QBE Insurance

Cyber risks and AI 2026

May 2026

Key findings

58%

of businesses experienced a cyber event in the past 12 months

21%

experienced disruption lasting a full working day or more

57%

of those with cyber events suffered revenue loss

80%

are already using AI in their operations

29%

experienced AI-enabled cyber attacks in the past year

72%

expect cybersecurity budget increase (37% beyond inflation)

Methodology

Survey details

Opinium Research conducted this quantitative online survey on behalf of QBE.

6,016 decisionmakers of IT, administration or insurance in businesses with 100-2000 employees

15 countries across Asia, AusPac, Europe, the Middle East and North America

Australia (400), Canada (400), Denmark (400), France (400), Germany (400), Hong Kong (400), Italy (400), Netherlands (400), New Zealand (410), Singapore (400), Spain (400), Sweden (400), United Arab Emirates (406), United Kingdom (400), United States (400)

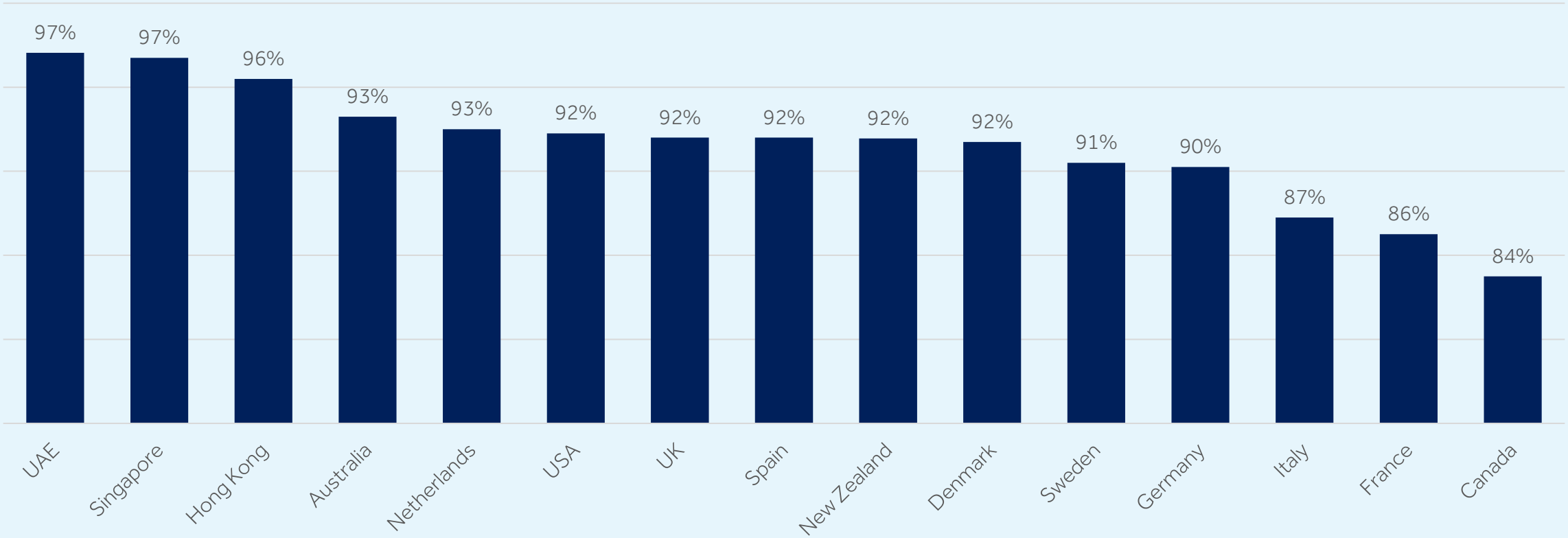
Fieldwork dates:
31 March-21 April 2026

Results are self-reported

Impact of Artificial Intelligence on business

Optimism about the business impact of AI is high across all markets, and highest in Asian markets

% saying AI will have a good impact on their business

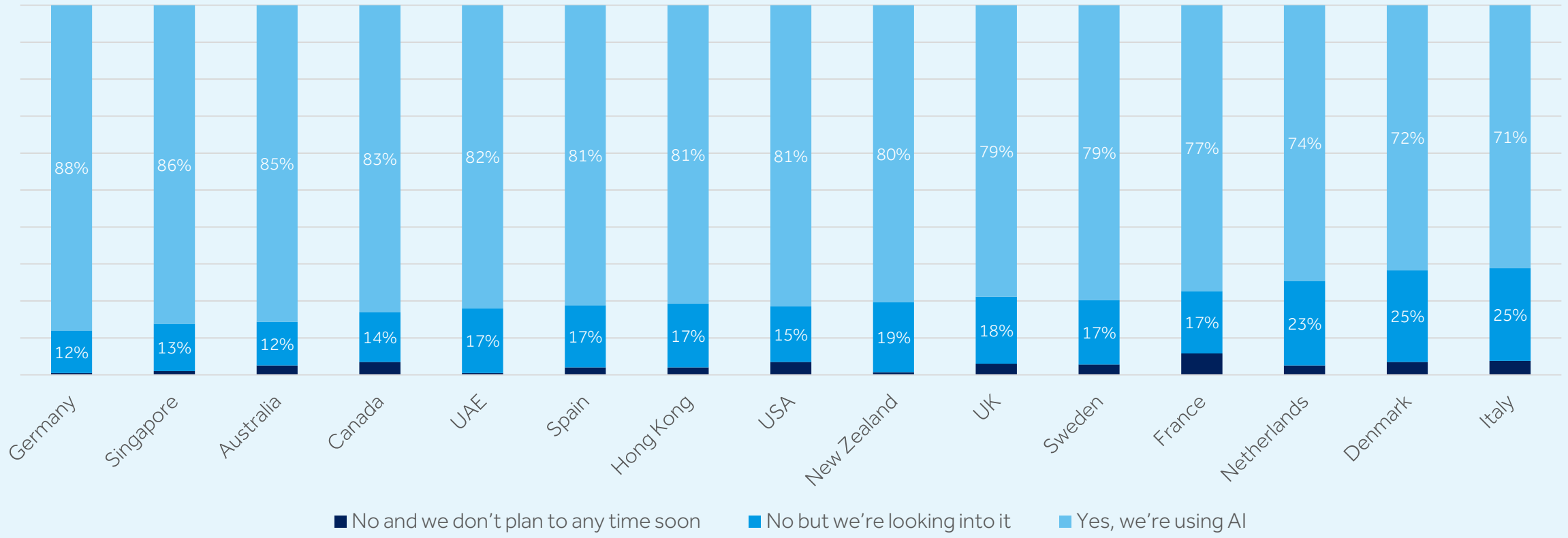


Q2. On balance, do you think Artificial Intelligence will have a good or bad impact on your business in the next two years? Base: All respondents (6,016)

