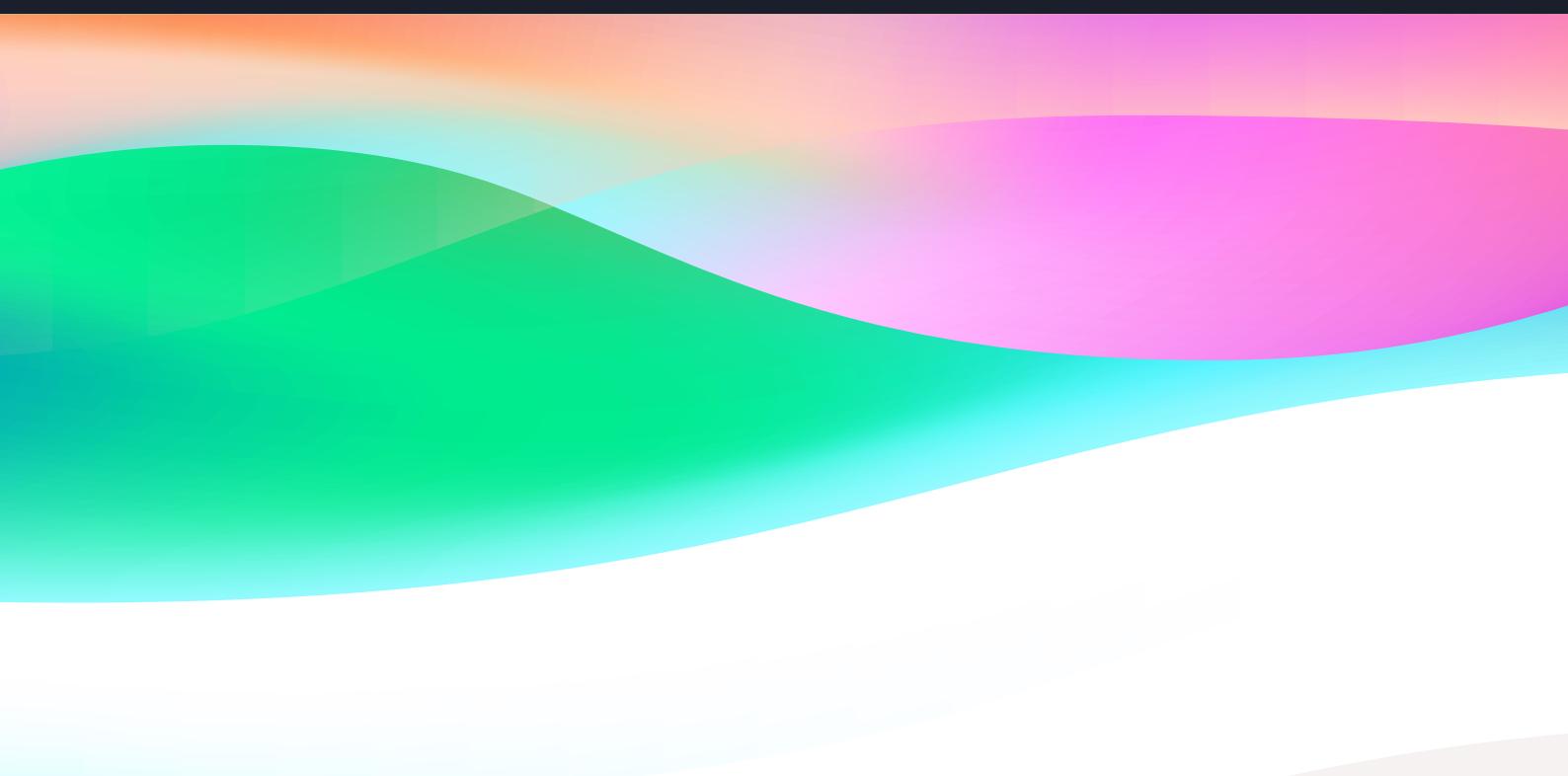




# The Insider AI Threat Report

Summer 2025





## The CalypsoAI Insider AI Threat Report

Originated by CalypsoAI, the leader in AI security, and gathered through *Censuswide*, an accredited third-party market research platform, this new data uncovers how today's workforce, from C-suite to entry level roles, are interacting with AI at work in light of – and more often despite – company policies. The findings illuminate an urgent need for enterprises to recognize and address the gravity of risks related to the internal use and misuse of AI within organizations, particularly in highly regulated sectors like banking, healthcare and security.

