



## Drive Secure Behavior With 4 Employee- Focused Tactics

Christine Lee, Prashast Gupta, Richard Addiscott, Alex Michaels, Phillip Shattan

# Introduction

Employee susceptibility to misinformation and risky behavior poses a threat as significant as traditional technological vulnerabilities. 41% of employees admit to bypassing their organization's cybersecurity guidance in the last 12 months, including mishandling sensitive data and using unauthorized applications.



# Insights at a Glance

A more sophisticated approach is required. Cybersecurity leaders must drive secure work practices based on an understanding of employee psychology, rather than rely on generic awareness training.



- Measure what people actually do wrong and target those behaviors. Employee benchmarking shows a wide range of risky behavior, not just phishing.



- Personalize training on a variety of real scenarios. Employees want more, but better training: short, targeted, based on real scenarios.



- Reduce cybersecurity-induced business friction through collaboration. Nearly 60% of employees who violate cybersecurity guidance say they were prioritizing business needs over cybersecurity risk.

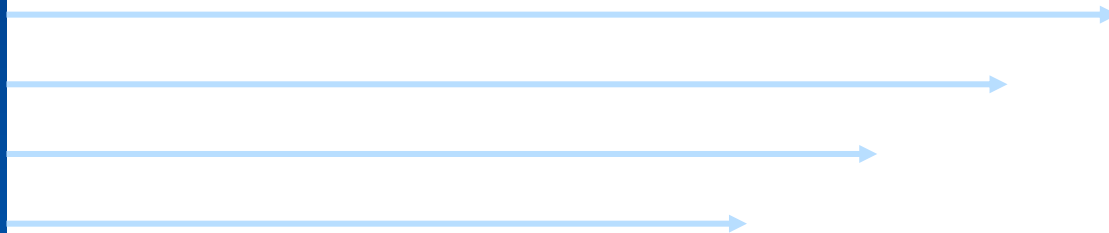


- Motivate secure behavior with recognition rather than punishment. Most employees respond to recognition for positive behaviors, not punishment for noncompliance.



The use of unsanctioned applications, because of GenAI, now carries more risk. Gartner benchmarking shows large proportions of employees misbehaving with GenAI.

The pressure to deliver AI value means shadow AI will increase. Organizations that block GenAI applications without providing viable alternatives will see their employees resort to using personal GenAI accounts for work.



# Figure 1: Employees Misbehaving With GenAI

|                                                                                                                                |   |
|--------------------------------------------------------------------------------------------------------------------------------|---|
| 57% of employees use personal GenAI account for work purposes                                                                  | F |
| 48% of employees use outputs from GenAI without reviewing for accuracy                                                         | F |
| 38% of employees use public or unapproved GenAI to generate code                                                               | F |
| 37% of employees download and/or use a GenAI application/feature on a work device without IT/cybersecurity approval            | F |
| 33% of employees build custom automation leveraging AI (e.g., AgentForce) without risk assessment or IT/cybersecurity approval | F |

n = 145 employees  
Q: Thinking of your workplace behavior over the past 12 months, how often did you use public GenAI or agentic AI applications (e.g., ChatGPT, Quillbot, Perplexity) for each of the following actions/activities?  
Source: 2025 Gartner Secure Behavior: Employee Perspective Survey

# Figure 2: What Employees Say Would Motivate Them to Behave More Securely

Cybersecurity team proactively working with me to reduce friction, improve UX, optimize controls for workflow