Use of Artificial Intelligence within businesses

AI adoption is widespread across markets, indicating that AI is embedded in mainstream business activity

% of businesses currently using AI

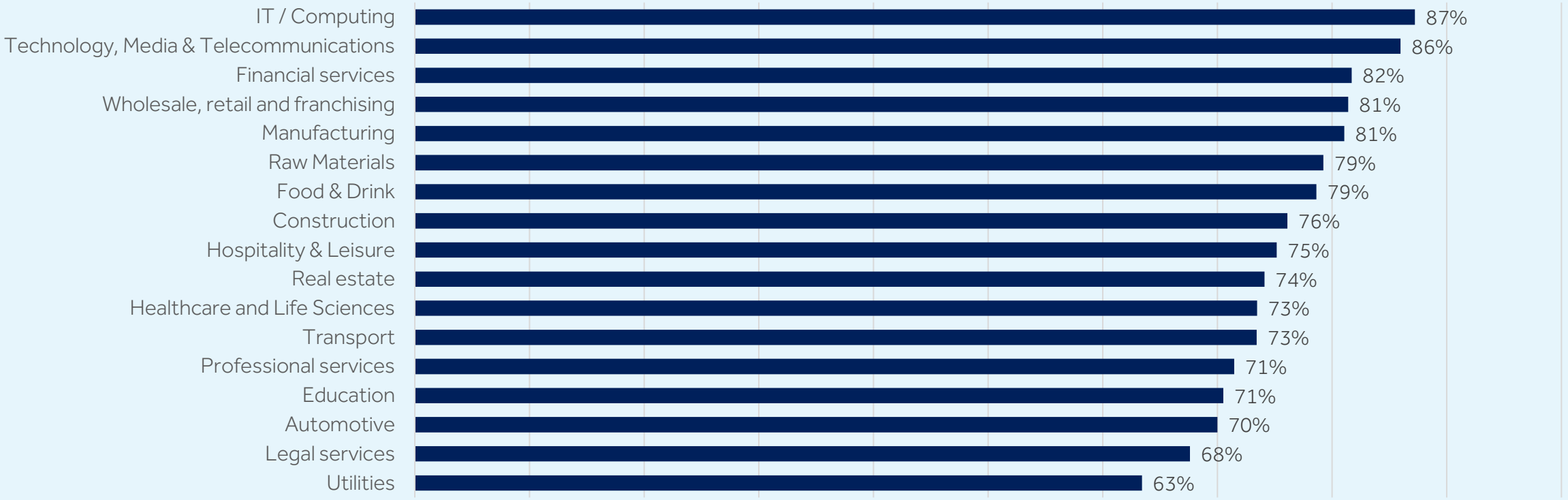


Q3 Does your business use Artificial Intelligence in its operations? Base: All respondents (6,016)

AI use by sector

While adoption is highest in technology-adjacent sectors, AI is being used across a broad range of industries, suggesting cross-sector integration rather than niche deployment

% of businesses using AI by sector

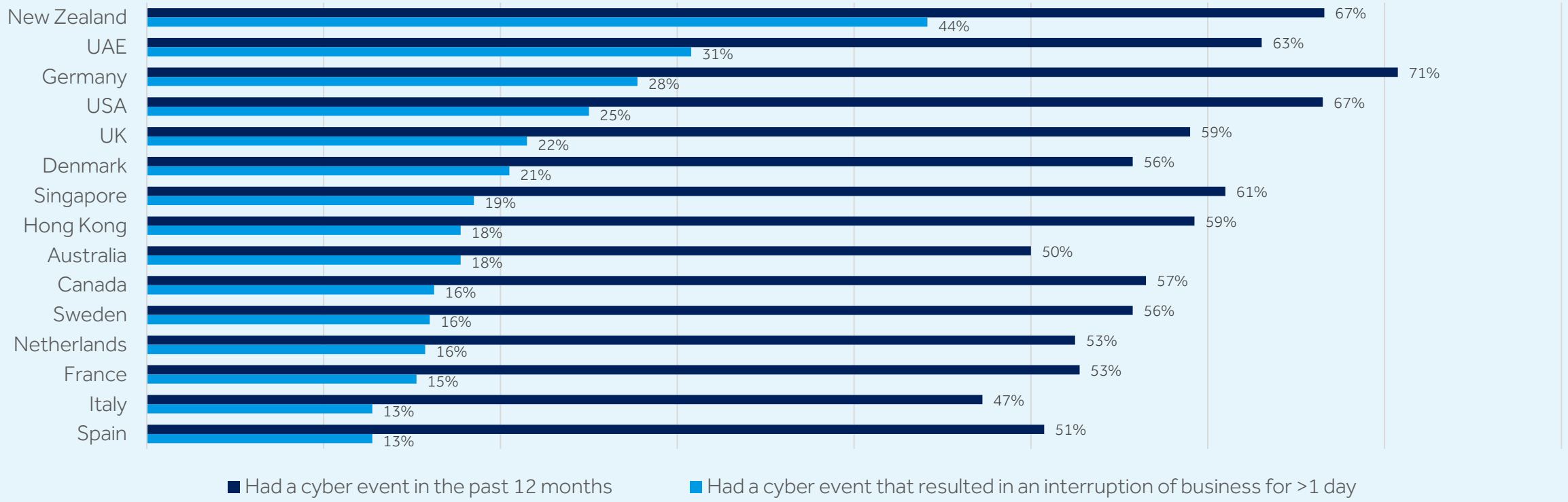


Q3 Does your business use Artificial Intelligence in its operations? Base: All respondents (6,016)

