

6 Ways to Transform Your Cybersecurity Awareness Program

Although traditional awareness programs dominate, they don't work

Security awareness approaches:



Take 6 actions to transition your awareness program into a more impactful security behavior and culture program

1 Clarify the cost of employee-driven incidents for leadership

Less than half of organizations measure the **business impact** of insecure behavior.

Percentage collecting employee-driven incident metrics:

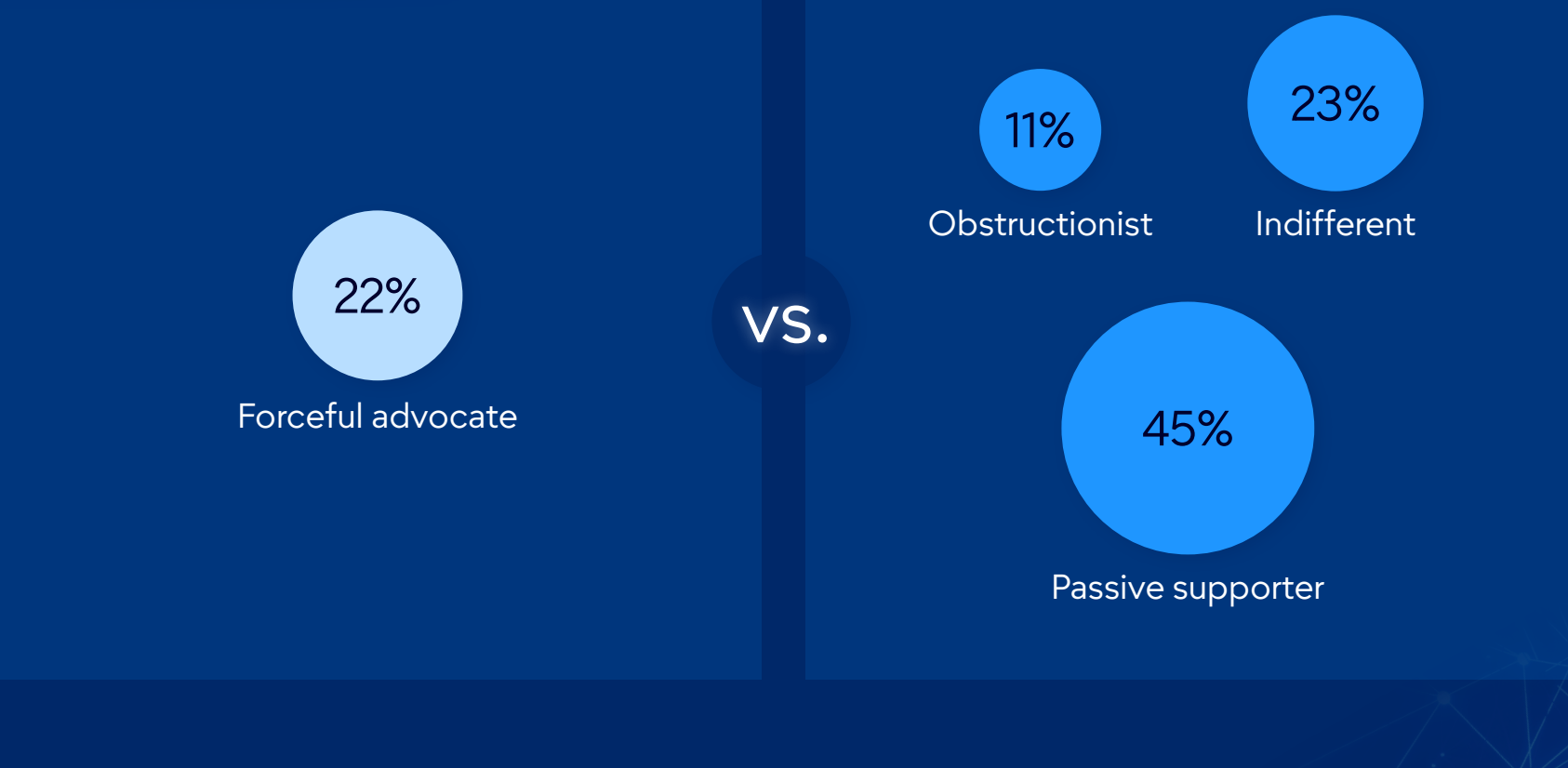


2 Drive executive action with specific asks

For example: Visible sponsorship, cybersecurity performance mandates, resourcing

Most executive leaders are passive supporters of cybersecurity

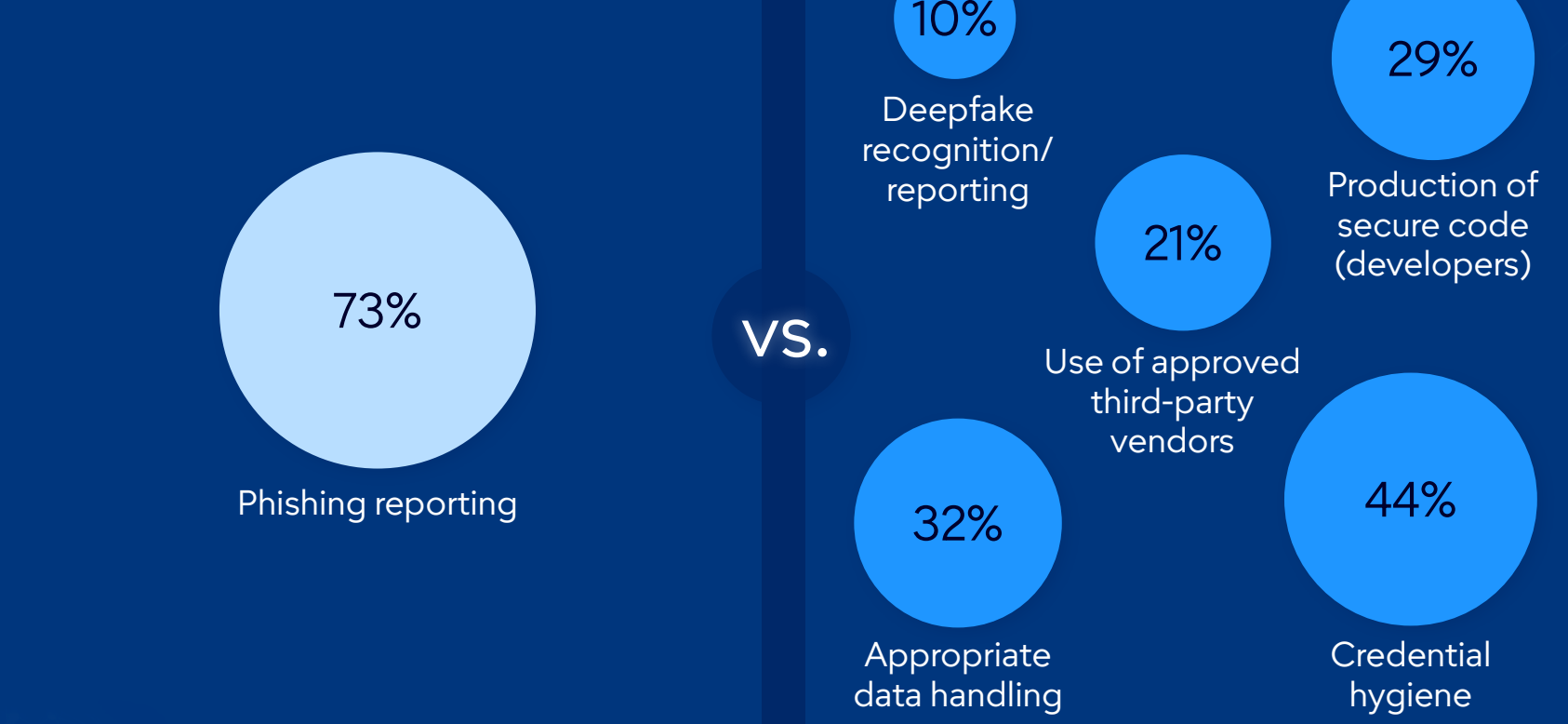
Leadership posture toward cybersecurity:



3 Target all high-risk behaviors, not just phishing

Most organizations focus too much on phishing

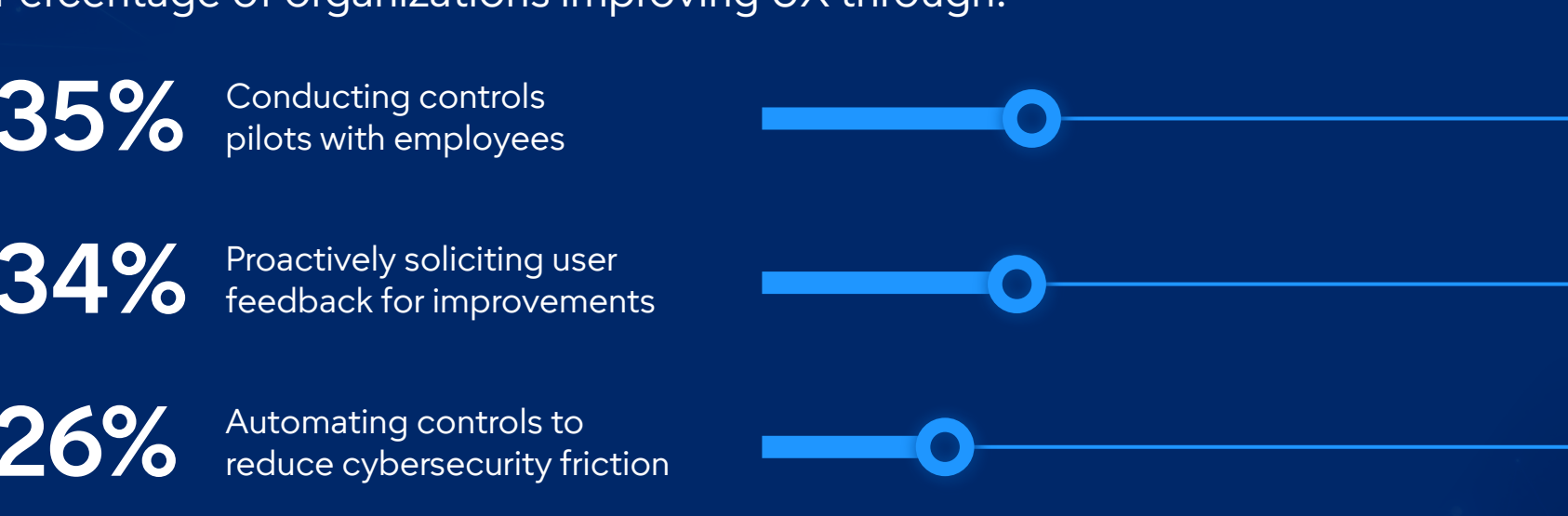
Percentage of potential high-risk behaviors receiving priority focus:



4 Co-create policy/controls with employees and commit to user experience

Employees behave insecurely due to controls-driven friction, yet most organizations don't prioritize UX improvement

Percentage of organizations improving UX through:



5 Push for accountability across the enterprise

Few organizations hold executives and their teams accountable for cyber risk

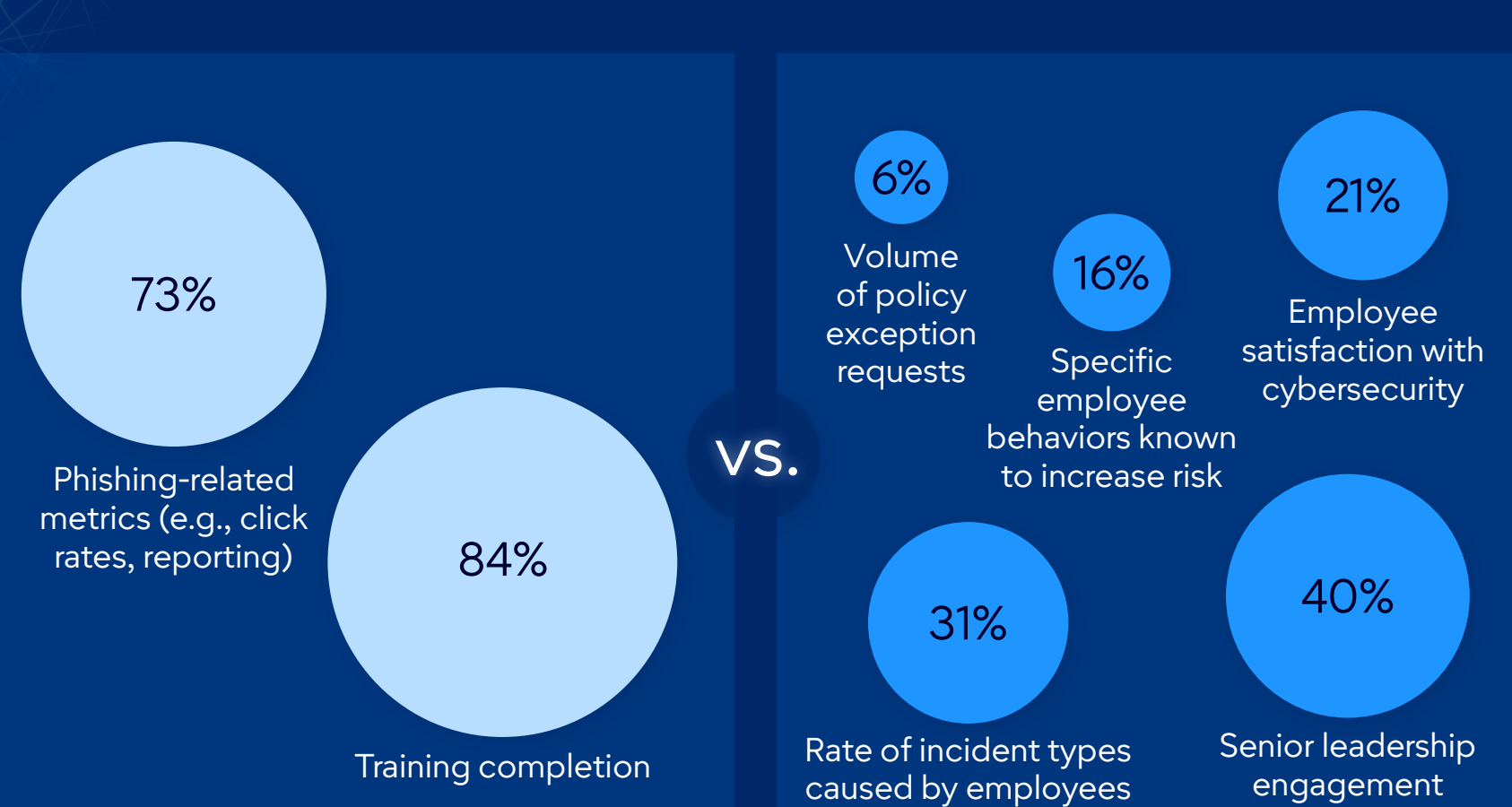
Underused tactics:



6 Measure program effectiveness with risk-relevant metrics

Organizations prioritize training and phishing at the expense of more risk-relevant metrics

Percentage of potential high-risk indicators receiving priority focus:



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.

[Learn More ↗](#)

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 ↗](#)

[Become a Client](#)

^aTraditional awareness programs use computer-based training, phishing simulations and cybersecurity risk communications to foster awareness.
^bAwareness programs enhanced for engagement use gamification, security champions and incentives to promote secure behavior.
^cSecurity behavior and culture (SBCP) is a formal program with systematic executive engagement, data-driven initiatives targeting high-risk areas, use of non-security practices and advanced platforms to drive secure behavior.