Crucially, these usage risks extend to the highest levels of these organizations. As the data shows, employees who are confused about or simply indifferent to rules about the secure use of AI tools in the workplace pose as great a threat to enterprise security and reputation as malicious threat actors.



Fear should never get in the way of innovation, but uncritical enthusiasm for technology can unravel progress just as fast. In the rush to adopt AI at scale, the lines between quick wins and true progress are becoming dangerously convoluted. Without the right awareness, blind eagerness will have detrimental impacts for enterprises when it comes to AI implementation.

We've seen this before. When cloud adoption took off, many enterprises rushed in without the controls, visibility, or shared responsibility models needed to manage it safely. AI is even more disruptive. It works and thinks like a human, and it's already reshaping how we define operational integrity, efficiency, and security.

We are now in an era where AI agents and employees are being put on the same pedestal. The key difference is that leaders have well-defined strategies to manage employees' risks and workflows, while agents are operating in sensitive environments unchecked, uncontrolled, and unprotected. Enterprises follow outdated traditional security methods to manage AI but fail to realize AI is not traditional.

Organizations need both technical controls and compliance, along with tools to educate employees and create a broader culture of respect for the power of AI.

**Donnchadh 'DC' Casey**  
CEO, CalypsoAI



01

# AI is Creating a Trust Transition in the Workplace

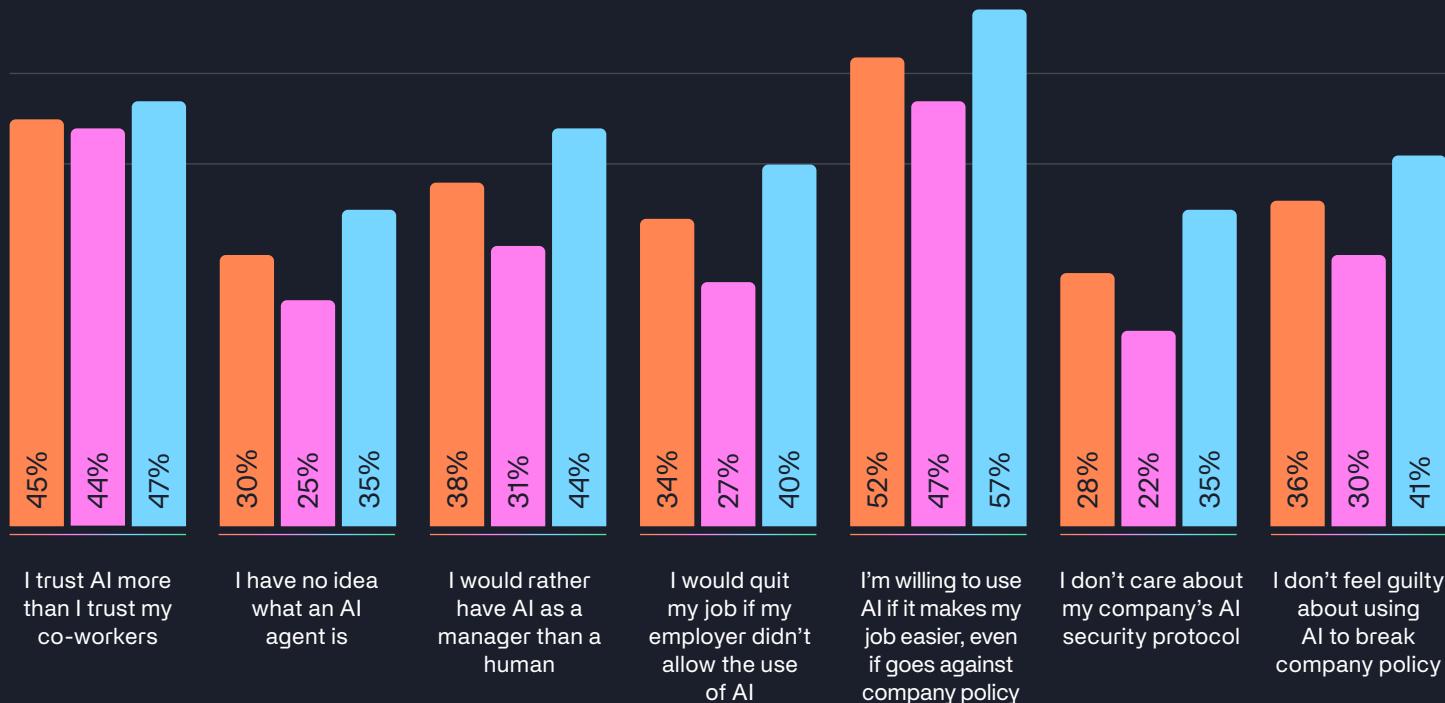
AI is no longer just a tool:  
it's becoming a trusted employee,  
and for some, a dealbreaker.



