The AI approval paradox: Why 2/3 of approved tools fail employees

Saturday 25 October, 2025

Related Sectors:

Computing & Telecoms ::

Scan Me:

Cybernews study reveals only 33% of employees find approved AI tools adequate, while shadow AI usage has surged to 59%, exposing the gap between IT approval and real-world usability.

Artificial Intelligence (AI) has moved from experimental to essential in record time. According to McKinsey's 2025 State of AI report, 78% of organizations now use AI in at least one business function, while their use of generative AI has increased to 71%.

However, widespread adoption masks failure in execution. According to the latest Cybernews survey, while 52% of employers have approved or provided AI tools for their workforce, only 33% of employees using those approved tools say they fully meet their work needs.

The result is that governance structures are failing to prevent the very vulnerabilities they were designed to address. Despite widespread awareness of the dangers, 59% of employees use unapproved AI tools, and 75% of them share sensitive company and customer data with these unauthorized applications, creating the very security breaches leadership aim to avoid.

Žilvinas Gir?nas, head of product at nexos.ai, a secure all-in-one AI platform for enterprises, explains why the approval paradox continues despite widespread awareness of security risks.

“This isn't a user problem but a procurement and implementation crisis. We're approving AI tools on promises and checklists, not on how well they fit work practices. Insufficient tools lead employees to bypass approval, risking customer data on unknown platforms,” he says.

The rise of “shadow AI”: A conflict between productivity and risk

The failure of approved tools is creating a dangerous trend known as “shadow AI.” This phenomenon describes employees using unauthorized software and platforms to get their work done, creating a massive blind spot for IT and security leaders. This practice results in a clash between the company's need for security and control versus the employee's interest in productivity and efficiency. Employees are rarely acting with malicious intent. They are simply seeking the convenience, speed, and features of AI tools that actually allow them to do their jobs better and faster.

Leadership then faces a dilemma — to either block the use of unapproved tools and risk losing a critical productivity edge or to permit their use and lose control over the company's most sensitive data. The potential risks are tangible. When employees use unapproved tools, 75% admit to sharing potentially sensitive information, including customer data, internal documents, financial records, and proprietary code. Once this data enters an unapproved AI platform, companies lose control over what happens to it. While these platforms have privacy policies, most employees never read them, and the policies themselves often permit data to be stored, used for model training, or even exposed to other users.

This leakage of intellectual property and confidential information increases a company's vulnerability to costly data breaches, a risk that can increase breach costs by an average of $670K, according to IBM. This entire shadow ecosystem often thrives in a corporate "gray zone," where official policies are either absent or quietly ignored by managers who also want their teams to perform.

“The gray zone exists because having a policy on paper doesn’t mean it is an effective one. Many organizations implement AI policies with just a simple ‘I acknowledge’ checkbox, without providing training, approved tools that work, or ongoing communication on how to apply the rules practically. When employees don't understand the policy or lack real alternatives, they make their own decisions. That's when sensitive data starts flowing onto platforms the company hasn't vetted. A policy is only as effective as the training, tools, and feedback systems that support it,” says Gir?nas.

Why sanctioned AI tools miss the mark

The disconnect between high adoption rates and low employee satisfaction is the direct result of a flawed, top-down implementation strategy common in many organizations. The problem often isn’t the technology itself, but an absence of planning and user involvement.

Leaders, rushing to participate in the AI boom, frequently make procurement decisions in a vacuum, choosing tools based on vendor promises or security checklists without a clear understanding of their teams' day-to-day workflows. This can lead to “innovation theater,” where companies adopt AI tools superficially to signal modernity but fail to integrate them into the business. When employees are not involved in the selection process, the result is predictable — a sanctioned tool that doesn't solve their problems.

This failure typically manifests in three critical areas:

1. **Limited functionality.** Companies approve generic, one-size-fits-all tools without understanding what different teams actually need, pushing employees toward unapproved alternatives built for their specific work.
2. **Poor workflow integration.** Approved enterprise tools are often standalone applications, disconnected from the daily systems where employees work.
3. **Lack of training and clear guidance.** Many organizations have a significant guidance gap, leaving employees without adequate training or support from leadership.

“The problem is that companies are treating AI adoption as a finish line. They buy a platform, check a box, and celebrate their ‘innovation,' but they skip the real work of changing processes and ensuring the tool actually solves a real-world problem for their employees. Employees aren't rejecting AI — they're rejecting a solution that was thrown over the wall at them without any thought. They’re left with a tool that feels more like a burden than a benefit,” says Gir?nas.

Practical steps forward

According to Gir?nas, solving the approval paradox requires a shift away from a top-down, tool-first mindset. He outlines four non-negotiables for organizations to build a secure and productive AI ecosystem.

1. **Map employee workflows before selecting tools.** Analyze daily workflows for different roles, from marketing to engineering, and identify friction points, data needs, and gaps. Use this map as a blueprint for selecting tools that solve real problems and drive meaningful adoption.
2. **Offer a secure sandbox, not just restrictions.** Creating a sanctioned alternative with a controlled environment provides access to powerful AI models with guardrails and audit trails. This meets employees' need for advanced tools while giving organizations control, turning a security risk into a managed asset.
3. **Implement a “living” policy with ongoing feedback.** Treat policies as living documents, not static ones. Create simple channels for employees to give feedback on tools and rules. This helps update policies to stay current, preventing them from becoming irrelevant as employees set their own rules.
4. **Identify internal AI champions.** Identify employees who are already seeing success with AI tools and create structured opportunities for them to showcase their workflows, share tangible results, and demonstrate the real-world changes they've achieved. This transforms AI adoption from a top-down process into a peer-driven one, where employees learn from colleagues who speak their language and understand their specific challenges.

ABOUT NEXOS.AI

nexos.ai is an all-in-one AI platform to drive secure, organization-wide AI adoption. Through a secure, web-based AI Workspace for employees and an AI Gateway for developers, nexos.ai enables companies to replace scattered AI tools with a unified interface that provides built-in guardrails, full visibility, and flexible access controls across all leading AI models—allowing teams to move fast while maintaining security and compliance. Founded in 2024 by Tomas Okmanas and Eimantas Sabaliauskas, who also co-founded several bootstrapped global ventures, including the $3B cybersecurity unicorn Nord Security and Oxylabs, nexos.ai addresses the urgent enterprise need to efficiently deploy, manage, and optimize AI models within organizations. Originating in the ecosystem of Lithuania-based tech accelerator Tesonet , the company attracted its first investment of €8M in early 2025 from Index Ventures, Creandum, Dig Ventures, and a number of prominent angel investors.

Company Contact:

_

Pressat Wire

E. support[@]pressat.co.uk

View Online

Newsroom: Visit our Newsroom for all the latest stories:
https://www.wire.pressat.co.uk