Cyber exposure in the last 12 months

While cyber events are common across all countries, the likelihood of significant business disruption varies substantially, suggesting differences in resilience and response rather than exposure alone

% of businesses experiencing cyber events and disruption lasting > 1 day

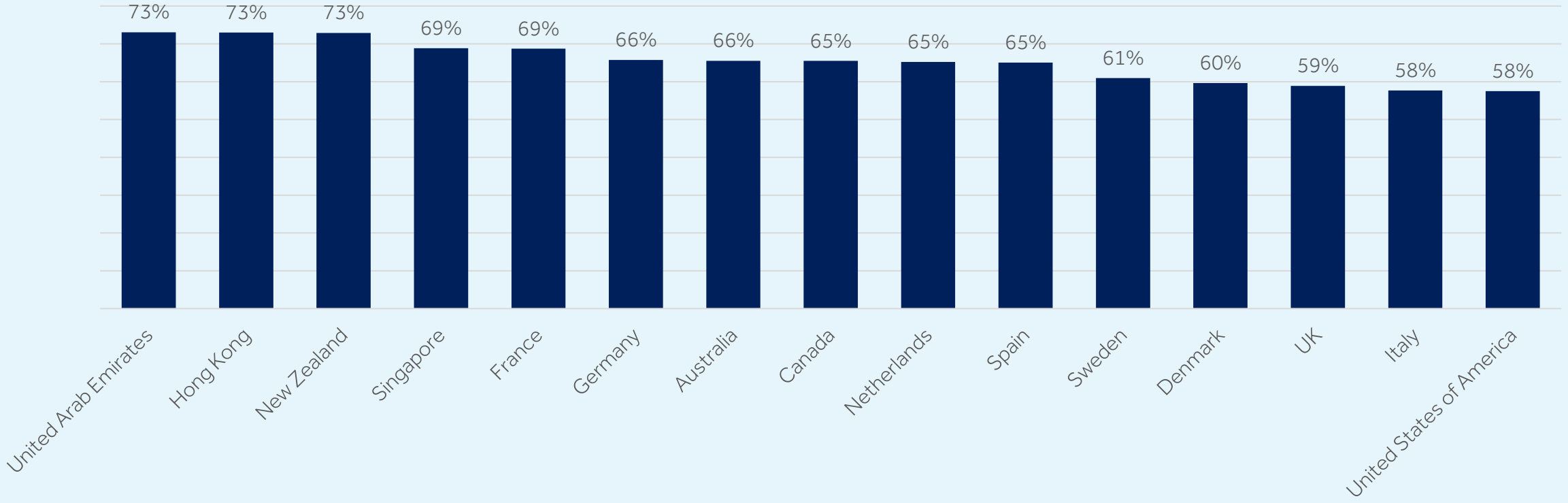


Q6 Over the past 12 months, how many cyber events resulted in an interruption of your business for more than a working day? Base: All respondents (6,016)

Supplier-related cyber attacks

Among businesses that experienced a cyber event in the past 12 months, two thirds (65%) say at least one incident was caused or related to a supplier

[Some, most or all attacks were related to a supplier]

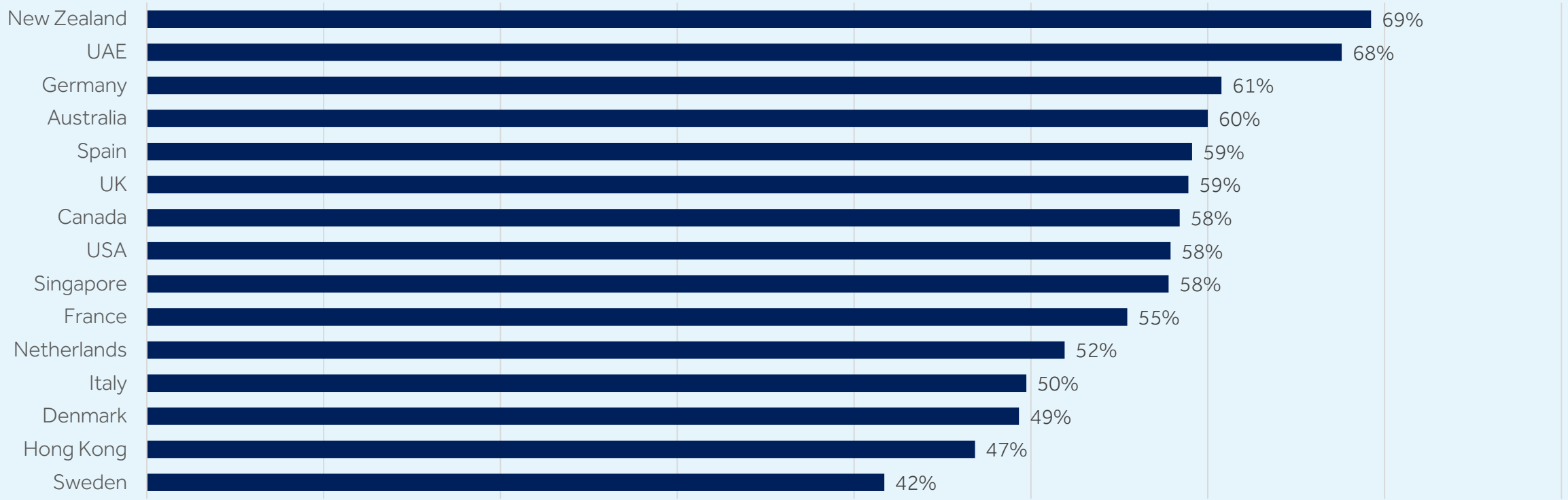


Q6A. You mentioned your business has experienced a cyber event in the past 12 months. In the past 12 months, were any of the attacks caused or related to a supplier of your business?
Base: All respondents whose business has experienced a cyber event in the past 12 months (3,480)

Financial impact of cyber attacks

Once cyber incidents occur, financial consequences are common. Some of the higher-loss markets tend to report greater disruption, suggesting that revenue impact tracks severity and duration of incidents

