



Attache Group Inc.
Information Technology Managed.

Copilot, Gemini & Information Information Security Readiness Readiness

Presented by

Steve Blanken · Attache Group · June 2026



AI Didn't Create These Risks

It just turned up the volume on old ones



The same fundamentals

These are the data governance and security basics that have always mattered — long before AI.



AI turns up the volume

Oversharing and stale data were quiet risks. An AI assistant actively finds and surfaces all of it.



A policy is just the manual

An AI policy tells staff what's approved and how to use it — useful, but not the real work.



Fix the foundation

On a cracked foundation, AI isn't a productivity boost — it's an exposure engine.

It boils down to three elements



Least Privileged Access

Access by job role, and nothing more — more access, more problems.



Data Governance

Know it, label it, dispose of it — having access doesn't mean it's AI-eligible.



Approved Tools

Only sanctioned tools and compliant devices ever touch your data.

More access means more problems



Define by role

People should reach the resources their job needs — and nothing beyond that.



The shared-folder trap

A combined HR and Accounting share hands everyone access they were never meant to have.



AI makes it real

The assistant sees everything a user can see — and it will pull from all of it.

The best-laid plans only work if they're followed



Meaningful, not maximum

Put barriers where they matter.
Don't create five shares per role —
no one can maintain that.



Operation rests with people people

Day-to-day security lives with the
staff handling the data, not with a
framework on paper.



Realistic over perfect

Security that gets bypassed isn't
security. Strike an achievable
balance and train for it.

The Data Lifecycle

Policies for every stage, from intake to disposal



1 · Intake

How data enters the organization, and where it's supposed to land when it arrives.



2 · Storage

Where it lives – in the right place, with the right protections and confidentiality labels.



3 · Sharing

Who it can go to, and under what controls. Having access doesn't make it AI-eligible.



4 · Disposal

Getting rid of data at the end of its useful or regulatory life – the stage everyone forgets.

Why Disposal Wins

You can't lose what you no longer have

01

Attackers can't steal it

Properly deleted data simply isn't there to be taken in a breach.

02

Insiders can't reach it

No employee — curious or disgruntled — can access what no longer exists.

03

AI can't surface it

Deleted data can't be indexed or regurgitated in a Copilot or Gemini summary.

The Side Door Problem

Don't build a moat and leave a side door open



Permissive by default

Out of the box, cloud vendors let end users connect third-party apps to their data.



One click, full access

An unreviewed app can read files, calendars, and meetings — bypassing every control you built.



Require approval

Connecting a tool to your data should need review, not an end user's good intentions.



Compliant devices only

A personal laptop running arbitrary software is just another side door into your data.

The path is already mapped



ISO · CIS · NIST

Everything here is already covered in mature, documented security frameworks — built and tested by people who solved these exact problems.



Proven and prescriptive

They give you the controls and checklists for access, governance, and tenant security.



AI just adds urgency

AI accelerates the journey down a trail that's already well marked. The destination hasn't changed.

Get the Foundation Right First

Five things to do before you flip the switch

1 · Tighten access

Define roles and grant least privilege.
More access, more problems.

2 · Govern the lifecycle

Intake, storage, sharing, disposal — with labels on what's sensitive.

3 · Lock the side door

Require approved tools and compliant devices to reach your data.

4 · Train your people

The framework lives in daily habits, not in a document.

5 · Then turn on AI

Let it accelerate good practice instead of amplifying neglect.



Attache Group Inc.
Information Technology Managed.

Questions? Let's Talk

Thanks for your time