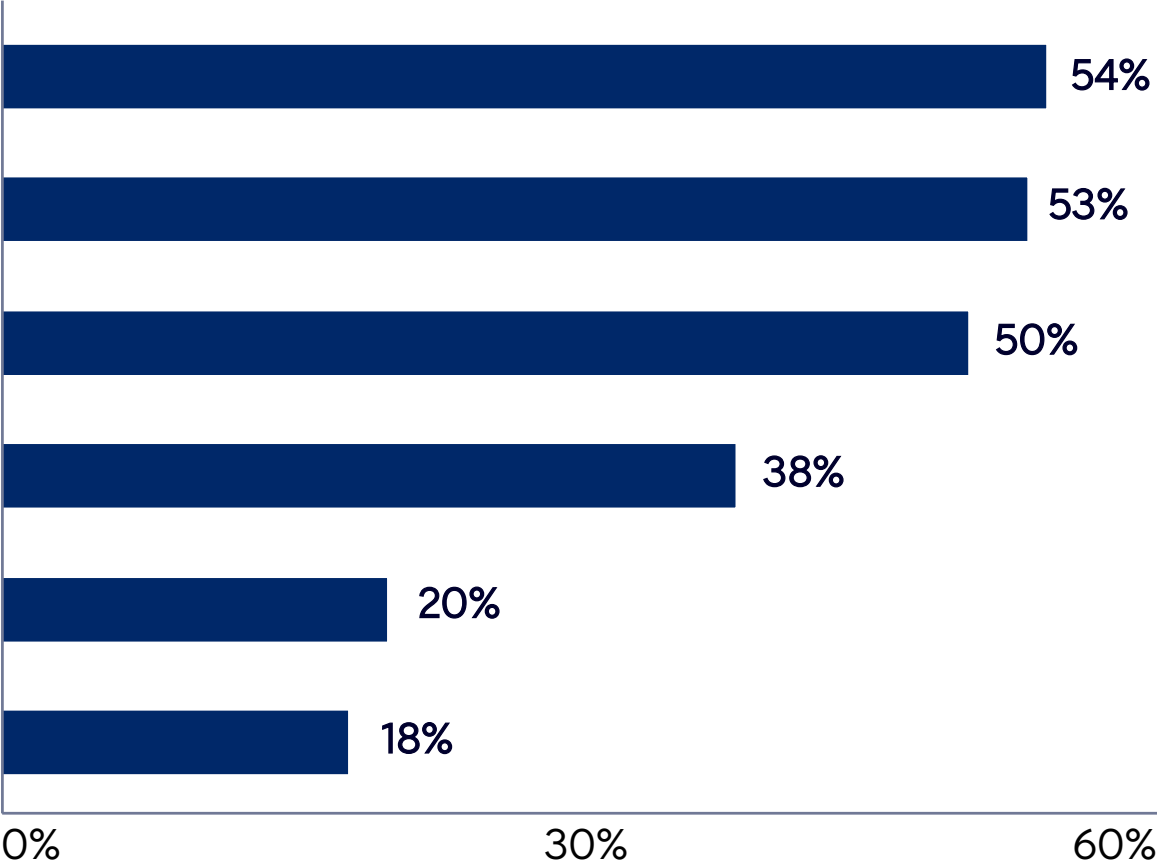
Improved training (personalization, gamification, shorter)

Recognition (townhall mentions, nominal prizes/gift cards)

Substantial material reward (e.g., bonus pay, material impact on annual performance review)

Substantial punitive measures (e.g. termination, loss of compensation)

Minor punitive measures (loss of privileges, remedial training)



n = 145 employees  
Q: Which of the following would motivate you to behave more securely (i.e., consistently comply with your organization’s cybersecurity guidance)? Select up to 3.  
Source: 2025 Gartner Secure Behavior: Employee Perspective Survey

# Actionable, objective insights

Position your organization for success. Explore these additional complimentary resources and tools for digital workplace leaders:

Conferences



Gartner Cybersecurity & Risk Management Summit

Secure your organization in the face of increasingly complex and evolving cyberthreats.

View Calendar

How We Help



Gartner for Chief Information Security Officers

Accelerate outcomes with AI-powered tools, on-demand insights and interactive experiences.

Explore Now

Tool



AI Controls Assessment

Assess your AI governance against leading frameworks and benchmark maturity against peers.

Learn More

Insights



Quarterly Insights for Cybersecurity Leaders

View the most utilized resources among cybersecurity leaders in 3Q26.

Learn More

Already a client? Get access to even more resources in your client portal. [Log In](#) ↗

# Connect with us

Get actionable, objective business and technology insights that drive smarter decisions and stronger performance on your mission-critical priorities.

U.S.: 1 855 322 5484

International: +44 (0) 3330 607 044

[Become a Client](#)

Learn more about Gartner for Digital Workplace Leaders

[gartner.com/en/cybersecurity](https://gartner.com/en/cybersecurity)

Stay connected to the latest insights



Attend a Gartner conference

[View Conference](#)