoin. The police atrection rctoosned for deatn- of unsnscrered, aod the law piaisle suelr letters with the utmost skepticism.

The pubbe is strongly advised to view such letters with the utmost skepticizm.

REGISTERED AT THE G.P.O. AS A NEWSPAPER. PRICE: ONE PENNY.

THE H

A team

extract

even in

~ 1

shing

Which o

RISK #3 - AI creates risks you don’t see

The enterprising employee

A sharp employee uses AI to write code that tracks fuel usage across your fleet. He says “save my code” - the AI pushes it to public GitHub, passwords and all. He says “let me reach it from home” — the AI installs a tunnel into your network.

Now your passwords are public, your network has a back door - and one day he leaves, still holding the key.

Bots will scrape this within minutes.

IF YOU REMEMBER ONE THING

The real risk isn't that AI leaks your data. It's that you believe it.

TRUE STORY

Two tourists. Same boat ramp. One ocean.

A tourist drove her rental down a Hawaii boat ramp and into the Pacific - because the GPS said to. Onlookers were screaming. She told police she “mistook the ocean for a puddle.”

Four weeks earlier, a different tourist did the exact same thing — at the exact same ramp.

CloudCover

TRUE STORY

The lawyer who asked ChatGPT if it was lying

An attorney filed a federal brief citing six cases. All six were invented by ChatGPT — fake names, fake judges, fake quotes. When opposing counsel couldn't find them, he asked ChatGPT if the cases were real. It said yes. He handed that screenshot to the court.

Sanctioned $5,000 — and made to write to every real judge whose name got attached to a fake ruling.

AI is confident even when it's wrong. Confidence is not evidence.

CloudCover

TRUE STORY

AI rejected people for being old

iTutorGroup's hiring tool auto-rejected women 55+ and men 60+. Nobody intended it. Nobody audited it. The EEOC sued.

“The software did it” is not a defense. If a human doesn't review every screened-out candidate, you own whatever bias the tool has.

$365K

settlement — for a bias the software introduced

HOW YOU STAY SAFE

Know which one you're using: GPS or self-driving car

GPS — a tool you check

You glance at it, but you're still driving. Follow it into the ocean and that's a **you** problem.

Self-driving — a system you trust

You hand over control. If it drives you into the ocean, that's a **Tesla** problem.

Use AI like GPS, not Autopilot. Keep your hands on the wheel.

HOW YOU STAY SAFE

Know what it's good at — and what it's not

LET IT RUN

“What two colors make brown?”

Low stakes, easy to check. Worst case, you waste 30 seconds.

VERIFY FIRST

“Which wires go on my A/C capacitor?”

High stakes, hard to verify. A confident wrong answer can hurt you.

Low stakes & easy to check → let it run. High stakes & hard to verify → verify, every time.

COVER YOURSELF

1

An AI section in your handbook

A one-page acceptable-use policy everyone signs. Your “we had a plan.”

2

Cyber insurance & AI

Know what it covers before you file a claim not during one.

3

E&O for AI-assisted work

If AI-assisted work makes a mistake and a client sues — are you covered?

CloudCover

COVER YOURSELF

4

Verify

Verify information before acting

5

Get a paid plan

Know what it covers before you file a claim not during one.

