



Assume Leaked.

Seven questions to ask
your CISO this week.

Swipe →

ASSUME LEAKED

Start from one assumption:

**some of our confidential
data is already
inside a public LLM.**

Not maybe.

Already.

1

**Which of our data
would actually hurt
us if it surfaced?**

Name the top five
datasets, not "everything".

2

Which contracts promise a confidentiality we can no longer guarantee?

Client NDAs, DORA and NIS2 obligations, GDPR processor terms.

3

**Which three workflows
push people to
unapproved tools,
and what approved
tool replaces each?**

4

Can we see what leaves?

Do we log prompts on approved tools, and do we know which unapproved tools are in use?

5

**What is our answer when
a client asks “has our data
been in your AI tools?”**

Have we written it down?

6

What breaks if a model vendor has a breach tomorrow?

Keys, documents, system prompts, customer data?

7

What would resilience look like instead of a ban?

Training, approved tools, a data classification people actually use.

ASSUME LEAKED

Good answers to all seven?

You are ahead of most companies.

Not yet?

This is the work for Q4.

Pushback welcome, I will
be saying this on stage.