

AVION CONSULTING

EXECUTIVE PERSPECTIVE

The Executives Are the Shadow AI Problem

Most governance conversations assume unsanctioned AI use starts with junior staff. The data points the other way, directly at the leadership table.

65% vs 31%

Senior decision-makers are more than twice as likely to use unapproved AI tools as the employees they manage

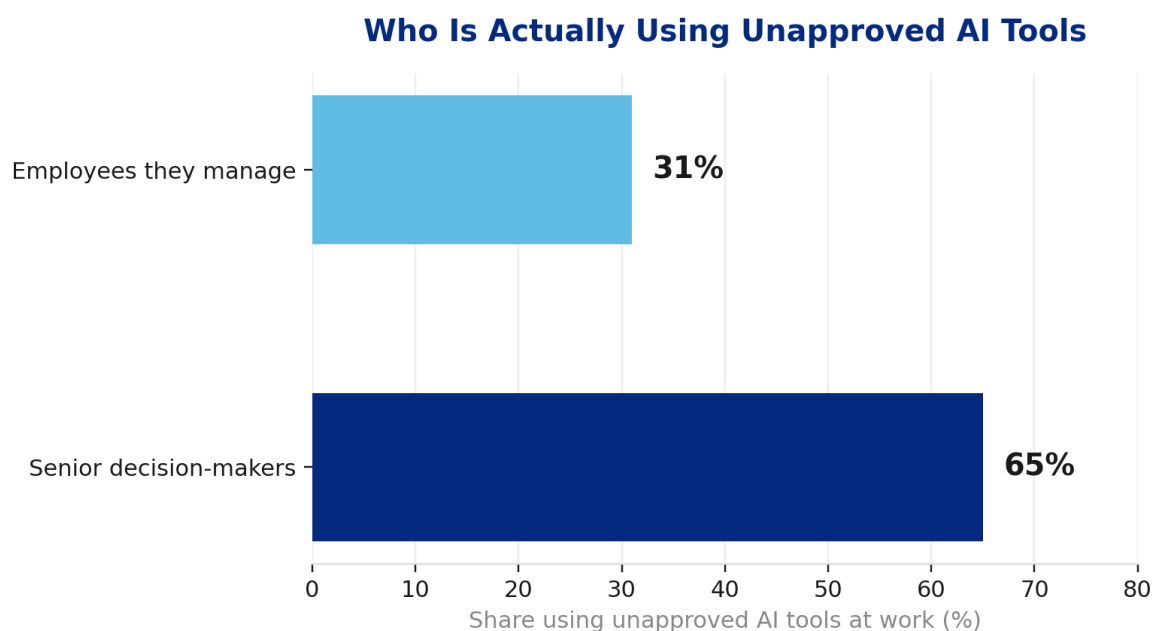
Nazma M. Rosado

Principal Consultant, Avion Consulting

nrosado@avionconsulting.com | avionconsulting.com

The Assumption Everyone Makes

Ask most IT and security leaders which employees worry them most on shadow AI, and the answer is usually some version of the digital native junior hire routing around policy with a personal chatbot account. That assumption is wrong, and the direction of the error matters. Original research conducted with Censuswide across more than 2,000 UK and US employees in March 2026 found senior decision-makers are more than twice as likely to use unapproved AI tools than the people who report to them, 65 percent compared with 31 percent.



Source: TrustedTech / Censuswide research, March 2026

Unapproved AI tool use by seniority level.

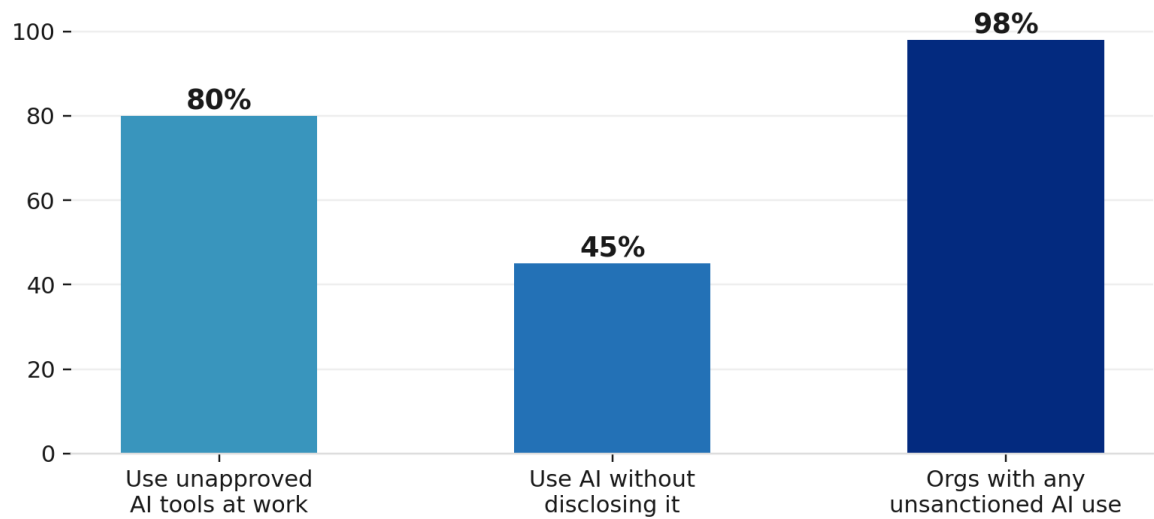
The governance risk most security teams are watching for is running directly out of the offices of the people who set the policy in the first place. That inverts the usual playbook of training the frontline and trusting leadership to model the behavior.