% of businesses experiencing revenue loss from cyber attacks

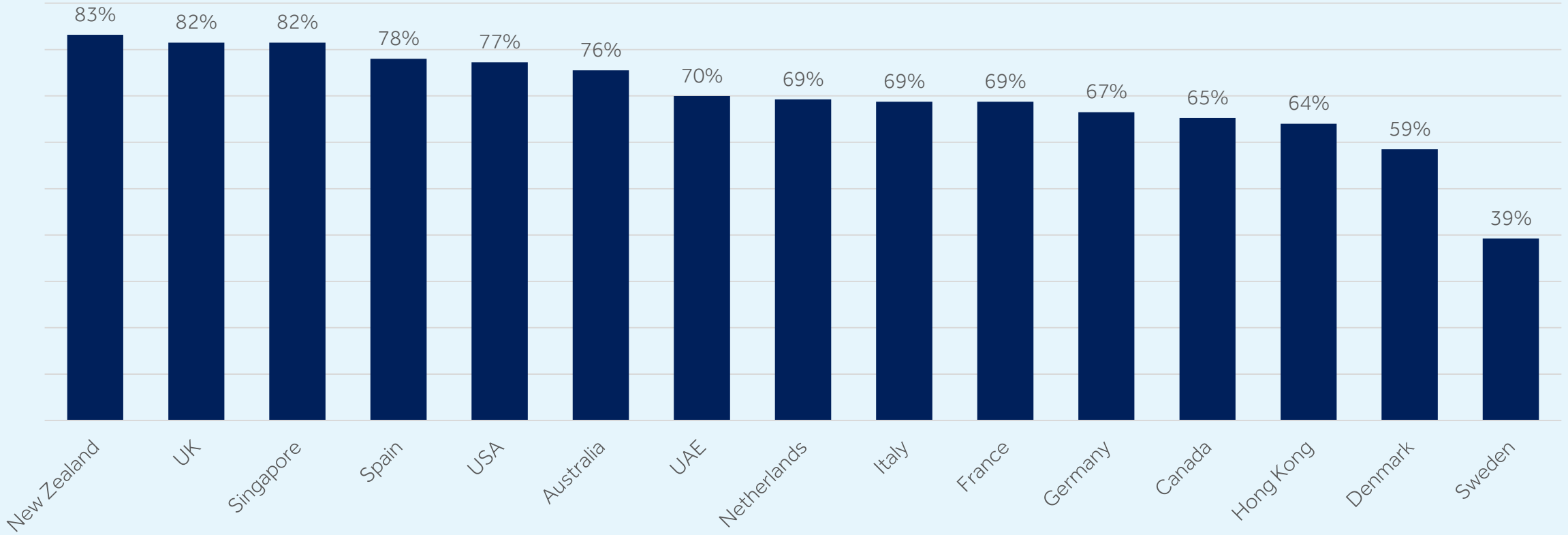


Q6B. Over the past 12 months, how many cyber attacks against your business or suppliers have resulted in a loss of revenue? Base: All respondents whose business has experienced a cyber event in the past 12 months (3,480)

Concern about cyber threats

While most business decision-makers express concern about cyber threats, intensity varies

% of business leaders concerned about cyber threats over the next 12 months

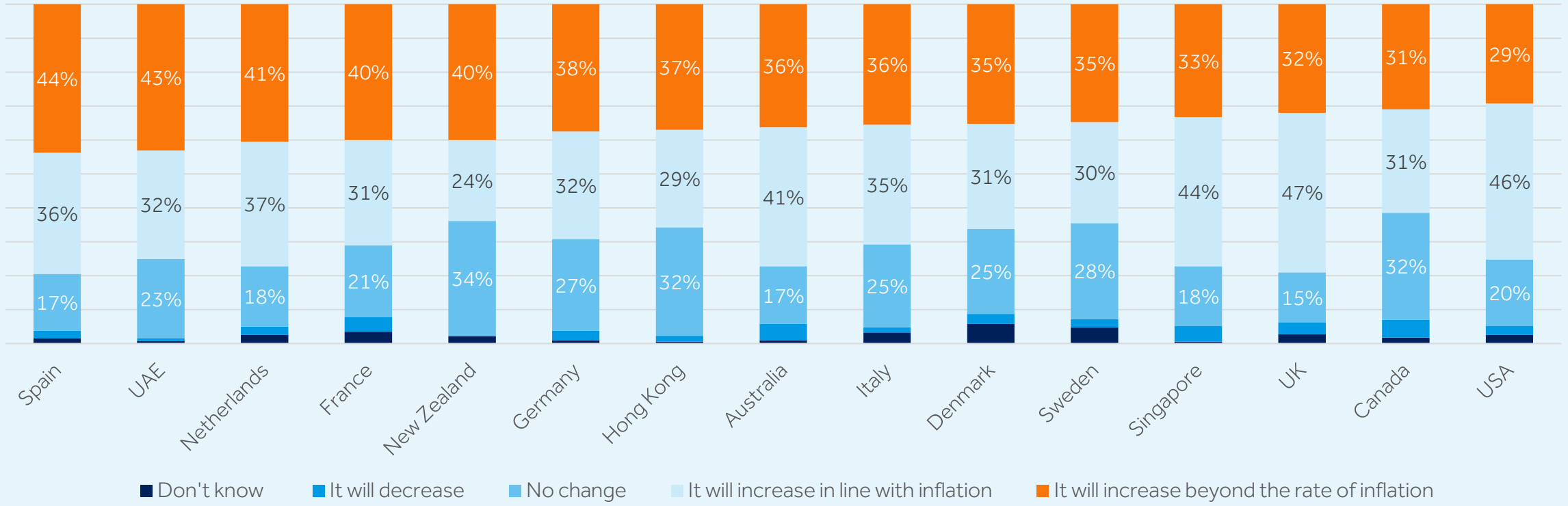


Q7. How concerned or not, do you feel about cyber threats your business may face over the next 12 months? Base: All respondents (6,016)

Cyber security budgets

Most businesses expect their cybersecurity budget to rise, but investment momentum is uneven globally, with inflation-level increases in English-speaking Western countries and real-term hikes elsewhere

