TAKING THE INITIATIVE

Rajat Bhargava *explores ways to step out from Shadow AI and turn risk to strategic advantage*

For years, shadow IT has been seen as a threat, an unmonitored and uncontrolled force undermining corporate policies, creating security gaps and circumventing procurement channels. If you're an IT professional working at a mid-sized organisation, there's a 90 percent chance you're worried about shadow IT, and rightfully so, it's become the second-most common cyber attack vector (following phishing attacks) with shadow IT linked to 37 percent of cyber attacks against SMEs.

With generative AI exploding across every corner of the enterprise, we're seeing the rise of a new iteration: shadow AI. Employees are integrating ChatGPT, Claude, Gemini and other tools into their workflows, often without the oversight of IT teams.

On the surface, this seems like deja vu: another technology movement threatening security, governance and operational cohesion. But dismissing or cracking down on shadow AI could be a missed opportunity. Forward-thinking organisations should see it as a signal of unmet need and a chance to turn decentralised experimentation into a strategic asset.

JumpCloud's recent report revealed a growing concern among IT professionals, with nearly 90 percent expressing anxiety over the risks associated with unsanctioned applications and devices. For the majority of employees, shadow AI has provided support with everyday tasks, from writing code or marketing copy, automating spreadsheets or summarising documents.

The fact that employees are adopting these tools on their own reveals something important: they are eager for greater efficiency, creativity and autonomy. Shadow AI often emerges because enterprise tools lag what's available in the consumer market or because official processes can't keep pace with employee needs.

Much like the early days of shadow IT, this trend is a response to bottlenecks. People want to work smarter and faster, and AI offers a shortcut. The instinct of IT and security teams might be to block access, issue warnings and attempt to regain control. This adversarial approach may work short term, but is unsustainable in the long run. Instead, organisations should look into channelling this grassroots momentum into something secure, scalable and strategic.

Rather than seeing these tools as a threat, leaders should view them as a discovery engine, a window into how their workforce wants to solve problems. Employees using AI independently are effectively prototyping new workflows. The question isn't whether they should be doing it, but how organisations can learn from and build on it.

What tools are employees using? What are they trying to accomplish? What workarounds are they creating? This bottom-up intelligence can inform top-down strategies, helping IT teams understand where existing solutions fall short and where there's potential for innovation.

Once shadow AI is acknowledged, IT teams can move from a reactive to a proactive stance, offering secure, compliant alternatives and frameworks that allow for experimentation. This might include vetted AI platforms, sandbox environments or policies that clarify use without stifling initiative.

The key to harnessing shadow AI lies in striking a balance between control and empowerment. Employees need guidance, they don't need to be micromanaged. This means establishing policies that ensure sensitive data is protected, AI outputs are validated and regulatory requirements are met. But it also means leaving room for exploration and trial and error.

Reclaiming shadow AI offers an opportunity to democratise AI literacy across the workforce. If employees are already experimenting, give them the training, support and resources to do so responsibly. Educating teams on bias, model limitations and data privacy isn't just good governance, it's good business.

Those who get ahead of shadow AI now will be better positioned for the next phase of enterprise transformation. Embracing this shift will allow organisations to unlock faster ideation, responsive workflows and a more engaged workforce.

There's a competitive edge in enabling employees to harness AI that aligns with business goals while maintaining security and compliance. Organisations that fail to engage with shadow AI will fall behind, not just in technology, but in agility, culture and talent retention.

Just as shadow IT eventually paved the way for cloud-first strategies, shadow AI has the potential to open a new era of decentralised, intelligent work. But only if leaders are willing to shift their perspective from gatekeepers to enablers ●

Once shadow AI is acknowledged, IT teams can move from a reactive to a proactive stance

Rajat Bhargava is CEO of JumpCloud.