# AI and Cyber Readiness: Risk, Reward, and the Rising Confidence Divide

## The C-Suite Perspective

AXIS

Specialty Solutions, Elevated


# A Letter from Vince Tizzio

Among the dominant themes across Boardroom and C-Suite conversations worldwide is the opportunity – and disruptive impact – that AI is bringing to all aspects of business.

The fervor surrounding AI as a transformative force is undeniable – as is the reality that AI is quickly propelling us toward an entirely new risk landscape. From the CEO to the Chief Information Security Officer, many executives are adapting to AI transformation in real time while making operational decisions that could impact their firms for years to come.

Against this backdrop, we are experiencing a "preparedness paradox" where AI is transforming corporate defense strategies.

Our hope is that this research, which offers a rare dual lens into executive decision-making, will inform the broader business community about building cyber resilience that keeps pace with technological change, while bridging divides that may exist among CEOs, CISOs, and other C-Suite leaders

A commonality among paradoxes is that while they appear contradictory on the surface, they often contain a deeper truth: It will be crucial for C-Suite executives to work in concert to grow organizational resilience while enabling their organizations to tap into the enormous promise of AI.

**Vince Tizzio**
President and CEO, AXIS

# Contents

# Summary

### Differing Viewpoints in the C-Suite

While CEOs champion AI as a catalyst for innovation and efficiency, CISOs tend to see it as a new frontier of risk and oversight.

### A Transatlantic Trust Divide

As U.S. executives are embracing AI as an engine of innovation and defense, their U.K. counterparts remain notably more wary.

### Heightened Vigilance Amid AI-Driven Cyber Threats

Organizations across both regions viewed AI-driven attacks as the top emerging cyber threat to their firms.

### AI Productivity Gains are Reshaping Resource Allocations

Organizations say they plan to rebalance their people, technology and budgets.

### Cyber Preparedness is High, AI Confidence is Not

Respondents generally felt comfortable with their cyber defense strategy – but that their peers were less prepared.

# Differing Viewpoints in the C-Suite

While CEOs champion AI as a catalyst for innovation and efficiency, CISOs tend to see it as a new frontier of risk and oversight.

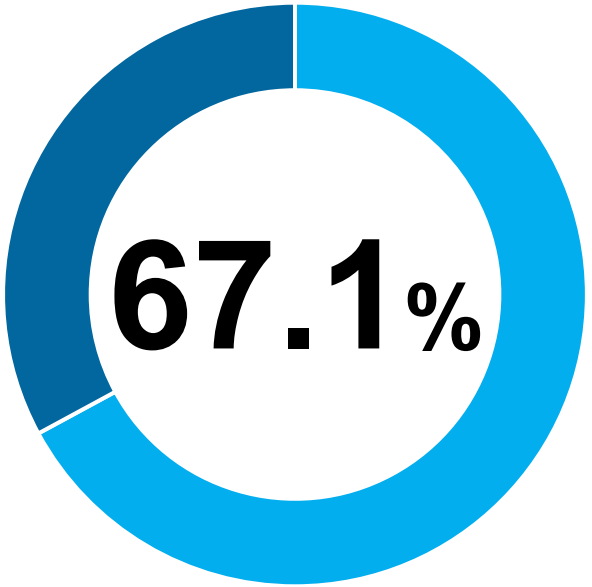
# Differing Viewpoints in the C-Suite

## Key Findings From Our Research:

CEOs view AI as a **driver of productivity** and competitive advantage. CISOs, however, approach the technology as a source of **increased exposure.**

# Differing Viewpoints in the C-Suite

## For Chief Executives, AI is Frequently Looked to as a Panacea; CISOs Brace for its Security Implications




of **CEOs:** trusting AI tools to help make cybersecurity decisions versus **58.6%** of **CISOs**

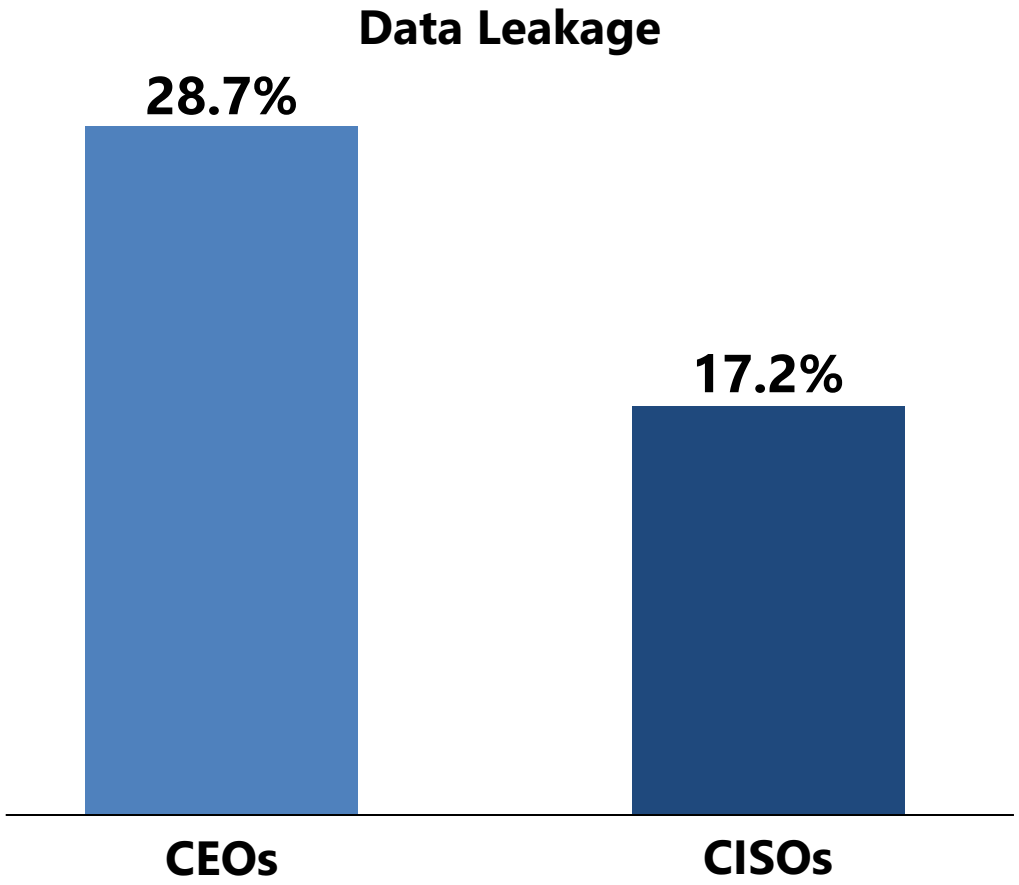
By a margin of **19.5%** to **29.7%, fewer CEOs than CISOs** indicated they did not trust that AI **would strengthen** their company's cyber defenses