## Many employees prefer AI to human colleagues and managers

- 45% of employees say they trust AI more than their co-workers
- 38% would rather have AI as a manager than a human
- 34% would quit their job if their employer didn't allow the use of AI

### US Employee Sentiments Surrounding AI Use in the Workplace



#### Key

█ All    █ Highly regulated industries    █ Non-highly regulated industries



02

## Internal Misuse of AI

Forget the image of the hooded hacker, the real AI security threat is inside the building.

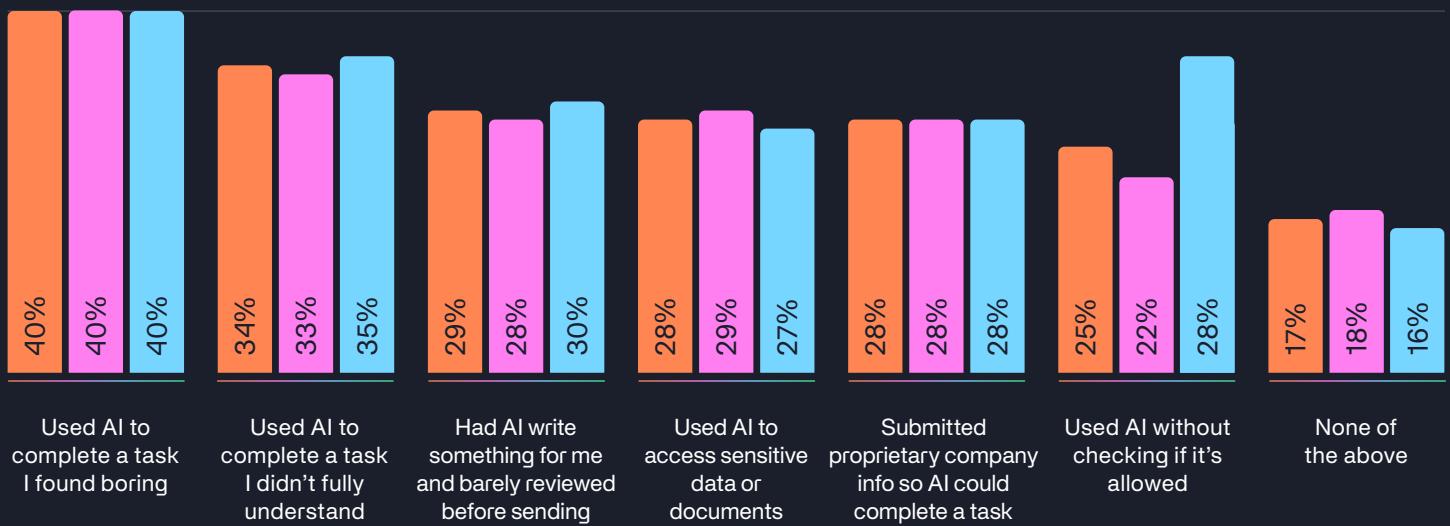


Employees increasingly see AI as a tool for efficiency or leverage, not a shared risk

- 52% of employees are willing to use AI to make their job easier, even if it means violating policy
- 28% of employees have already used AI to access sensitive data or documents
- 84% are somewhat or very confident their company's CEO/IT team would catch an AI-led breach

Blind faith dominates

Which, if any, of the following have you ever done with AI tools at work?