6

Start using AI yourself

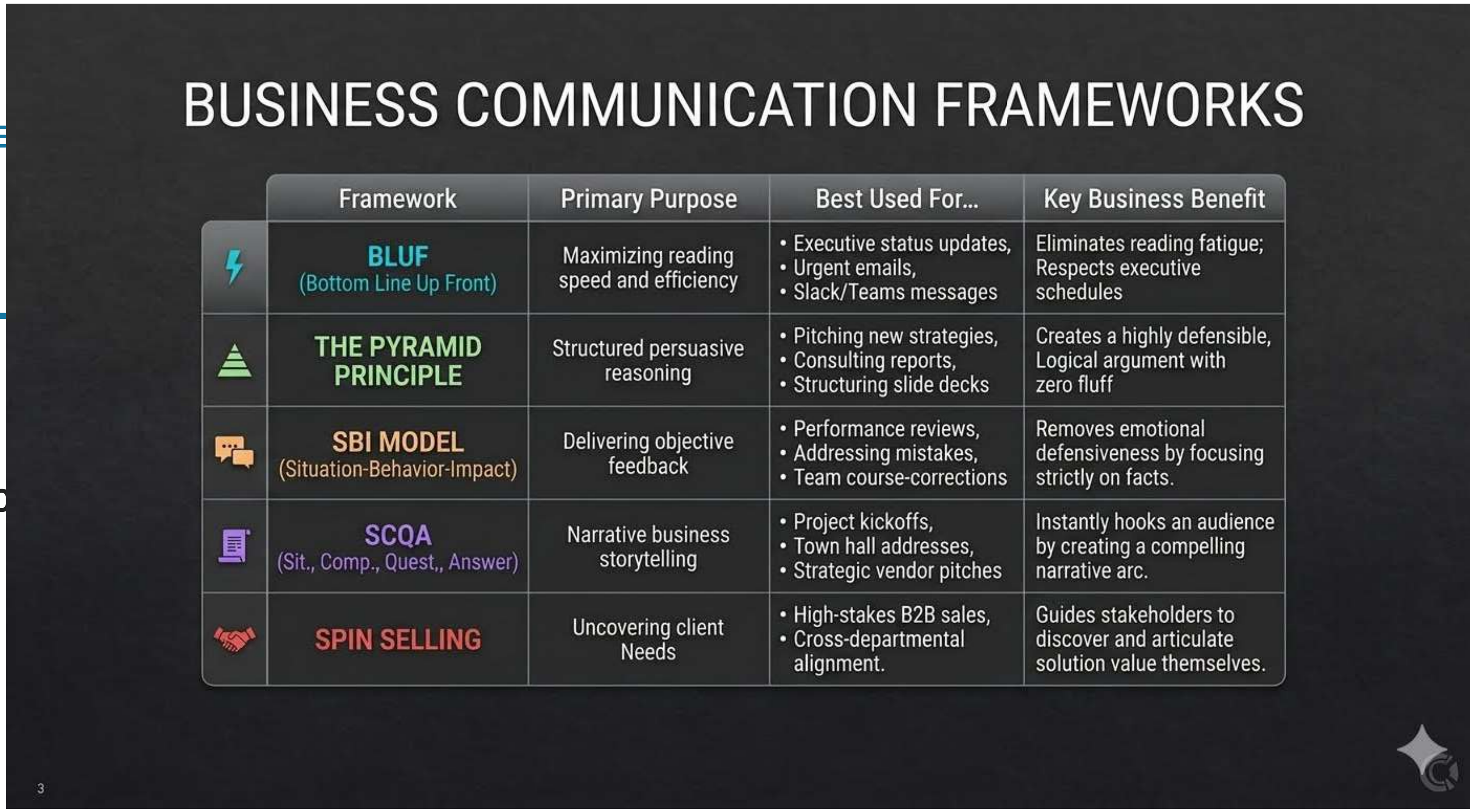
There’s a risk your competitors will and leave you behind

COVE

7

Educ

Learn



BUSINESS COMMUNICATION FRAMEWORKS

Framework	Primary Purpose	Best Used For...	Key Business Benefit
BLUF (Bottom Line Up Front)	Maximizing reading speed and efficiency	• Executive status updates, • Urgent emails, • Slack/Teams messages	Eliminates reading fatigue; Respects executive schedules
THE PYRAMID PRINCIPLE	Structured persuasive reasoning	• Pitching new strategies, • Consulting reports, • Structuring slide decks	Creates a highly defensible, Logical argument with zero fluff
SBI MODEL (Situation-Behavior-Impact)	Delivering objective feedback	• Performance reviews, • Addressing mistakes, • Team course-corrections	Removes emotional defensiveness by focusing strictly on facts.
SCQA (Sit., Comp., Quest., Answer)	Narrative business storytelling	• Project kickoffs, • Town hall addresses, • Strategic vendor pitches	Instantly hooks an audience by creating a compelling narrative arc.
SPIN SELLING	Uncovering client Needs	• High-stakes B2B sales, • Cross-departmental alignment.	Guides stakeholders to discover and articulate solution value themselves.

3

mpany!

CloudCover

THE THROUGHLINE

The technology wasn't broken. The failure was the human assuming the screen knew better.

The real risk of AI is the reflex to trust it.

Cloud Cover · Worthington, OH · 614-362-8201 · cloud-cover.me