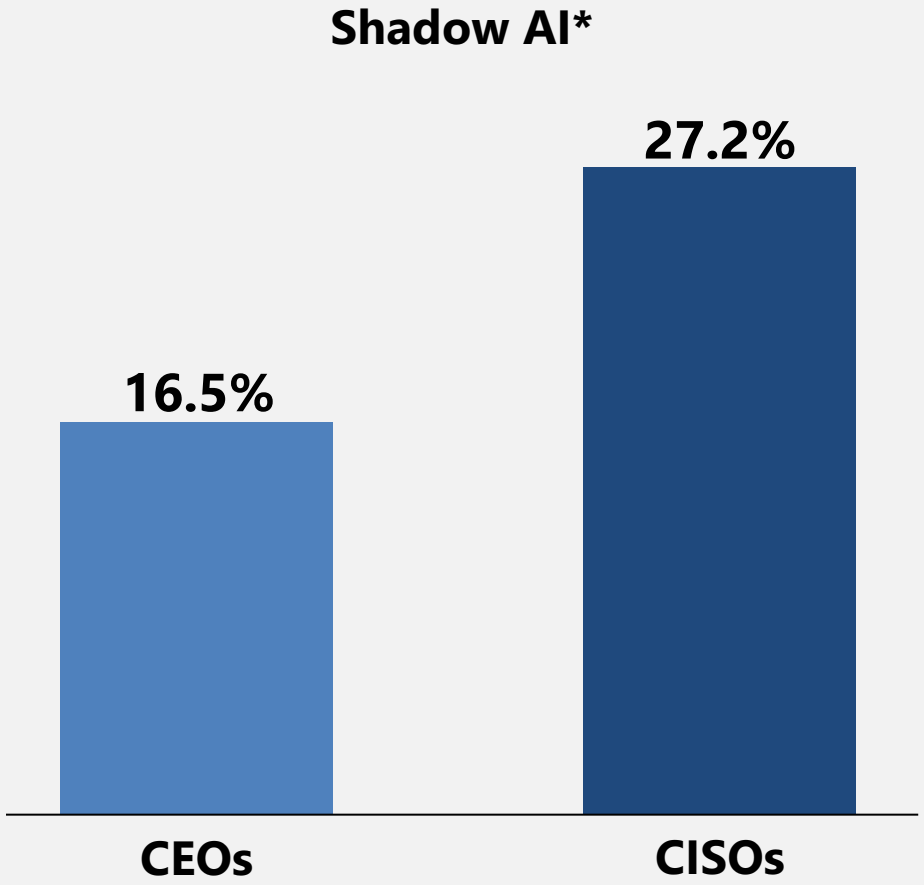
**Q15.** To what extent, if at all, do you personally trust AI tools to help make cybersecurity decisions?

**Q5.** How confident or not confident are you that AI will strengthen your organization's cyber defenses over the next 3 years?