Key

All   Highly regulated industries   Non-highly regulated industries



03

# The C-Suite is Leading AI, but Doesn't Understand It

Lack of AI fluency at the top now  
poses a significant business risk.



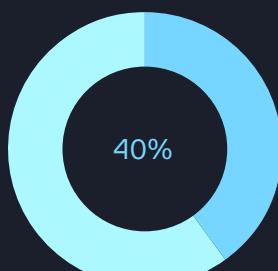
## C-level leaders are lacking AI comprehension

- **38%** have no idea what an AI agent is (the highest level of AI ignorance among all levels of seniority)
- **10%** can't tell the difference between an AI agent and a virtual employee

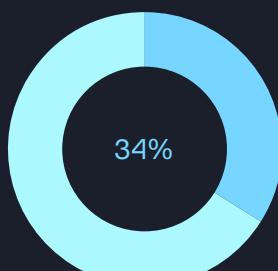
## ... but not AI enthusiasm

- **67%** are willing to use AI if it makes their job easier, even if it goes against policy
- **58%** say they trust AI more than they trust their co-workers
- **50%** say they'd prefer an AI manager over a human one

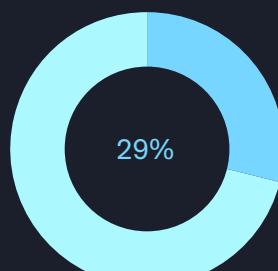
Which, if any, of the following have you ever done with AI tools at work?



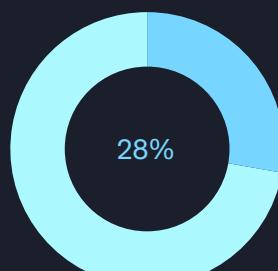
Used AI to complete a task I found boring



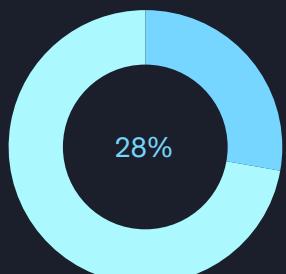
Used AI to complete a task I didn't fully understand



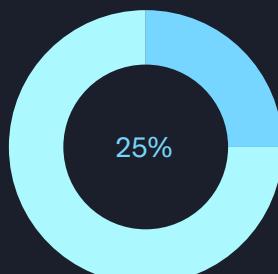
Had AI write something for me and barely reviewed before sending



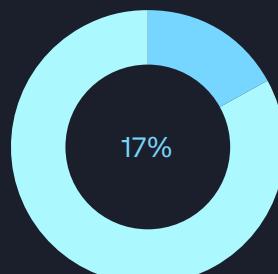
Used AI to access sensitive data or documents



Submitted proprietary company information so AI could complete a task



Used AI without checking if it's allowed



None of the above

Key  
C-Level executives



“Leaders are green-lighting AI faster than they can explain it. You can’t govern what you don’t understand, and that disconnect is now a top-tier enterprise risk.”

DC Casey  
CEO, CalypsoAI

## Risks remain a concern for C-Suite

**57%**

say if their company’s AI made an error like sharing private data or making an offensive statement, they’d seek a new role

**66%**

are ‘very confident’ an AI-led breach would be detected by their IT team



04

## Entry-Level Troubles

Entry-level employees pair technical naivety with disengaged attitudes toward AI policies.



