

Article

Oct 2026

Secure AI adoption: cyber brakes make you go faster

AI adoption is happening in your business whether you've signed off on it or not. The question is whether you're steering it or chasing it.



David Dove

Senior Information Security Consultant

Email david.dove@waterstons.com

In Formula 1, good brakes let the driver commit fully into every corner, trusting that the car will do exactly what's needed. Cyber security in AI adoption works the same way: strong access controls, data governance, monitoring and clear usage policies aren't there to slow you down, they're what let the business move fast without ending up in the barriers.

Without controls you can trust, people tend to operate in one of two ways:

- **Crash mode:** AI gets used without proper controls. Data is leaked, models are manipulated, and the business suffers a breach that sets AI adoption back years.
- **Handbrake mode:** the exec team, worried about exactly that risk, pulls the handbrake and keeps AI away from real work. Competitors race past while the car sits in the garage

A ban simply pushes AI underground. Staff who need AI to do their jobs will use it anyway, off the radar and outside any controls. That's shadow AI, and it's harder to manage than AI you actually know about.

It's already happening at scale. Among UK businesses that are using, adopting or considering AI, only 24% have cyber security practices in place to manage the risk according to the [Cyber Security Breaches Survey 2025/2026](#). And just 5% have a formal written AI policy, as reported in the [UK Business Data Survey 2026](#).

Shadow AI isn't a fringe problem. For most organisations, it's the default position.

The highly cited Samsung case from 2023, where employees pasted proprietary source code into a public AI tool, is still a fair illustration, but it's an old one. Today's risks are sitting inside your own business: internal copilots and chatbots rolled out without the same scrutiny as customer-facing systems, AI features embedded in everyday tools, agents taking actions no one explicitly signed off. Same risk, closer to home, and harder to spot because it looks like it was already approved.

Clear guardrails do the opposite of a ban. They let you deploy AI with confidence, and give your exec team the assurance it's being done safely, responsibly and transparently.

So where do I start?

Understand your AI readiness

Get a clear picture before you move:

- Does your leadership believe in the benefits of AI?
- What are the real risks of using it in your organisation?
- What data privacy and security obligations do you need to meet?
- Where could AI genuinely help?
- What access to AI tools do you already have through existing systems?
- What data would AI need access to? (plus is that data in a useable, integration-ready format?).

Establish AI governance

None of this is glamorous. But it's also the bit that stops you explaining a breach to the board.

- Build an AI asset inventory – know where AI is used, or could be used, so nothing sits in the shadows.
- Run a risk assessment – evaluate the security and privacy risks of AI in your business. Where AI processes personal data of staff or customers, follow ICO guidance, including a Data Protection Impact Assessment (DPIA) as a minimum.
- Approve a list of tools that meet your security, privacy and compliance requirements, communicate the list clearly, and review it regularly as technologies, risks and business needs change.
- Write a clear acceptable use policy, to formalise rules on what's allowed and what isn't. Covering things like data sharing and use of public tools.
- Assign clear accountability – give appropriate individuals responsibility for overseeing AI use and governance. Depending on your organisation's size, structure and level of risk, this could be an accountable senior leader, an existing governance group or a cross-functional committee involving areas such as IT, security, legal and data protection.
- Keep humans in the loop for review and sign off on anything high-risk, such as recruitment or financial decisions.
- Set up an AI working group – bring in the people keen to use AI so they help shape the guidelines, controls, and use cases, rather than working around them.
- Raise awareness of AI threats – make sure staff know what to look out for: AI-generated content, deepfakes, AI-enhanced phishing, and misinformation.

Put safe use into practice

- Train staff on an ongoing basis, focused on how to use AI safely rather than just what is banned.
- Back that up technically: data loss prevention tooling to stop sensitive information reaching public tools, web and application filtering so staff can only reach approved applications
- Manage third-party risk – check how your suppliers use AI to make sure their practices don't undermine your data security and privacy.

Keep optimising

- Monitor continuously – track AI system behaviour and unapproved tool use, and audit regularly to catch anomalies early
- Measure the benefits – check that AI is actually delivering what you expected, and look for further opportunities as you go.

The organisations getting the most out of AI aren't the ones taking the biggest risks. They're the ones building trust, governance and security into their adoption from day one. Security and privacy aren't obstacles to innovation. They're the foundations that let you use AI with confidence and get long-term value from it.

Five questions to put to your exec team

1. What business outcomes are we trying to achieve with AI?
2. What data will AI need access to?
3. How will we manage privacy and regulatory obligations?
4. Which AI tools are approved for use?
5. Who is accountable for AI governance?

If you can answer all five with confidence, you're in good shape. If not, that's a conversation worth having before AI finds the gaps for you.

To get a clear view of where you stand and what to do next, talk to us about our [AI maturity assessment](#).