Expected change in cyber security budgets over the next 12 months

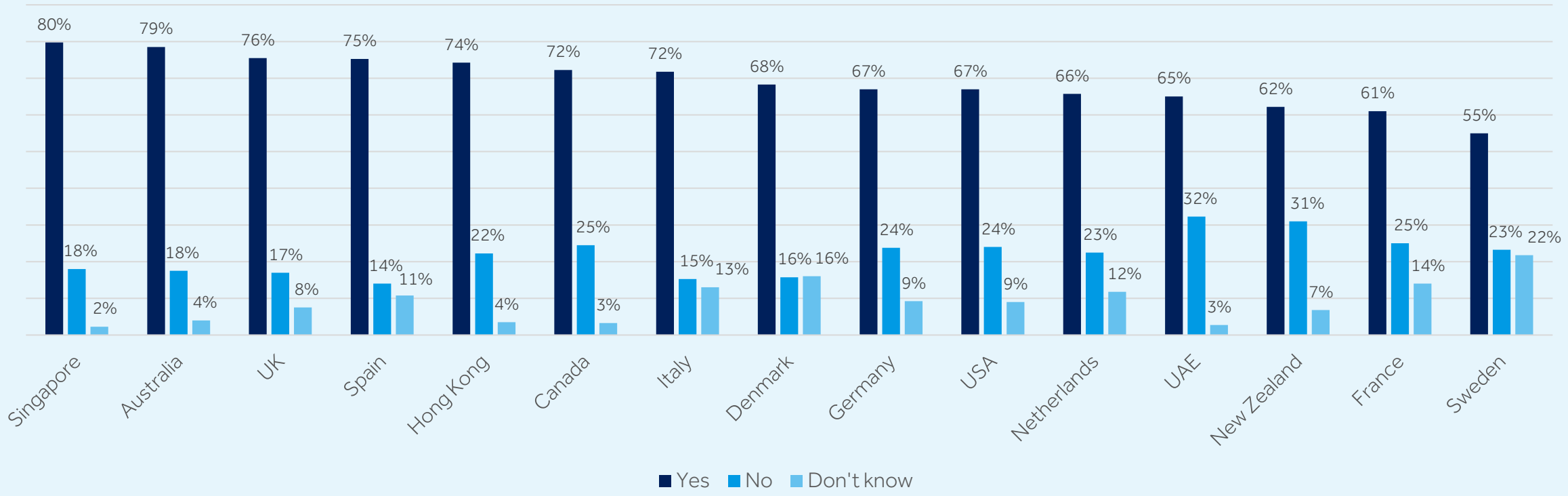


Q8. Over the next 12 months, how do you expect your business's IT cybersecurity budget to change? Base: All respondents (6,016)

Cyber insurance penetration

Cyber insurance is a standard feature of risk management for many businesses, although uptake still varies by market

% of businesses with cyber insurance

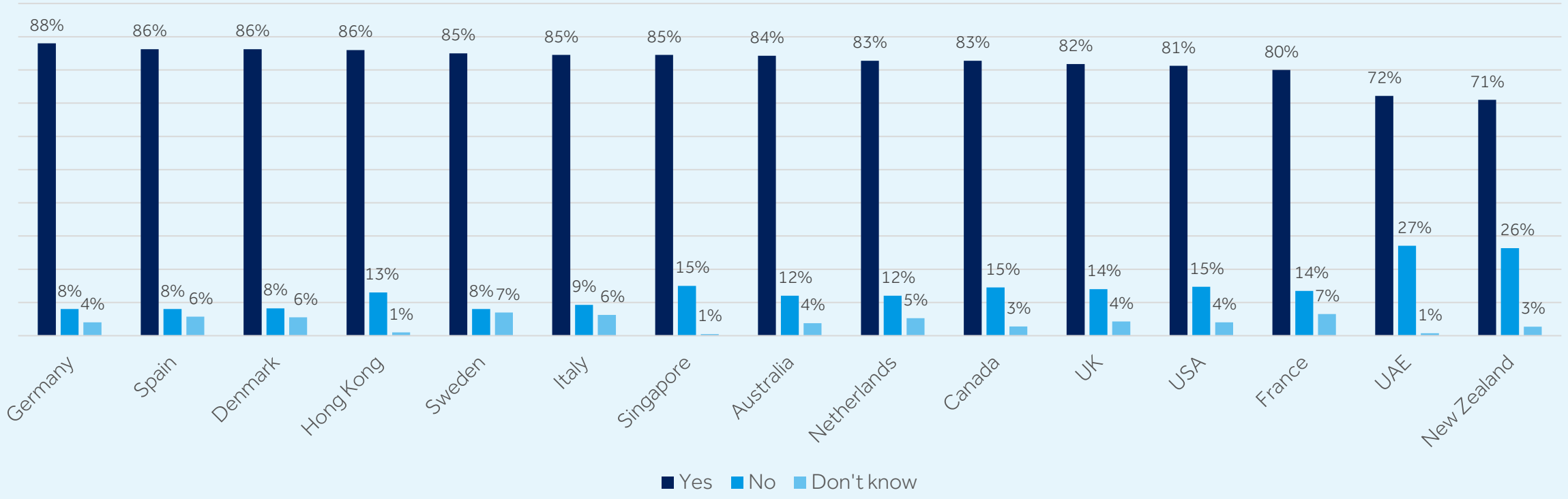


Q9. Does your business have cyber insurance? Base: All respondents (6,016)

Incidence response preparedness

Businesses with cyber insurance are more likely to have an incident response plan, suggesting a structured approach to risk management

