



2026 Intangible Versus Tangible Risks Comparison

EMEA Edition

Sponsored by Aon Risk Solutions
Independently conducted by Ponemon Institute LLC
Publication Date: May 2026



1

Executive Summary



Introduction

The 2026 Intangible versus Tangible Risks Comparison Report, consistent with findings from Aon’s Global Risk Management Survey, highlights a growing reality for organisations across Europe, Middle East and Africa. As business value becomes increasingly tied to intangible assets, the risks associated with protecting them are continuing to evolve. From cyber threats and AI-generated attacks to intellectual property exposures, the risk landscape continues to evolve at pace. The findings reveal a widening gap between the value organisations place on these assets and the measures in place to govern, manage, and transfer them effectively.

Cyber Risk Requires a More Integrated Approach

Cyber risk remains one of the most significant challenges facing organisations today, having evolved from a predominantly technical concern into a strategic business issue with direct implications for organisational performance, resilience and long-term value creation. As organisations become increasingly dependent on digital assets, interconnected technologies and third-party ecosystems, they face a growing need to understand cyber risk not only as a security challenge, but also as a business and financial risk that requires coordinated oversight across technology, risk management, finance and insurance functions.

Aon’s latest Global Risk Management Survey (GRMS) identifies cyber attack and data breach as the number one current and future business risk globally. Despite

increasing awareness, the GRMS highlights a persistent preparedness gap. Only 14% of organisations quantify their exposure to their most significant risks, while just 19% use analytics to evaluate the effectiveness of their insurance programmes. These findings suggest many organisations continue to face challenges in understanding, measuring and managing cyber-related exposures across the enterprise.

Most respondents expect their organisation’s cyber exposure to increase over the next two years, while a majority report having experienced a significant security exploit or data breach within the past 24 months. Beyond malicious attacks, organisations also face growing exposure from operational failures, human error and increasingly interconnected third-party ecosystems. Together, these factors reinforce the importance of adopting a broader approach to cyber risk management that supports resilience before, during and after an event.

Closing the Intangible Protection Gap

The research highlights a substantial protection gap between tangible and intangible assets. While physical assets benefit from relatively high levels of insurance protection, only 19% of losses associated with information assets are insurance covered, with a further 59% retained through self-insurance. As organisations become increasingly reliant on digital infrastructure, data, intellectual property and AI-enabled technologies,

understanding and managing these exposures is becoming a critical business priority.

The findings suggest that addressing intangible risks requires more than insurance alone. Organisations have an opportunity to strengthen how they identify, assess, quantify and manage cyber and information asset exposures across the enterprise. By combining governance, risk assessment, security controls, financial analysis and risk transfer strategies, organisations can make more informed decisions about protecting critical assets and improving resilience in an increasingly digital operating environment

At the same time, demand for cyber insurance continues to strengthen. Seventy-five percent of companies indicate plans to purchase cyber insurance in the near term, reflecting growing recognition of its role in supporting financial resilience as part of a broader approach to cyber risk management.

Managing AI Risks Responsibly

Artificial intelligence (AI) is rapidly becoming a critical enabler of efficiency, innovation and business performance across EMEA. Reflecting its growing importance, AI entered the GRMS top 10 future business risks for the first time, rising nine places since 2023 and ranking among the most significant risks organisations expect to face by 2028.

However, organisational readiness remains uneven. Many organisations continue to face uncertainty about the financial, operational, compliance and regulatory risks associated with AI. Awareness of evolving international regulatory requirements remains relatively limited, creating potential governance and liability challenges as organisations deploy AI at scale. There is a growing interest in risk transfer solutions to help organisations manage and mitigate this expanding risk landscape. As adoption accelerates, organisations have an opportunity to strengthen governance frameworks and review insurance programmes to ensure risks are effectively managed.

Protecting Intellectual Property Value

Intellectual property continues to represent a significant and growing proportion of enterprise value. Yet it appears to be receiving less strategic oversight, with its inclusion in enterprise risk management programmes falling from 67% to 49%, potentially leaving this critical asset class under protected. As these assets increasingly underpin competitive advantage and business growth, organisations should consider whether their insurance and risk strategies provide sufficient protection and reflect the increasing value and importance of these exposures.

Building Resilience Through Integrated Risk Management

Overall, the 2026 findings reinforce a broader trend identified in the GRMS: intangible risks are becoming increasingly important drivers of organisational performance, resilience and long-term value creation. As cyber threats evolve, AI adoption accelerates and intellectual property continues to grow in strategic importance, organisations have an opportunity to strengthen governance, improve visibility into risk exposures and address existing protection gaps.