# Differing Viewpoints in the C-Suite

## CISOs and CEOs Hold Different AI Risk Outlooks



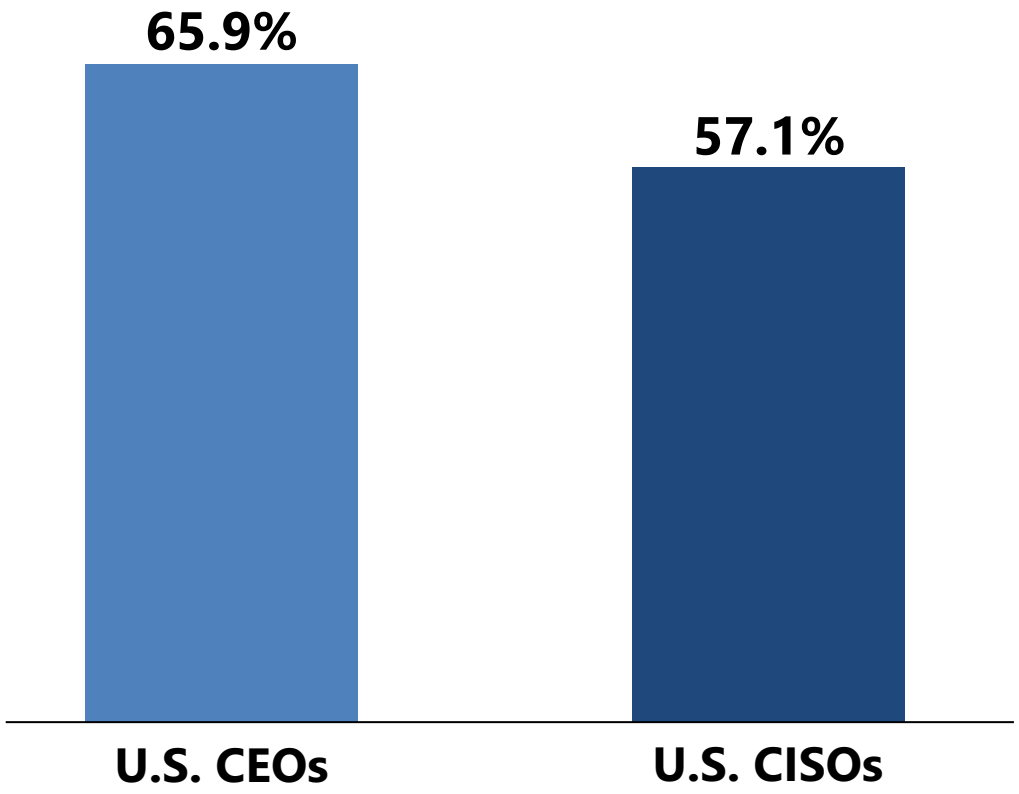

**Q1.** What do you see as the greatest risk posed by AI to your organization's cybersecurity, if anything?

** Shadow AI is the unsanctioned use of AI tools by employees without IT/security safeguards or approval*

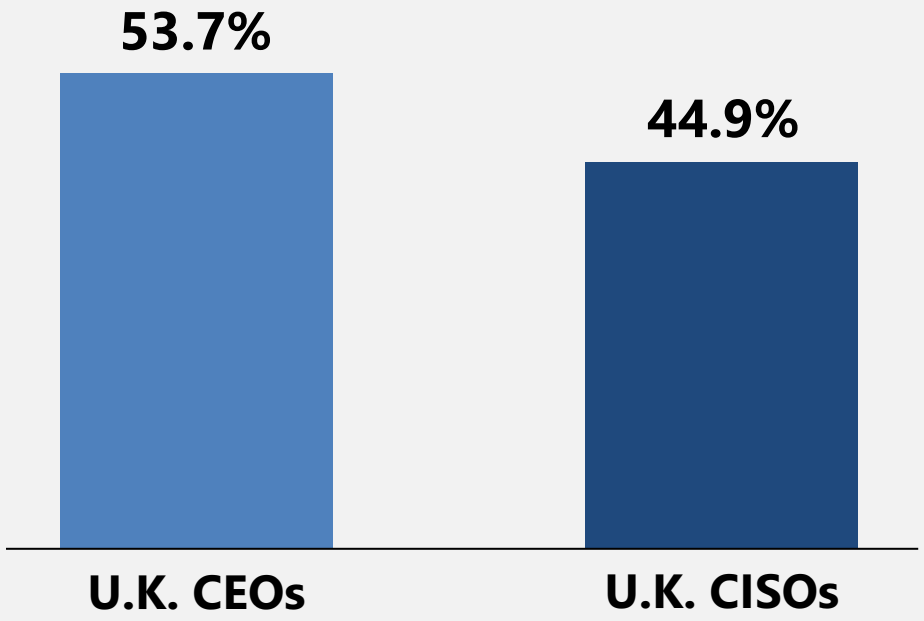
# Differing Viewpoints in the C-Suite

## The Preparedness Paradox

**Believe their company would respond to an AI-driven threat faster than their peers**



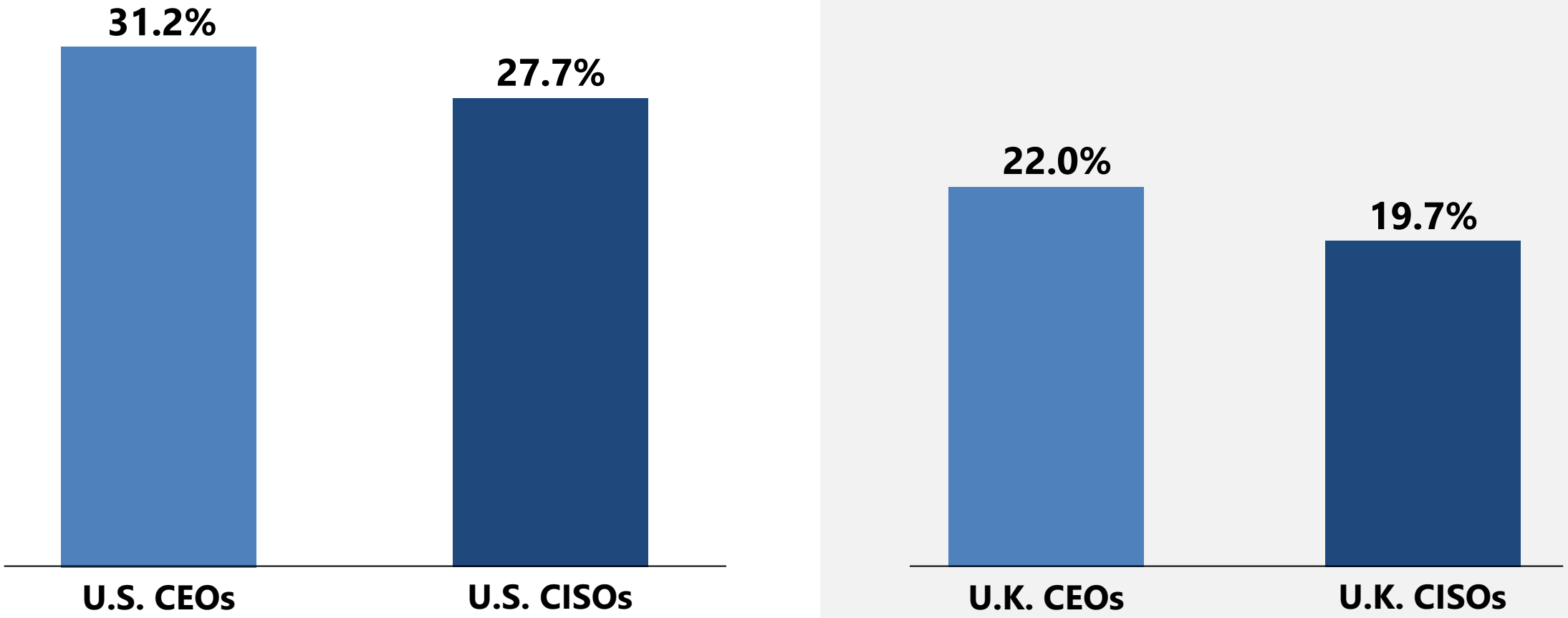

**Believe their company would respond to an AI-driven threat on par with their peers**




**Q6.** Compared to peers in your region, how would you rate your organization's readiness for risks related to your use of AI tools?

# Differing Viewpoints in the C-Suite

## CEOs Slightly More Concerned Than CISOs About AI-Driven Attacks




**Q8.** What do you see as the greatest emerging cyber threat for your organization over the next 12 months, if anything?

# A Transatlantic Trust Divide

As U.S. executives are embracing AI as an engine of innovation and defense, their U.K. counterparts remain notably more wary.

# A Transatlantic Trust Divide

## Key Findings From Our Research:

AI is generally viewed as an opportunity across both the U.S. and U.K., **though levels of its uptake and prudence vary**.

There exists a **confidence and trust gap** across regions, as U.K. respondents express more caution about AI adoption than their U.S. counterparts.

# A Transatlantic Trust Divide

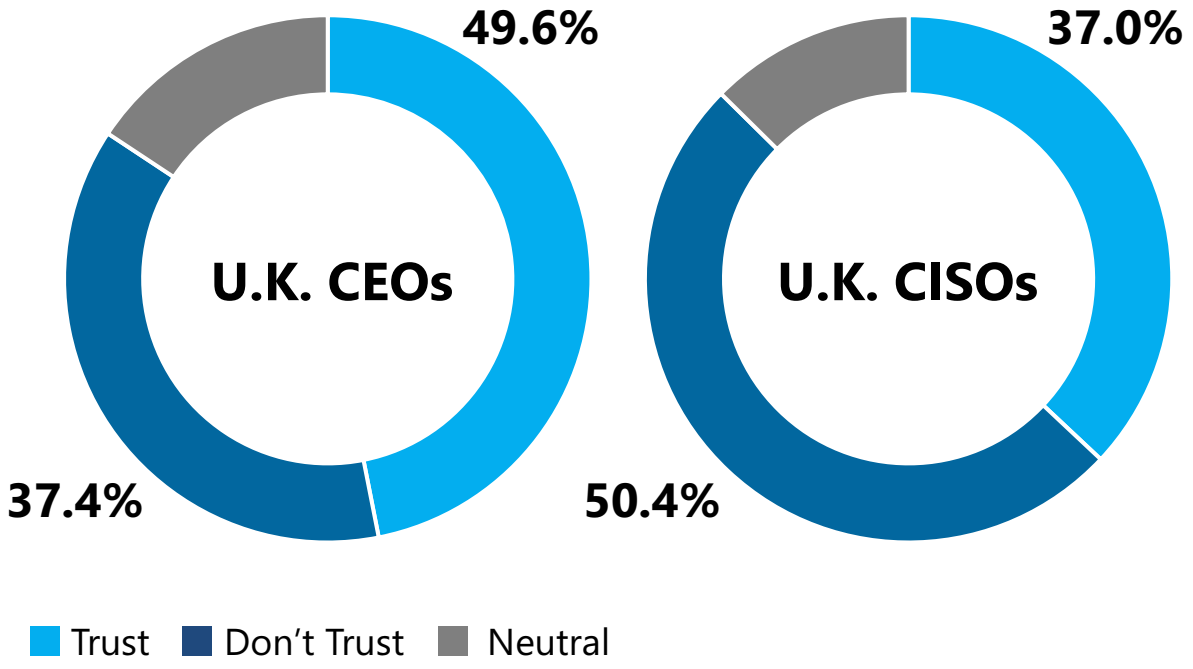
## U.S. Respondents are All In On AI

| | U.S. | U.K. |
|---|---|---|
| CEOs said they **were confident** AI would better their company's safeguards | **88.4%** | **55.3%** |
| CEOs said they **were not confident** AI would better their company's safeguards | **8.0%** | **32.5%** |

**Q5.** How confident or not confident are you that AI will strengthen your organization's cyber defenses over the next 3 years?