% of businesses with an incident response plan

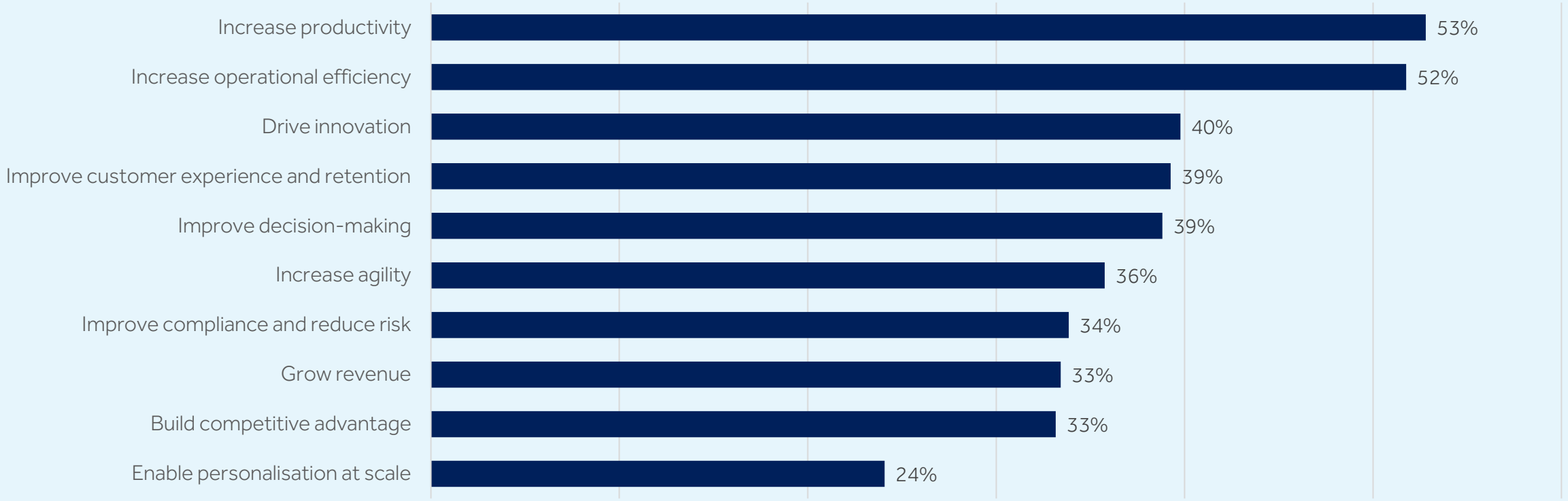


Q10. Does your business have an incident response plan to address a cyber event? Base: All respondents (6,016)

Why businesses use AI

AI adoption is primarily driven by productivity and efficiency gains, indicating a focus on enhancing existing operations rather than radical transformation

Main reasons for adopting AI

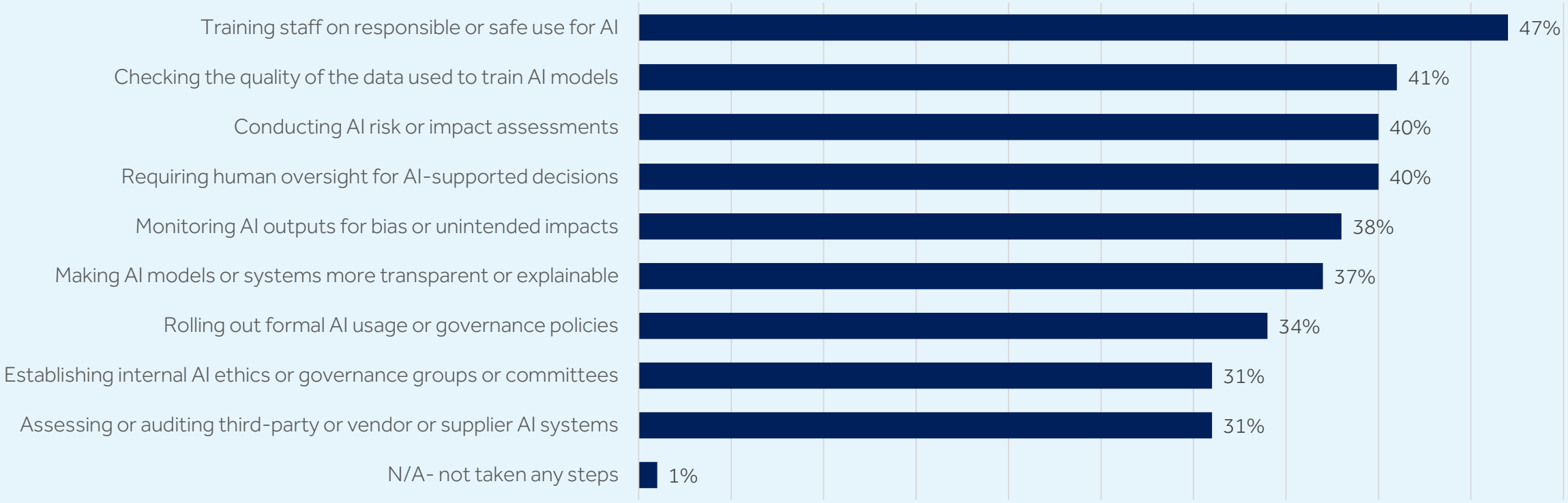


Q11. You mentioned your business uses Artificial Intelligence (AI) in its operations. For which of the following reasons, if any, is your business using AI?
Base: All respondents who say their business uses artificial intelligence in its operations (4,801)

Managing AI risks

Most businesses who use AI report some governance or oversight measures, although the mix of controls varies