The Scale Underneath the Headline

This is not a fringe problem contained to one function or one generation. More than 80 percent of workers report using unapproved AI tools in their jobs, with fewer than one in five relying only on

sanctioned solutions. Forty five percent of US workers admit to using AI at work without disclosing it. Nearly every organization surveyed, 98 percent, has at least some employees using AI tools outside approved channels. Detections of shadow AI activity in enterprise environments rose fourfold in a single year according to Verizon's 2026 Data Breach Investigations Report.

The Scale of Unsanctioned AI Use



Source: SQ Magazine and Second Talent shadow AI research, 2026
The scale of unsanctioned AI use across the workforce.

The Numbers at a Glance

Metric	Figure	Source
Senior decision-makers using unapproved AI tools	65%, vs. 31% of employees they manage	TrustedTech / Censuswide, March 2026
Workers using unapproved AI tools generally	Over 80%	SQ Magazine, 2026
Organizations with any unsanctioned AI use	98%	Second Talent, 2026
Office professionals using AI against known policy	66%	PagerDuty Shadow AI Survey, 2026
Year-over-year rise in shadow AI detections	4x	Verizon 2026 Data Breach Investigations Report

Why the Ban Doesn't Work

The instinct in a lot of boardrooms is to tighten the policy and increase the warnings. That approach has already been tried and it has not moved the number. Two thirds of office professionals report using AI tools at work despite believing the use was against company policy, often while feeding sensitive business data into public models in the process. The data entering unsanctioned tools now regularly includes source code, client proposals, HR records, and financial documents.

63%

Of organizations cannot enforce purpose limitations on their own AI agents, according to the Kiteworks 2026 Data Security, Compliance and Risk Forecast Report

Two Different Jobs to Do

For the CEO

This is a modeling problem before it is a policy problem. If you or your direct reports are using AI tools your own security team has not approved, no acceptable use policy below you will hold. The fastest fix costs nothing: disclose what you personally use, why, and what you have decided not to use, in front of the leadership team.

For the CHRO

Shadow AI usually gets filed as an IT and security issue. The root cause, unclear expectations and slow approved alternatives, sits squarely in your territory. Employees are not defying policy for the thrill of it. They are choosing speed over process because the sanctioned path is slower than the deadline in front of them.

The Incentive Problem Hiding Underneath

Research from Microsoft in 2026 found that only 13 percent of AI users say they are rewarded for reinventing their work with AI when results are not guaranteed. That single number explains a great deal of the behavior above. When the sanctioned path is slow and the unsanctioned path is fast, and experimentation outside approved channels carries no visible penalty while missing a deadline does, the rational choice for a capable, motivated employee is the one the policy was written to prevent.

This is why organizational factors, not individual mindset, determine whether AI investment converts into real outcomes. Microsoft's 2026 research attributes 67 percent of AI's actual business impact to organizational structure and culture, versus 32 percent to individual enthusiasm for the technology. The lever that works is structural, not motivational.

What This Actually Requires

This is not a training problem you solve with an all hands reminder. It is a leadership behavior problem wearing a technology costume. If the people setting AI policy are also the people most likely to work around it, the fix starts above the org chart line where the policy gets written, not below it. Boards that have made real progress on this are not the ones with the strictest acceptable use policy. They are the ones where the executive team uses the sanctioned tools visibly, names the tradeoffs out loud, and treats convenience as a reason to build better approved options rather than a reason to look the other way.

References

1. TrustedTech, "Bosses Using Banned AI Are the Biggest Threat to Workplace Data Security," original research with Censuwide, March 2026.
2. SQ Magazine, "Shadow AI Usage Statistics 2026: Latest Insights," March 31, 2026.
3. Second Talent, "Top 50 Shadow AI Statistics 2026: The Risk of Unsanctioned AI Tools," citing IBM, ISACA, and Reco AI research, updated May 12, 2026.
4. PagerDuty, "Shadow AI Is Happening Within Your Organization," 2026 Shadow AI Survey conducted by Wakefield Research, June 11, 2026.
5. Tech Times, "Shadow AI Cybersecurity Risk Spikes as 45% of Workers Use Unsanctioned Tools," citing Verizon 2026 Data Breach Investigations Report, June 16, 2026.

6. Kiteworks, "2026 Data Security, Compliance and Risk Forecast Report," cited in "AI Governance in 2026: Why Boards That Wait Will Inherit an Ungovernable Mess," May 20, 2026.