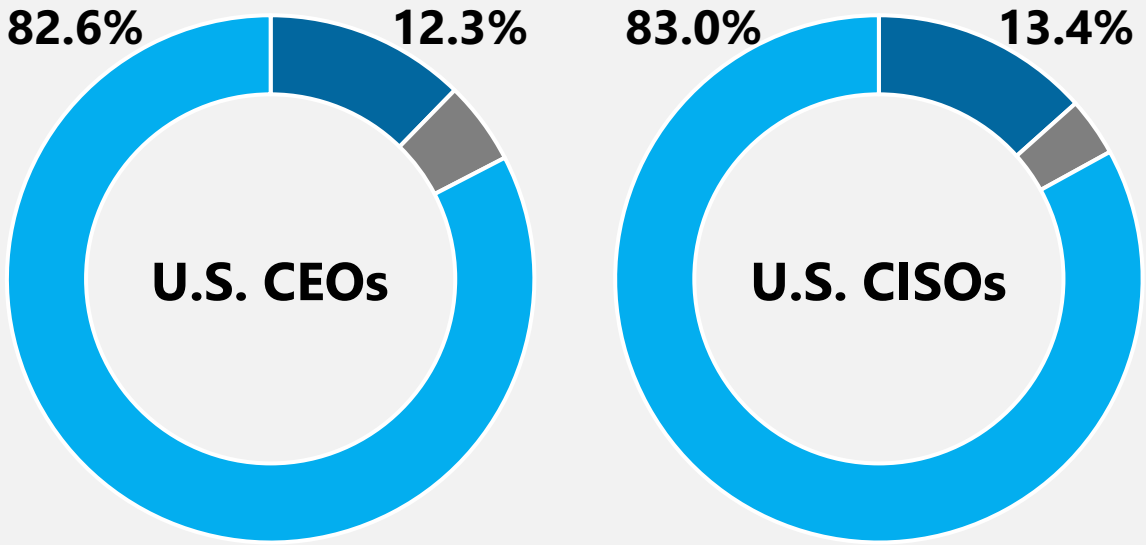
# A Transatlantic Trust Divide

## Distrust in AI was Relatively Common in the U.K.



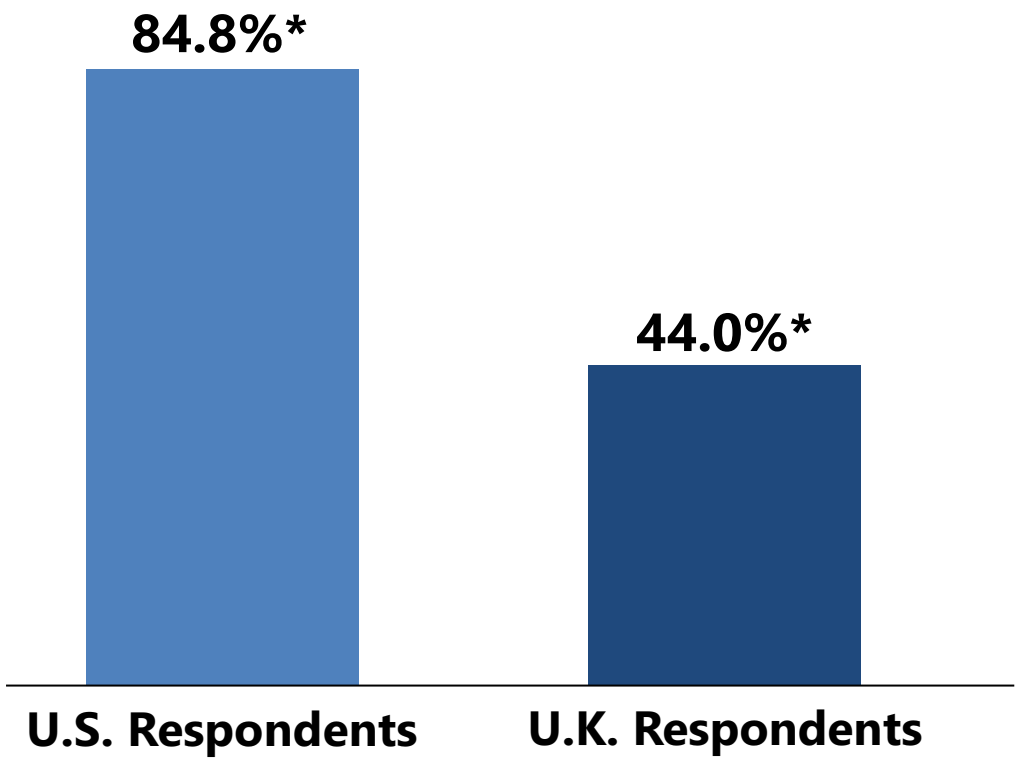

**Q15.** To what extent, if at all, do you personally trust AI tools to help make cybersecurity decisions?

## American Respondents Feel Differently



# A Transatlantic Trust Divide

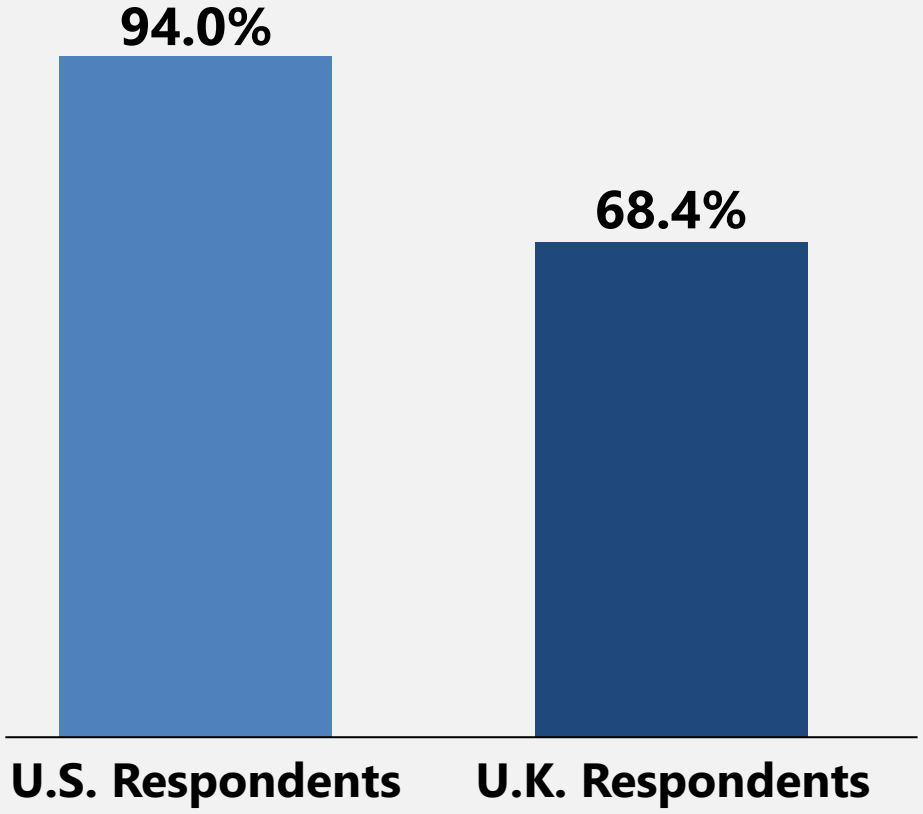
## U.S. Leaders Feel Ready for AI Threats, U.K. Leaders are Less Certain




**Q7.** On a scale of 1-5, how prepared, if at all, do you believe your organization is to defend against AI-driven cyber threats?

*Indicated they were 'somewhat prepared' (4) or 'very prepared' (5).