Steps taken to manage AI use

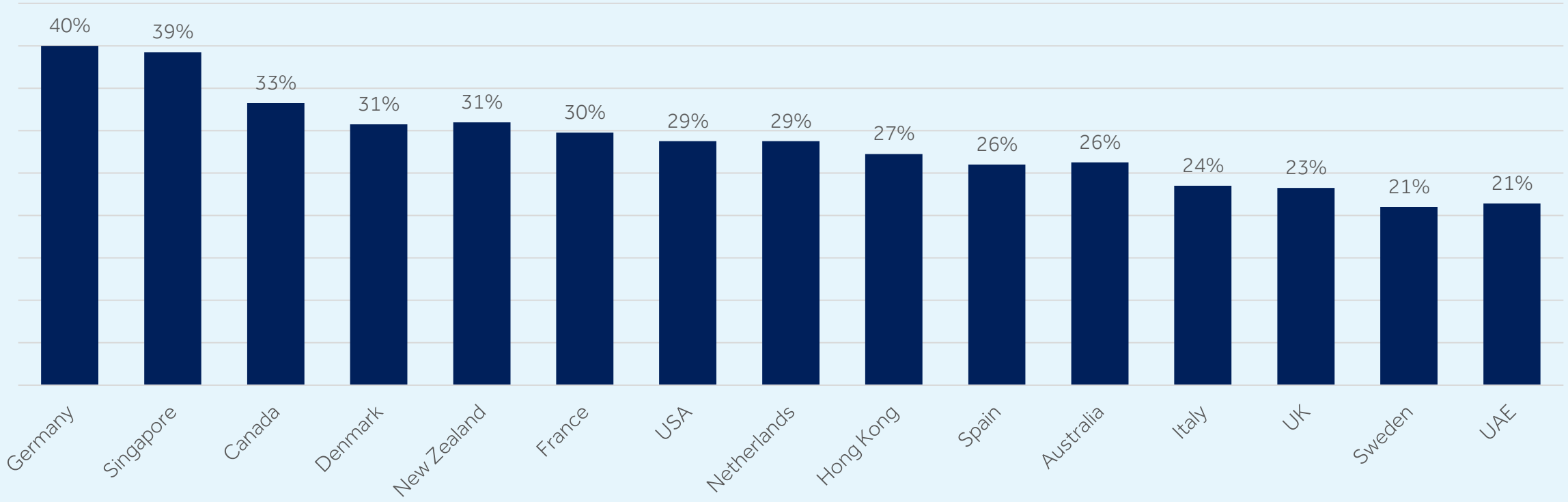


Q12. You mentioned your business uses Artificial Intelligence (AI) in its operations. Which, if any, steps has your organisation taken to manage the use of AI?
Base: All respondents who say their business uses artificial intelligence in its operations (4,801)

AI-enabled cyber attacks by market

A significant share of businesses report AI-enabled cyber incidents in the past year, with this most common in Germany and Singapore

% of businesses experiencing AI-enabled cyber attacks in the past 12 months by market

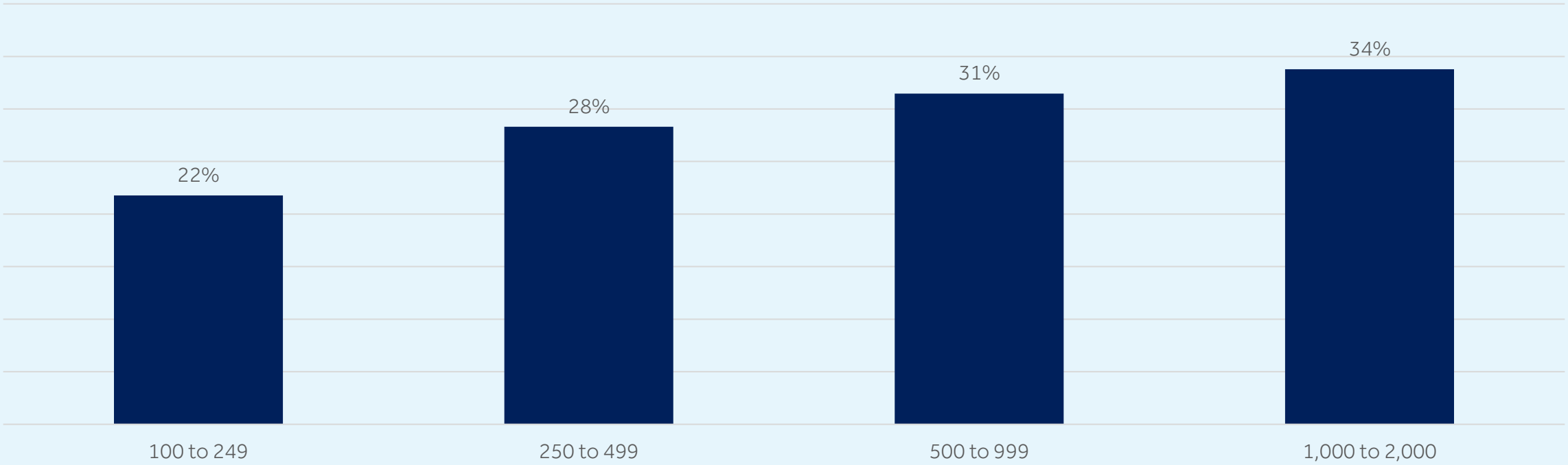


Q13. To the best of your knowledge, has your organisation experienced any cyber incidents in the past 12 months where AI was believed to have been used as part of the attack?
Base: All respondents (6,016)

AI-enabled cyber attacks by business size

Exposure is higher among larger organisations but not confined to them. Smaller firms also report AI-enabled attacks, highlighting that AI-driven threats are not limited to the largest or most visible targets

% of businesses experiencing AI-enabled cyber attacks in the past 12 months by business size