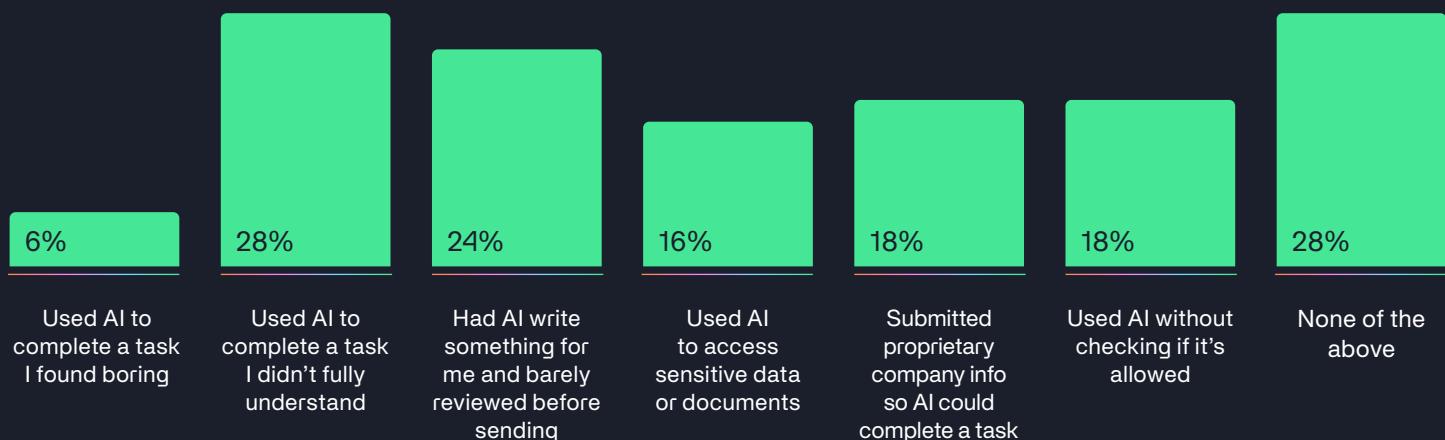
## Confusion runs amok

- **33%** of entry-level employees say they don't know what an AI agent is
- **21%** say their company's policies on AI are unclear, so they use AI as they wish
- **16%** can't tell the difference between an AI agent and a virtual employee

## ... but even clear policies aren't a fail-safe

- **30%** say they don't care about their company's AI policy
- **37%** wouldn't feel guilty if they broke AI protocol
- **25%** would quit their job if they couldn't use AI

Which, if any, of the following have you ever done with AI tools at work?



### Key

Entry-level employees



# Risk by Highly Regulated Industries

- Financial Services & Banking
- Healthcare
- Security



05

## Financial Services & Banking

AI is quietly overriding the industry's long-standing compliance culture.



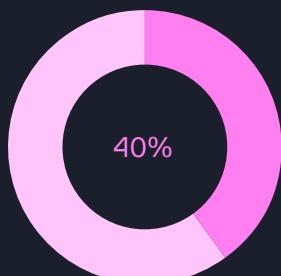
## Employees are using AI, allowed or not

- **60%** of employees in financial services & banking say they use AI tools even if it violates their company policy
- **36%** say they don't feel guilty about it

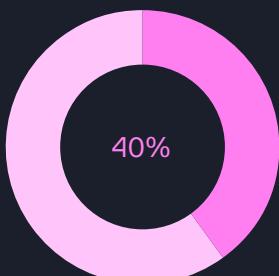
## Trust pulls ahead of comprehension

- **33%** of employees in financial services & banking don't know what an AI agent is
- **43%** say they trust AI more than their co-workers
- **36%** say they'd prefer to report to AI over a human

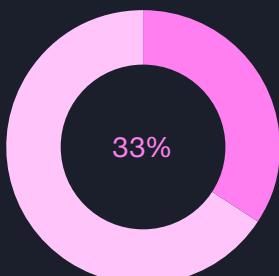
Which, if any, of the following have you ever done with AI tools at work?