## U.S. Leaders are More Likely to Carry Cyber Insurance




**Q16.** Does your organization have cyber insurance in place?

# A Transatlantic Trust Divide

## Americans' Conviction in AI's Returns Contrasts with U.K. Caution

| | U.S. | U.K. |
|---|---|---|
| CEOs | 93.5% | 69.1% |
| CISOs | 87.5% | 74.0% |

**Q18a.** Do you believe AI delivers on return on investment for cybersecurity?

# A Transatlantic Trust Divide

## AI is Allowing Firms to do More with Less

**75.2%**

of respondents are likely to reduce headcount

**3.2%**

of U.S. respondents said they were unlikely to cut headcount, whereas

**10.4%**

of U.K. respondents who said the same thing

**Q4.** How likely or unlikely is it that you may reduce cybersecurity headcount as a result of greater productivity through investment in AI cybersecurity tools?

# Heightened Vigilance Amid AI-Driven Cyber Threats

Organizations across both regions viewed AI-driven attacks as the top emerging cyber threat to their firms.

# Heightened Vigilance Amid AI-Driven Cyber Threats

## Key Findings From Our Research:

Executives across both regions identify **AI-driven attacks as the top emerging cyber threat**, outranking identity theft and supply-chain compromise.

Still, U.S. executives feel more prepared than those in the U.K., underscoring a **widening divide** in defensive readiness.

What keeps leaders up at night isn't just the attack itself, but the **reputational** and **customer fallout** it could unleash.

# Heightened Vigilance Amid AI-Driven Cyber Threats

## Respondents Across Both Regions Viewed AI-driven Attacks as the Top Emerging Cyber Threat

**Top three emerging cyber threats**

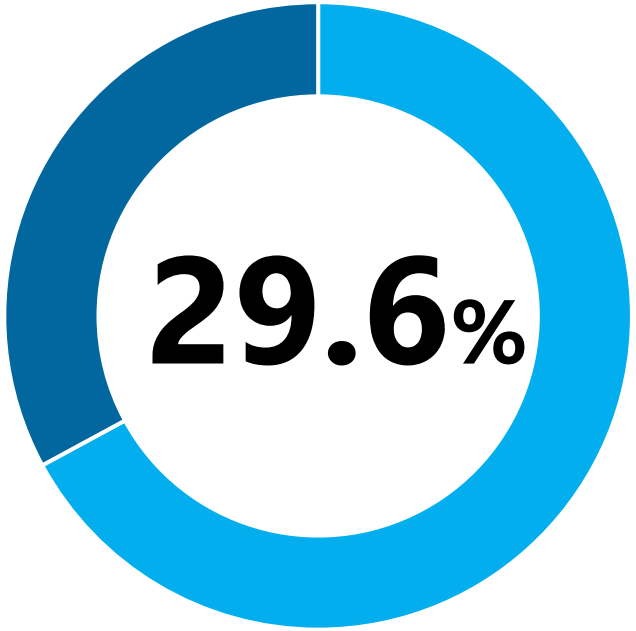
| | Avg. |
|---|---|
| AI-driven attacks | 25.2% |
| Identity theft/credential abuse | 18.0% |
| Supply chain compromise | 16.6% |

**Q8.** What do you see as the greatest emerging cyber threat for your organization over the next 12 months, if anything?

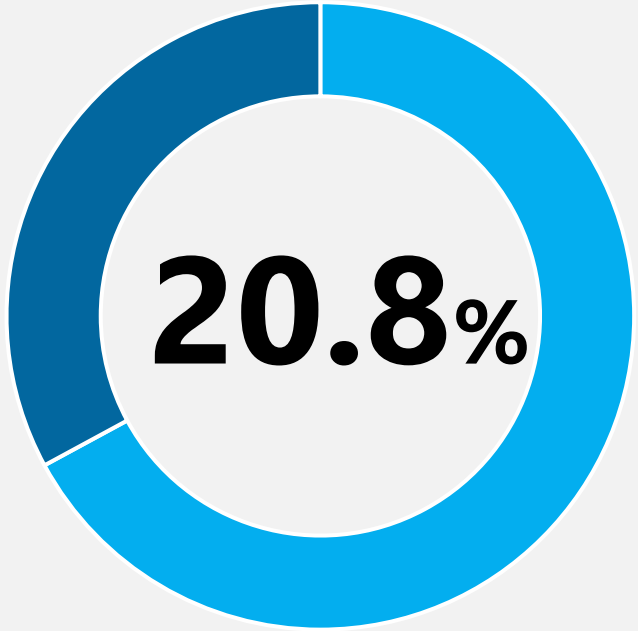
# Heightened Vigilance Amid AI-Driven Cyber Threats

## Respondents Across Both Regions Viewed AI-driven Attacks as the Top Emerging Cyber Threat

**Concern among U.S. Executives**




**Concern among U.K. Executives**




**Q8.** What do you see as the greatest emerging cyber threat for your organization over the next 12 months, if anything?

# Heightened Vigilance Amid AI-Driven Cyber Threats

## Respondents Ranked Their Greatest AI-Related Risks Ranking as Follows:

| | Avg. | U.K. | U.S. |
|---|---|---|---|
| **Data Leakage:** Unauthorized exposure of sensitive information outside its intended environment | **23.2%** | 17.2% | **29.2%** |
| **Shadow AI:** Unsanctioned use of AI tools by employees without IT/security safeguards or approval | 21.6% | 21.2% | 22.0% |
| **Model Manipulation:** Deliberate tampering with an AI model to alter its behavior or outputs | 19.0% | **23.2%** | 14.8% |
| **Deepfake/Social Engineering:** Fake/AI-generated content used to deceive audiences and/or trick people into revealing information/taking harmful actions | 17.6% | 20.4% | 14.8% |
| **Regulatory Noncompliance:** Failure to meet legal or industry rules governing data, security, or AI use | 17.4% | 17.2% | 17.6% |

**Q1.** What do you see as the greatest risk posed by AI to your organization's cybersecurity, if anything?

# Heightened Vigilance Amid AI-Driven Cyber Threats

## Were an Attack to Occur, Respondents are Bracing for Repercussions

| | Avg. | U.K. | U.S. |
|---|---|---|---|
| **Fear from reputational damage** | 39.4% | 42.8% | 36.0% |
| **Fear of customer attrition** | 38.8% | 38.0% | 39.6% |

**Q11.** If your organization suffered a major AI-driven cyber incident tomorrow, which impact would concern you most, if any for cybersecurity? (Select up to 3)

# AI Productivity Gains are Reshaping Resource Allocations

Organizations say they plan to rebalance their people, technology and budgets.