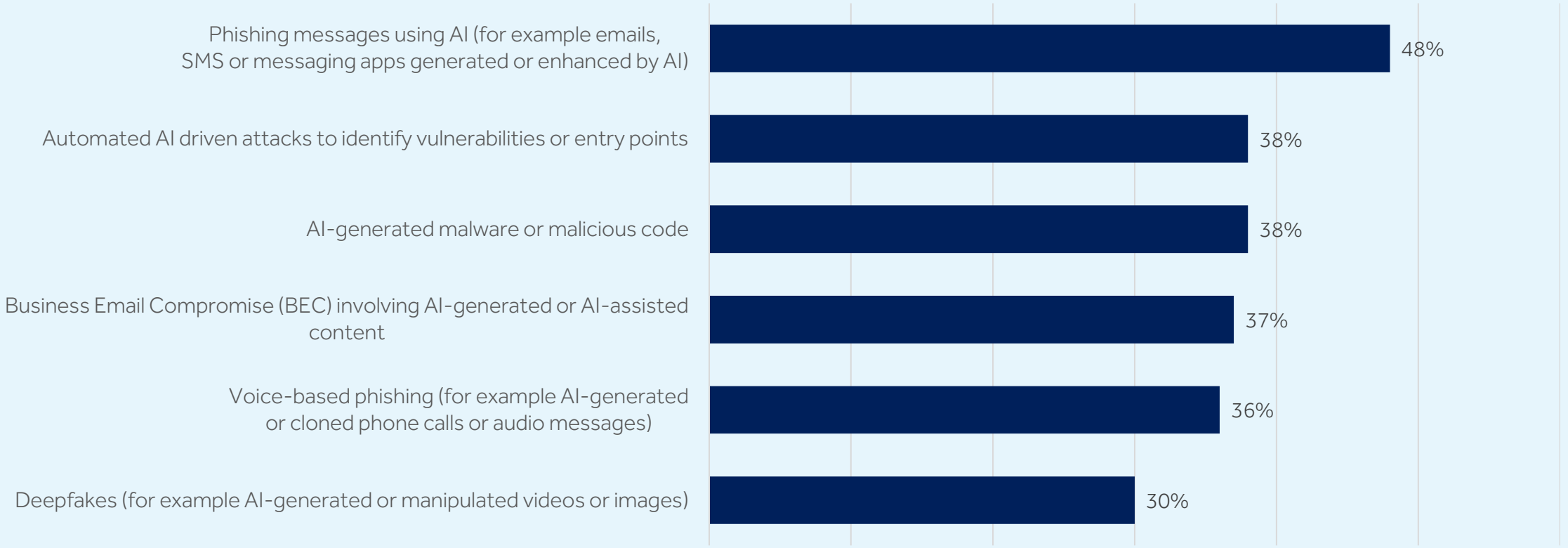


Q13. To the best of your knowledge, has your organisation experienced any cyber incidents in the past 12 months where AI was believed to have been used as part of the attack?
Base: All respondents (6,016)

Types of AI-powered cyber attacks

AI-generated phishing is the most commonly reported AI-enabled attack type

Types of AI-enabled attacks experienced

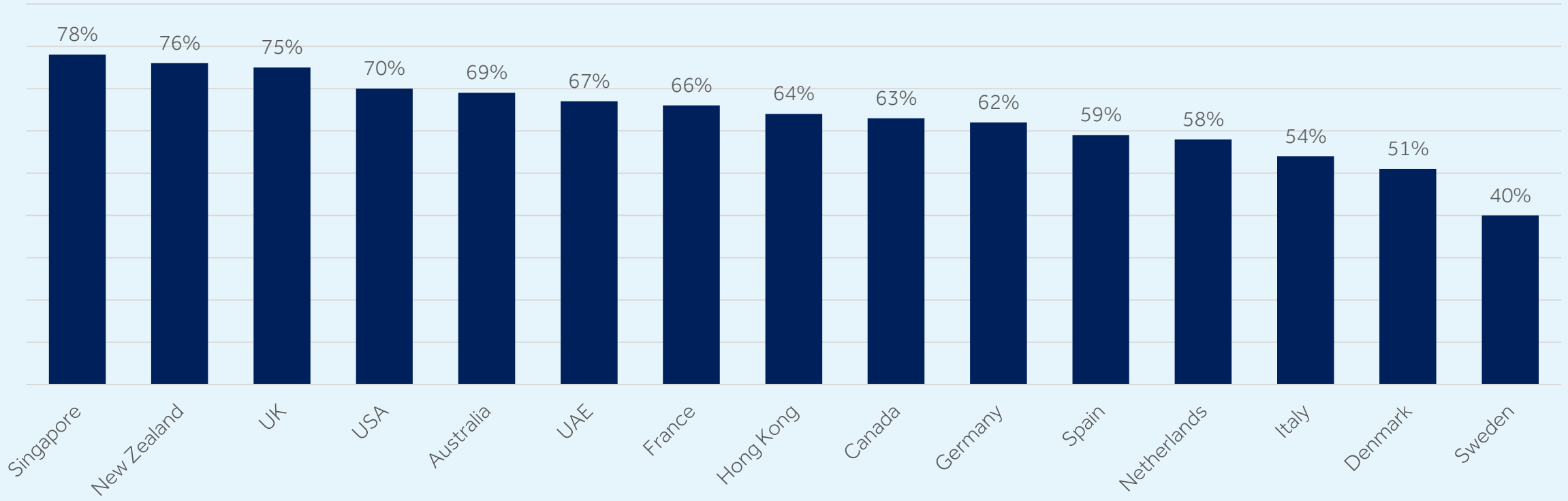


Q14. To the best of your knowledge, which type(s) of AI-powered attack targeted your business in the past 12 months?
Base: All respondents whose business experienced an AI-powered cyber incident in past 12 months (1,725)

Concern about supplier AI risks

Concern about supplier AI practices is widespread. Even in lower-concern markets, a substantial minority still report concern, suggesting supplier AI governance is emerging as a global issue

% of businesses concerned about risks from supplier use of AI



Q15. How concerned, if at all, are you about potential risks arising from how your vendors or suppliers use AI? Base: All respondents (6,016)

Key summary

Cyber risk is a routine business issue. Across markets, a majority of businesses report experiencing cyber events, and a substantial minority have faced operational disruption and revenue loss. Cyber risk is not confined to exceptional incidents but represents an ongoing operational exposure for many businesses.

The financial consequences of cyber incidents are tangible. Once cyber events occur, they frequently lead to direct revenue loss, highlighting that cyber resilience has clear commercial implications beyond reputational or technical considerations alone.

AI adoption is widespread across markets and sectors, driven primarily by productivity and efficiency gains. At the same time, a significant share of businesses report AI-enabled cyber attacks, showing that AI is accelerating both business capability and attacker sophistication.

Key summary

Most businesses report having cyber insurance and incident response plans, and many expect cybersecurity budgets to increase. However, a sizeable proportion of anticipated budget growth is expected to align with inflation rather than represent real-terms expansion.

Supplier involvement in cyber incidents is common, and concern about how vendors use AI is widespread. This reinforces the importance of managing cyber and AI risks beyond organisational boundaries.

While the overall patterns are broadly consistent across regions, including widespread cyber exposure, high AI adoption, and concern about third-party risk, the intensity of impact, concern and response varies by market. This suggests that global businesses are operating within a shared risk environment, but with differing levels of maturity, resilience and confidence in their existing controls.

Thank you