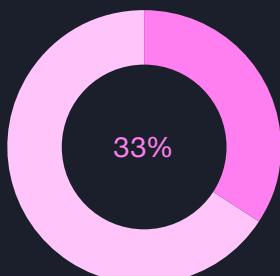
Used AI to complete a task I found boring



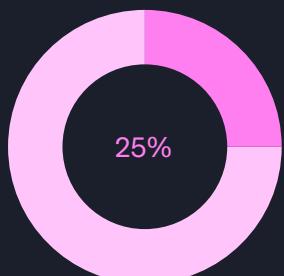
Used AI to complete a task I didn't fully understand



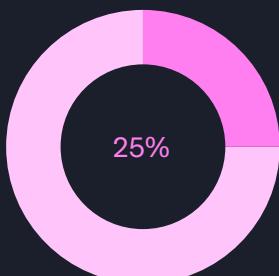
Had AI write something for me and barely reviewed before sending



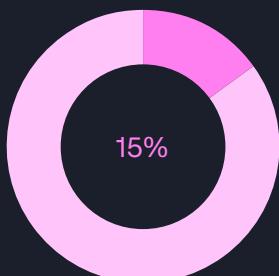
Used AI to access sensitive data or documents



Submitted proprietary company information so AI could complete a task



Used AI without checking if it's allowed



None of the above

Key  
■ Finance and banking employees



06

## Healthcare

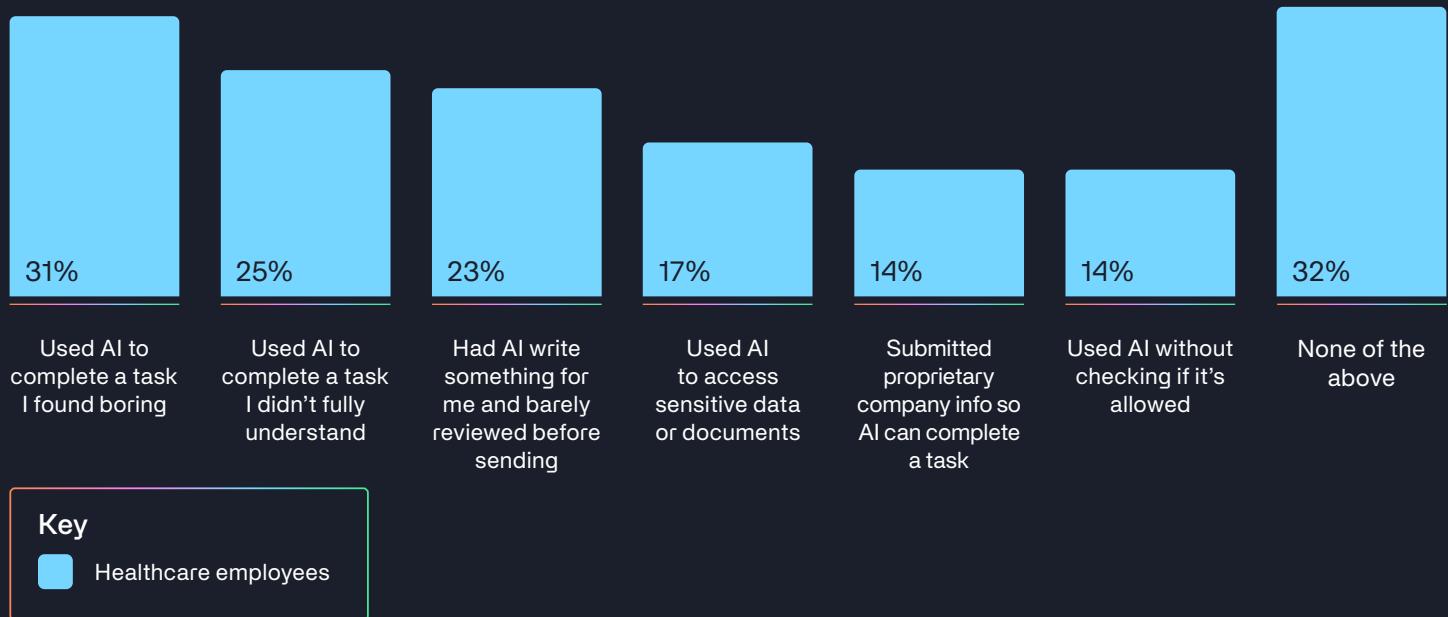
The people closest to sensitive healthcare data now see AI as more of an ally than a threat.