# AI Productivity Gains are Reshaping Resource Allocations

## Key Findings From Our Research:

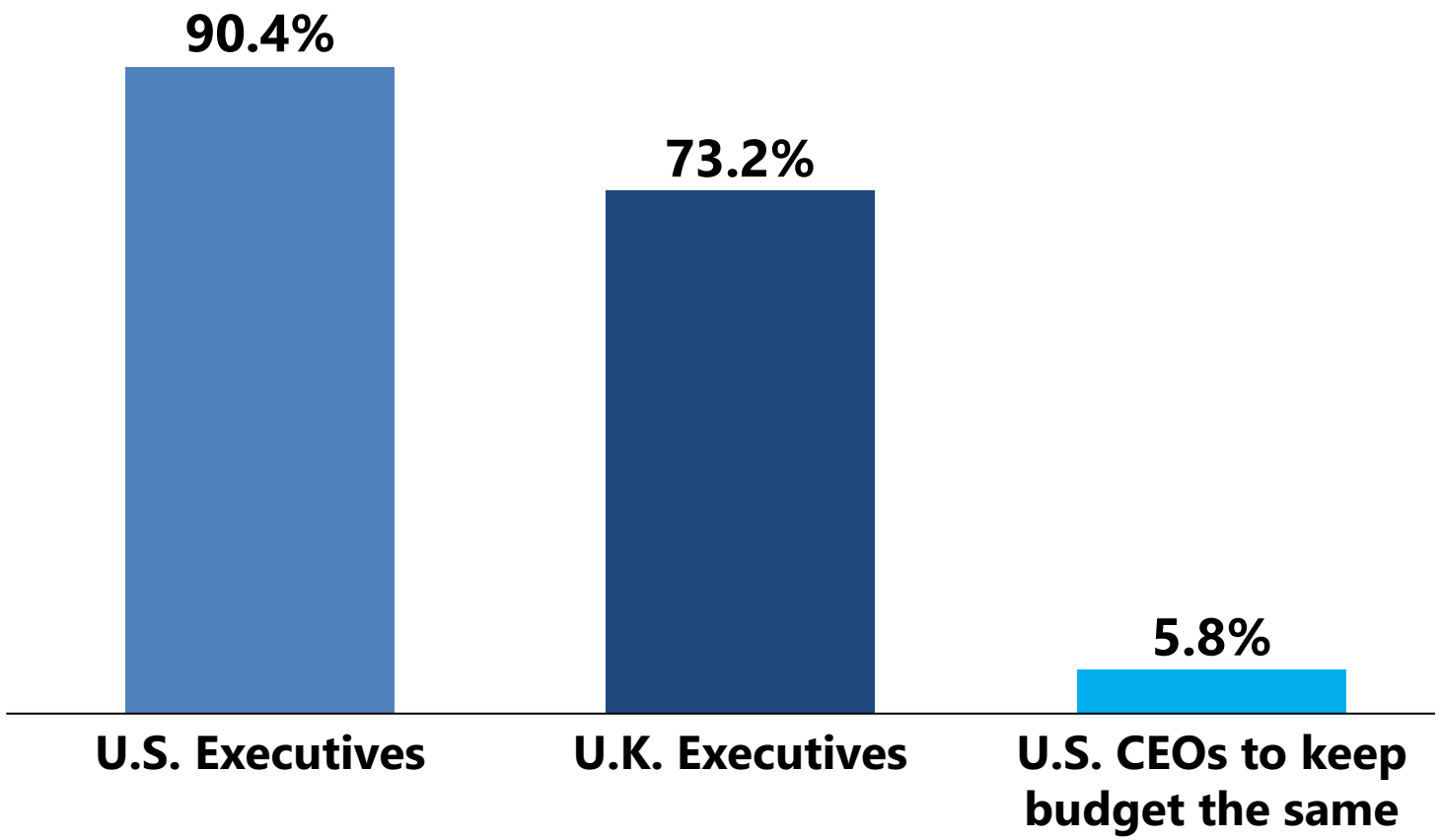
With AI viewed by C-Suite leaders as both an efficiency driver and investment priority, **organizations** say they **plan to rebalance their people, technology and budgets.**

Most respondents were so optimistic about AI's productivity gains that they indicated plans to reduce their staff as these tools take hold.

# AI Productivity Gains are Reshaping Resource Allocations

## Cybersecurity Budgets to Bulge

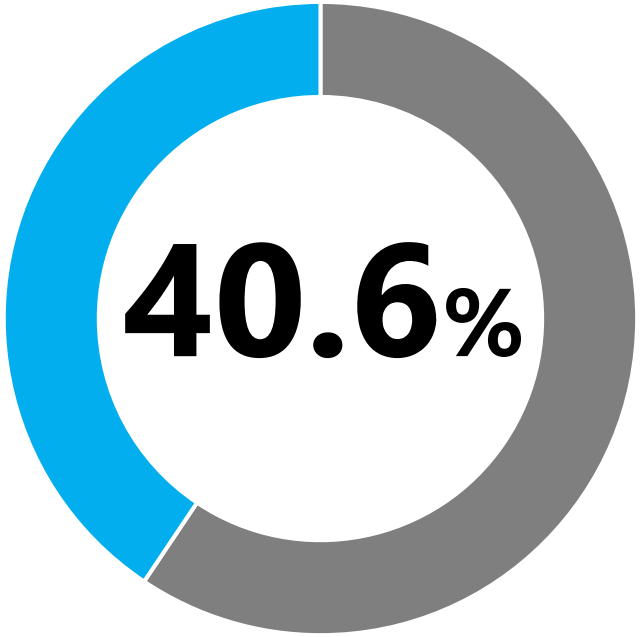
- **90.4%** of U.S. executives said they expected their cybersecurity budgets to increase compared to **73.2%** of U.K. ones
- Less than **6%** of U.S. CEOs said they'd keep their cybersecurity budgets the same



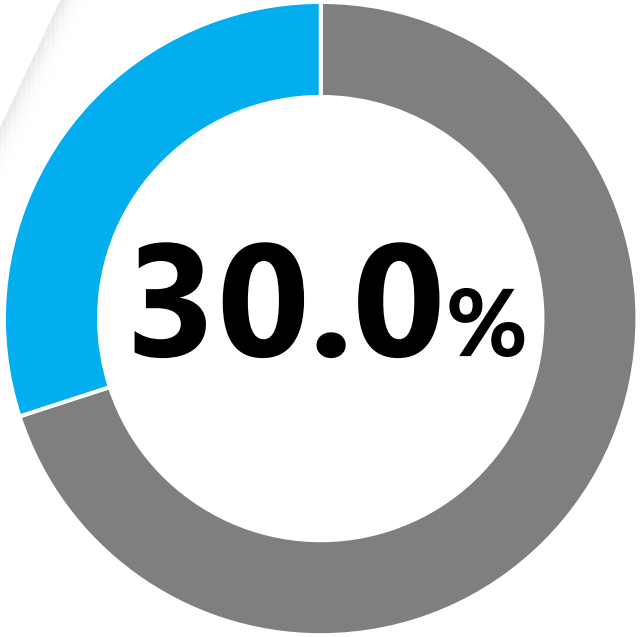

**Q19.** Over the next 12 months, how, if at all, do you expect your organization's cybersecurity budget to change?

# AI Productivity Gains are Reshaping Resource Allocations

## Cybersecurity Budgets are a Priority




of U.S. CEOs said they'd increase cybersecurity budgets significantly

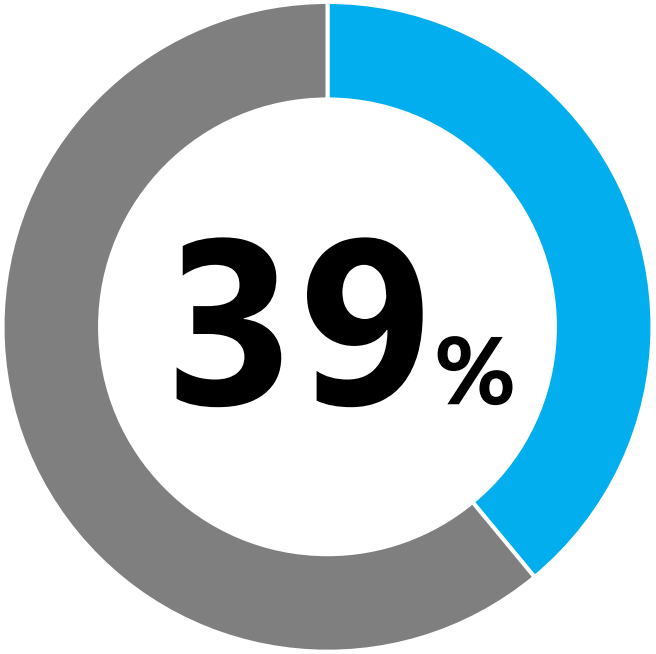



of U.K. CEOs said their cybersecurity budgets will increase significantly

**Q19.** Over the next 12 months, how, if at all, do you expect your organization's cybersecurity budget to change?

# AI Productivity Gains are Reshaping Resource Allocations

## Cybersecurity Budgets are Shifting Toward AI Solutions




The plurality of respondents now **allocate between 26-50%** of their cybersecurity budget to AI tools and solutions

**Q20.** What proportion of your cybersecurity budget is currently allocated to tools and solutions incorporating AI?

## The finding was consistent across regions

| U.K. | U.S. |
|---|---|
| 38.8% | 39.2% |

# Cyber Preparedness is High, AI Confidence is Not

Respondents generally felt comfortable with their cyber defense strategy – but that their peers were less prepared.

# Cyber Preparedness is High, AI Confidence is Not

## Key Findings From Our Research:

Respondents across both regions indicated comfort in their ability to contain a cyberattack tomorrow. But AI-related threats are a different story.

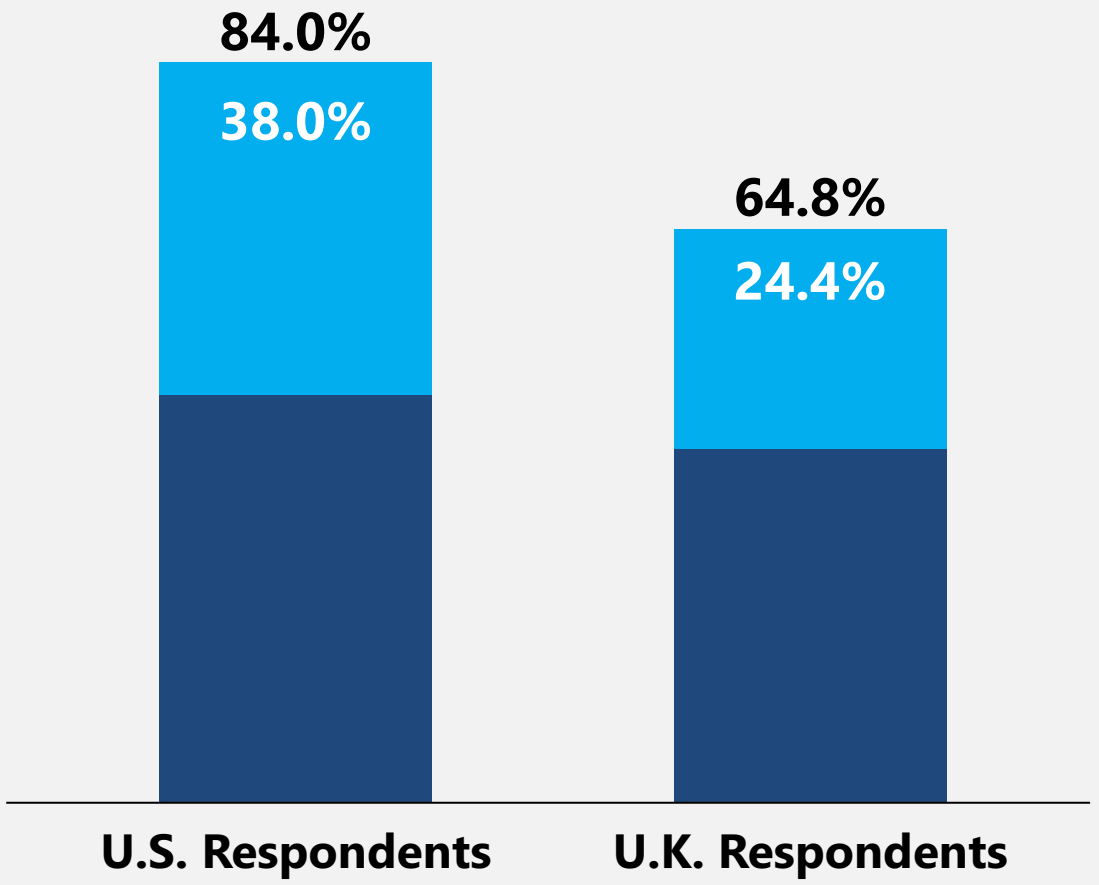
**The preparedness gap is especially pronounced in the U.K.,** where fewer than half of respondents in the region said their organization could defend itself against AI-driven cyber threats.

The data points to a pivotal moment: as AI transforms both offense and defense, leaders have a **narrow window to translate confidence** into competence and ensure their defenses evolve as quickly as the threats.

# Cyber Preparedness is High, AI Confidence is Not

## Greater Preparedness in America

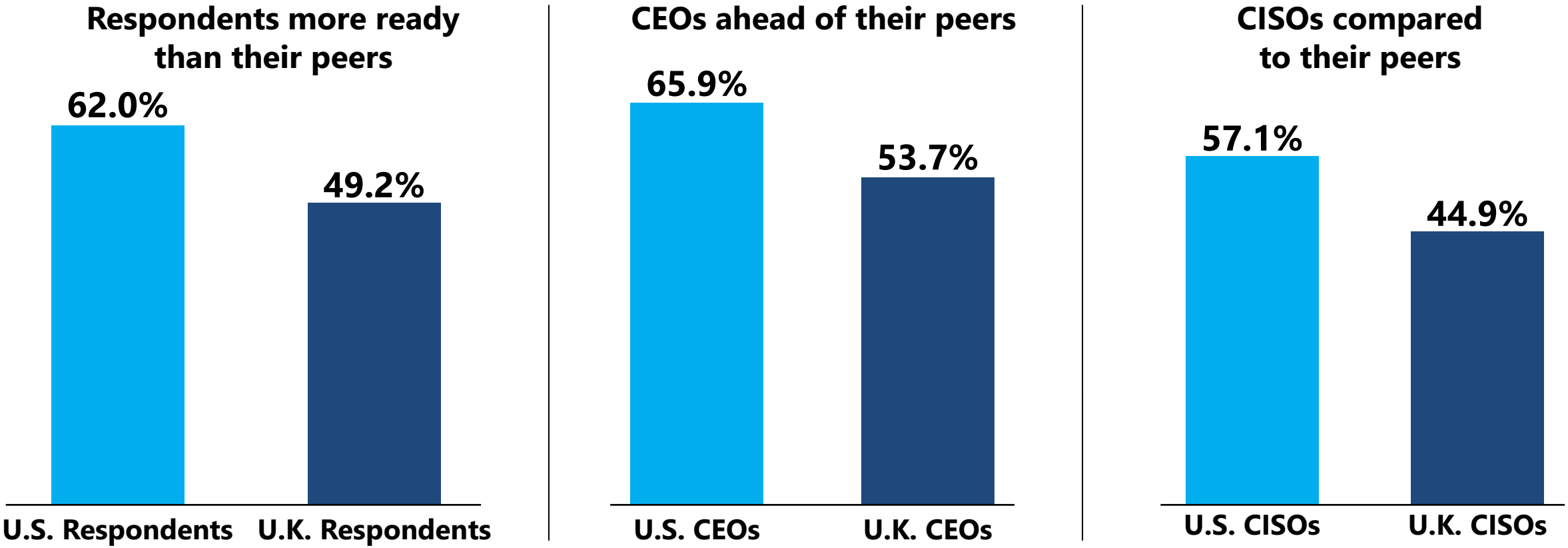
- **84%** of U.S. respondents said they'd be faster than their peers at containing a cyberattack tomorrow. **38%** of them '**much faster**'
- **64.8%** of U.K. respondents said they would be faster than their peers. **24.4%** of U.K. executives indicated they'd be '**much faster**'