## Low policy follow-through meets naivety towards AI security risks

- **55%** of healthcare employees say they know and follow their organization's AI policy (the lowest of any regulated industry)
- **21%** say their company's policies on AI are unclear, so they use AI as they wish
- **18%** don't believe their IT department would detect a data leak if it came from AI
- **17%** have used AI to access sensitive data or documents

Which, if any, of the following have you ever done with AI tools at work?





“In healthcare, the stakes are higher but safeguards remain deficient. When AI becomes a trusted aide without being a secured one, sensitive data is exposed. The intent may not be malicious, but the impact can be catastrophic. We need to match AI optimism with appropriate security measures.”

DC Casey  
CEO, CalypsoAI

## Fondness for AI grows

**31%**

of healthcare employees trust AI more than their co-workers

**27%**

would rather report to AI than a human supervisor

**31%**

have leaned on AI to complete a task they found boring



07

# Security

AI isn't only a risk  
for the untrained.

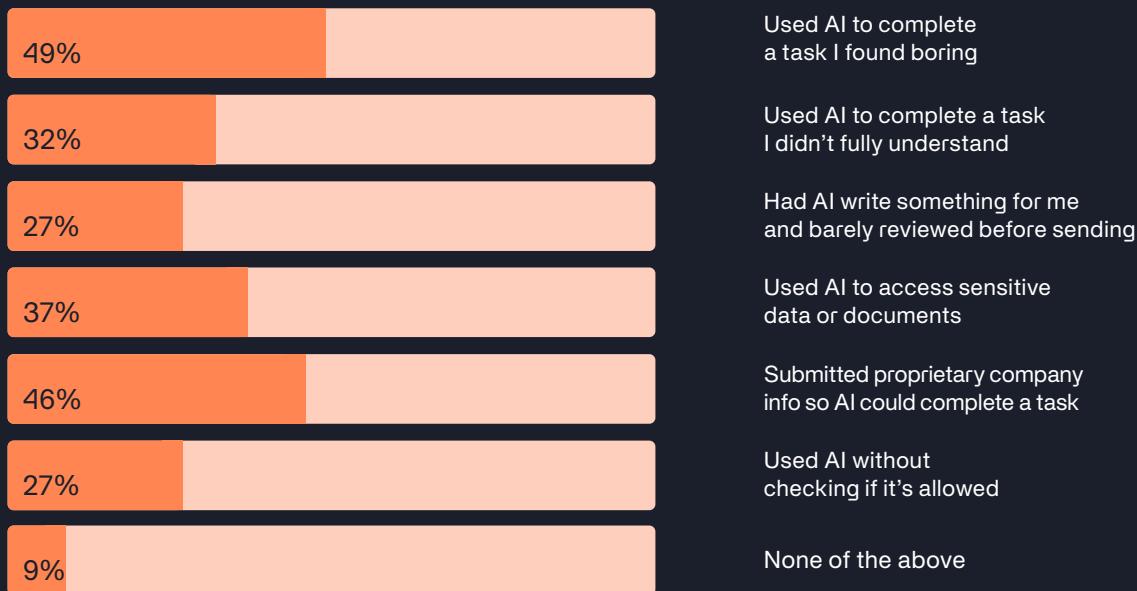


Over two-fifths of security professionals admit they'd use AI and break policy if it made their work easier, and 33% say they feel no guilt when they do

Allegiance to AI... up to a point

- 58% of security employees say they trust AI more than their own colleagues
- 42% say they'd use AI and break policy if it made their work easier
- 48% say they'd look for another role if their company's AI made an error like sharing private data
- 16% don't believe their IT team would catch a leak caused by AI
- 15% don't know what an AI agent is
- 48% say their company's AI policy is unclear, so they use it as they wish

#### Which, if any, of the following have you ever done with AI tools at work?



#### Key

Security employees



“The most dangerous threats aren’t coming from outside the firewall, they’re coming from trusted insiders empowered by AI. When policy becomes optional and trust shifts from people to AI, security programs need more than compliance checklists. They need visibility, enforcement, and cultural change.”

DC Casey  
CEO, CalypsoAI



# Risk in Additional Industries

IT & Telecoms



08

## IT & Telecoms

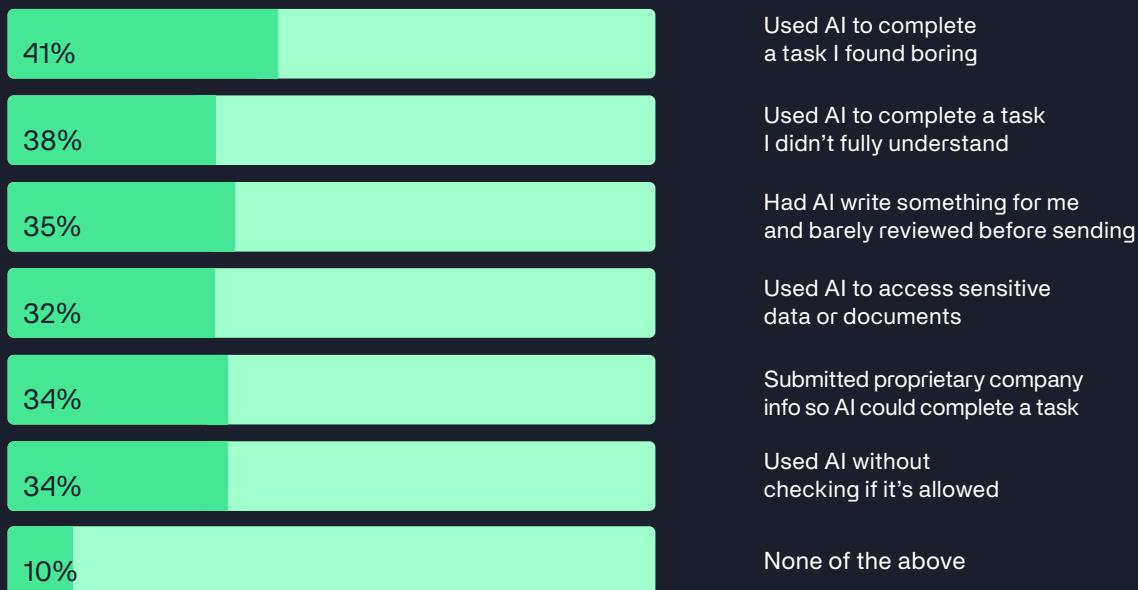
IT professionals are some of the most enthusiastic about using AI at work, and the most confident that they're on top of its threats.



Among all industries polled,  
IT & Telecoms employees  
were the most likely to use AI,  
despite the risks

- **92%** say that if AI was used to access or leak sensitive data, the IT team or the company's CEO would know
- **78%** believe they can tell the difference between an AI agent and a virtual employee
- **57%** would look for another job if their company's AI made an error (like making an offensive statement)
- **55%** would prefer to have AI as a manager than a human
- **52%** would quit their job if their employer didn't allow the use of AI
- **51%** don't feel guilty about using AI to break company policy

#### Which, if any, of the following have you ever done with AI tools at work?



#### Key

IT and Telecoms employees



## Methodology

The total sample size was 1,002 full-time office workers in the United States, aged 25 - 65. The survey was conducted from June 11 - 17, 2025. Censuswide abides by and employs members of the Market Research Society which is based on the ESOMAR principles.

## About CalypsoAI

CalypsoAI provides the only full-lifecycle platform to secure AI models and applications at the inference layer, deploying Agentic Warfare™ to protect organizations from evolving risks and adversaries. Trusted by global enterprises including Palantir and SGK, CalypsoAI's industry-leading team of experts is doing the hard miles to ensure security keeps pace with AI innovation.

CalypsoAI was founded in 2018 and has secured over \$40 million in venture funding from investors including Paladin Capital Group, Lockheed Martin Ventures and Hakluyt Capital. CalypsoAI was a Top-Two Finalist in the 2025 RSAC Innovation Sandbox contest and is named on Fast Company's Most Innovative Companies in AI for 2025. Learn more at [calypsoai.com](http://calypsoai.com) and [LinkedIn](#).

## Media Contact

Diffusion PR on behalf of CalypsoAI

[CalypsoAI@diffusionpr.com](mailto:CalypsoAI@diffusionpr.com)

(646) 571-0120