**Q10.** If your organization were to experience a major cyberattack tomorrow (such as ransomware or a data breach), how do you think your ability to contain it would compare to that of your industry peers?

# Cyber Preparedness is High, AI Confidence is Not

## Across Roles and Regions, U.S. CEOs Stand Out as the Most AI-Confident




**Q6.** Compared to peers in your region, how would you rate your organization's readiness for risks related to your use of AI tools?

# Cyber Preparedness is High, AI Confidence is Not

## Firms are Ready for Cyberattacks

| | U.S. Prepared | U.K. Prepared |
|---|---|---|
| CEOs | 94.9% | 70.7% |
| CISOs | 92.9% | 81.9% |

**Q9.** If your organization experienced a significant cyberattack tomorrow, how prepared or not prepared is your organization to contain it?

# Cyber Preparedness is High, AI Confidence is Not

## Leaders Feel Prepared for Cyberattacks, But Not for AI-driven Ones

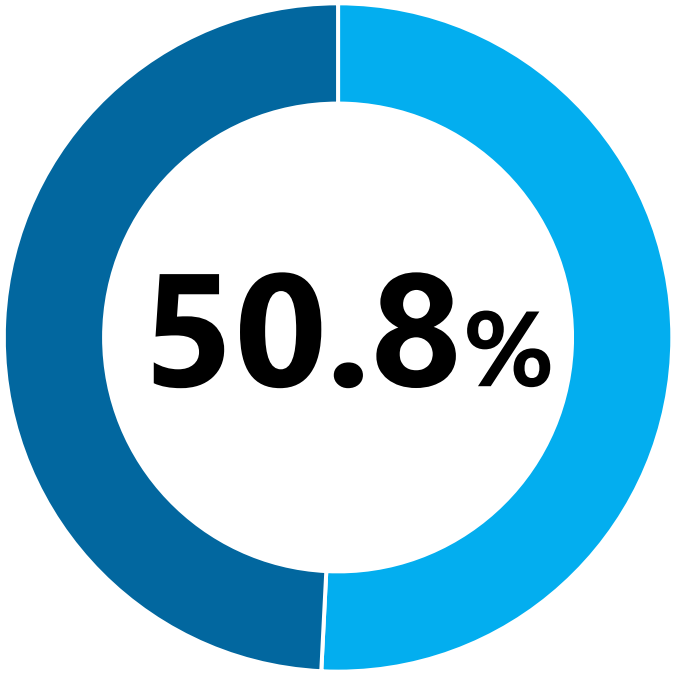
| | U.S. Not Prepared* | U.K. Not Prepared* |
|---|---|---|
| CEOs | 10.1% | 35.8% |

**Q7.** On a scale of 1-5, how prepared, if at all, do you believe your organization is to defend against AI-driven cyber threats?

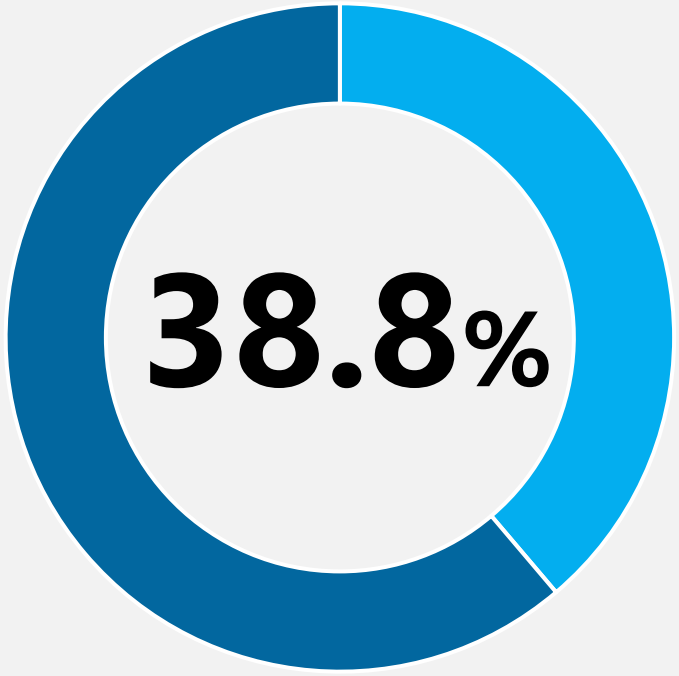
*Indicated they were 'not at all prepared' (1) or 'not that prepared' (2).

# Cyber Preparedness is High, AI Confidence is Not

## U.S. Respondents Felt 'Very Prepared' to Respond to an Attack




## A Minority of U.K. Respondents Felt 'Very Prepared'




**Q9.** If your organization experienced a significant cyberattack tomorrow, how prepared or not prepared is your organization to contain it?

# Conclusion

Our survey findings indicate that we are experiencing a '**preparedness paradox',** where AI is transforming corporate defense strategies, while also exposing a divide between C-Suite's strategic optimism and security pragmatism.

As CEOs champion AI as a catalyst for innovation and growth, CISOs are confronting a new set of risks, responsibilities, and vulnerabilities that **demand greater vigilance**. Navigating this moment will require closing the confidence gap, aligning leadership priorities, and ensuring defenses evolve as quickly as the threats themselves.

# Methodology

## Data Gathering

- Findings were derived from a 23-question survey among a total of **500 CEOs and CISOs** across the United Kingdom and United States
- In the U.S., the respondent pool consisted of **138 CEOs and 112 CISOs**, while in the U.K. it comprised **123 CEOs and 127 CISOs**
- Respondents represented companies with at least **250 employees**
- Fielding for this study was conducted by an independent company from October 22–29, 2025

# Glossary

**Data Leakage:**
Unauthorized exposure of sensitive information outside its intended environment

**Shadow AI:**
Unsanctioned use of AI tools by employees without IT/security safeguards or approval

**Model Manipulation:**
Deliberate tampering with an AI model to alter its behavior or outputs

**Deepfake/Social Engineering:**
Fake/AI-generated content used to deceive audiences and/or trick people into revealing information/taking harmful actions

**Regulatory Noncompliance:**
Failure to meet legal or industry rules governing data, security, or AI use

# Contact

**Lori Bailey**
Head of Global Cyber and Technology
AXIS
Lori.Bailey@axiscapital.com

Specialty Solutions, Elevated