The findings also suggest a growing need for a more integrated approach to risk management. Rather than viewing cyber, AI and intellectual property risks as isolated challenges, organisations can benefit from considering how these exposures interact across operations, technology, finance and risk management

functions. By embedding intangible asset considerations within enterprise risk management frameworks, organisations can better align risk mitigation, financial resilience and long-term business objectives.

By adopting a more holistic approach to risk management and securing appropriate insurance and risk financing solutions, businesses can better protect critical intangible assets, support informed decision-making and enhance their ability to respond to an increasingly complex risk landscape.

This report is designed to help organisations turn greater awareness of intangible risk into informed action. By providing clearer insight into the evolving exposures associated with cyber, AI and intellectual property, the findings can support more effective conversations across risk, finance, technology and leadership teams. As organisations seek to better understand their exposure, evaluate protection gaps and strengthen resilience, the research provides a foundation for more informed decisions regarding risk mitigation, risk financing and long-term enterprise value protection.

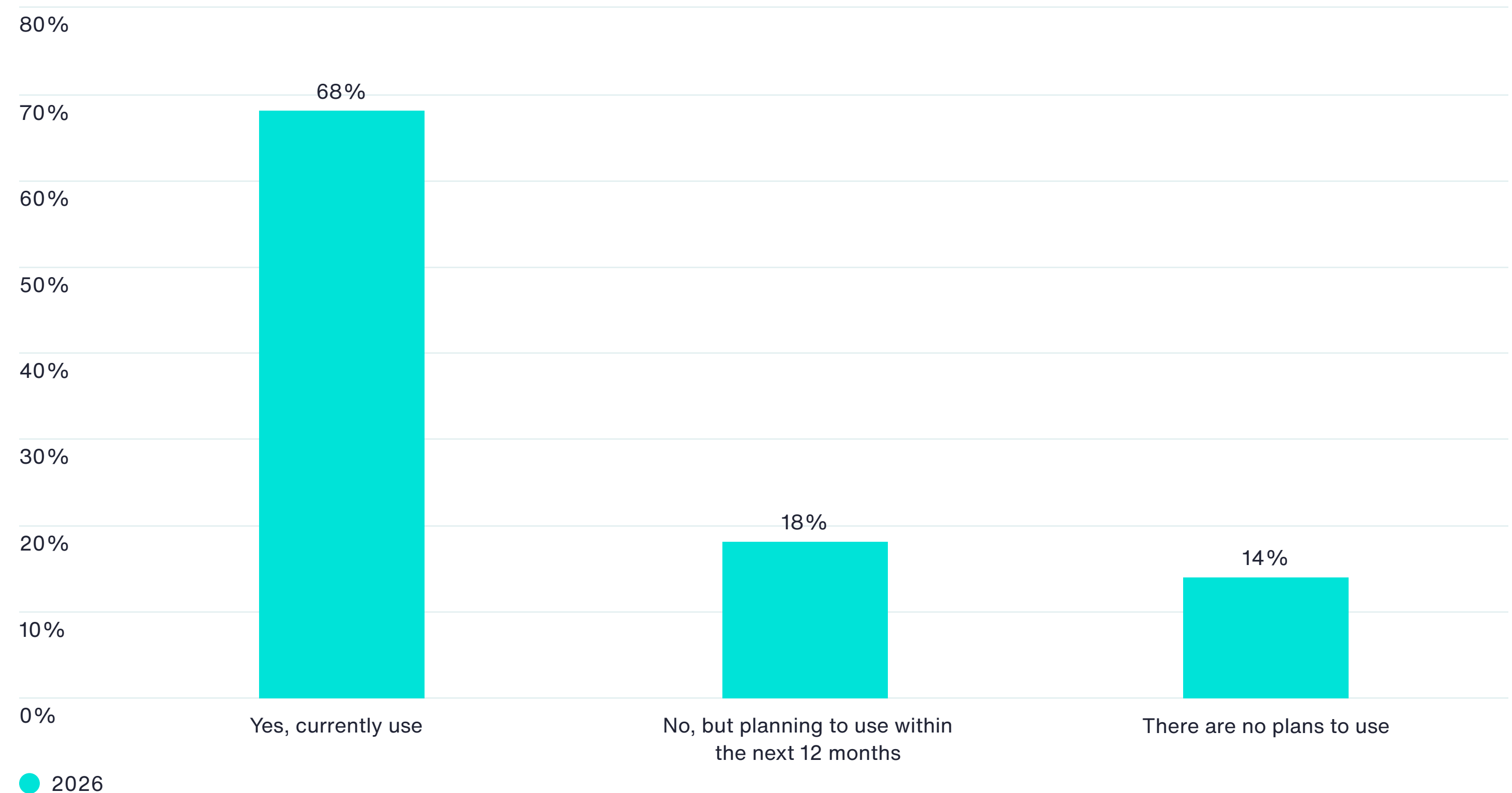
Contents

Table of Contents	Page
Part 1. A High-level Overview of the Consolidated Global Findings	14
Part 2. Key Findings	18
The Valuation of PP&E, Information Assets and Probable Maximum Loss	14
Cyber Risk Exposures Continue to Increase	15
The Use of Cyber Insurance to Mitigate the Financial Consequences of Data Breaches and Security Exploits	36
The Vulnerability of IP Assets	41
The Use of AI to Reduce Cyber Risks	49
Methods	53
Appendix 1. Caveats	56
Appendix 2. Survey Data Tables	58

Growth of Artificial Intelligence by AI Deployers

However, as digital transformation accelerates, information assets—including customer data, algorithms, source code, quantum computing, artificial intelligence, crypto ¹ and intellectual property—have become equally or more valuable.²

Most organisations (86 percent of respondents) use or intend to use artificial intelligence (AI) products or services.

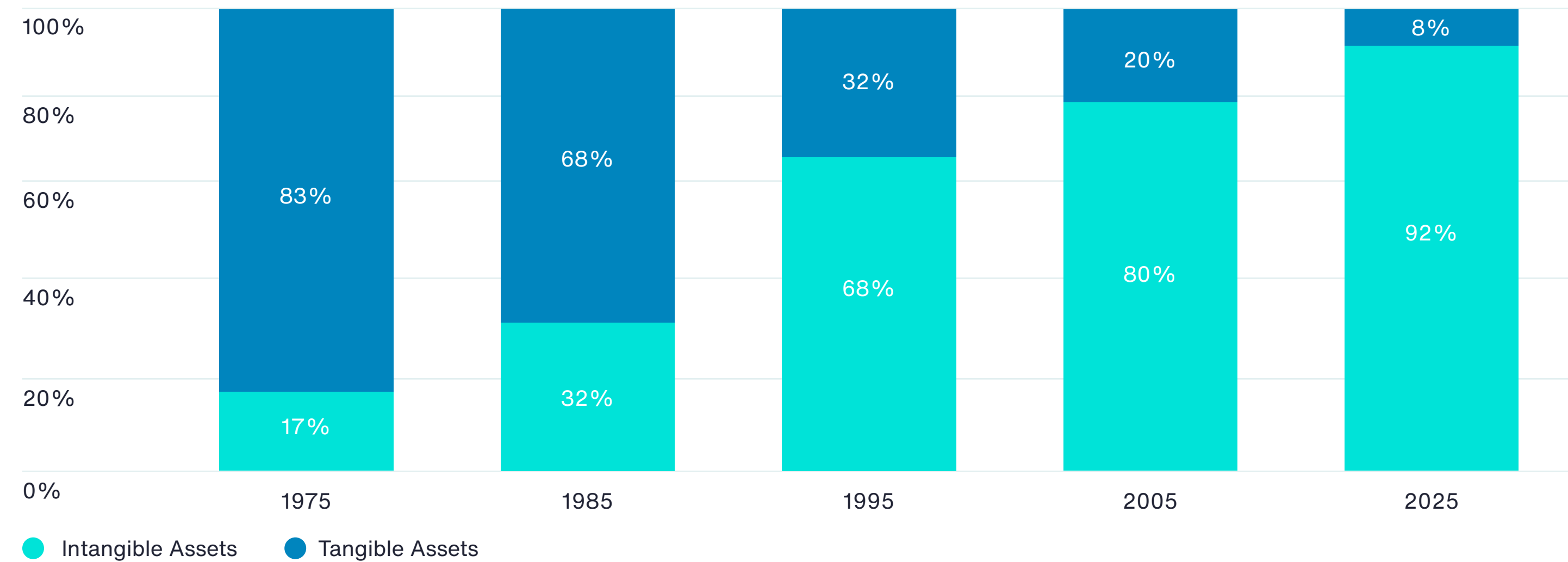


¹ [Aon Announces First Stablecoin Insurance Premium Payment](#)

² 2026 Ponemon Intangible Risks Comparison Report (AI CHART & CRYPTO GRAPH); and Ocean Tomo 2025 Intangible Asset Market Value Study Results

Historical Evolution from Tangible to Intangible Assets

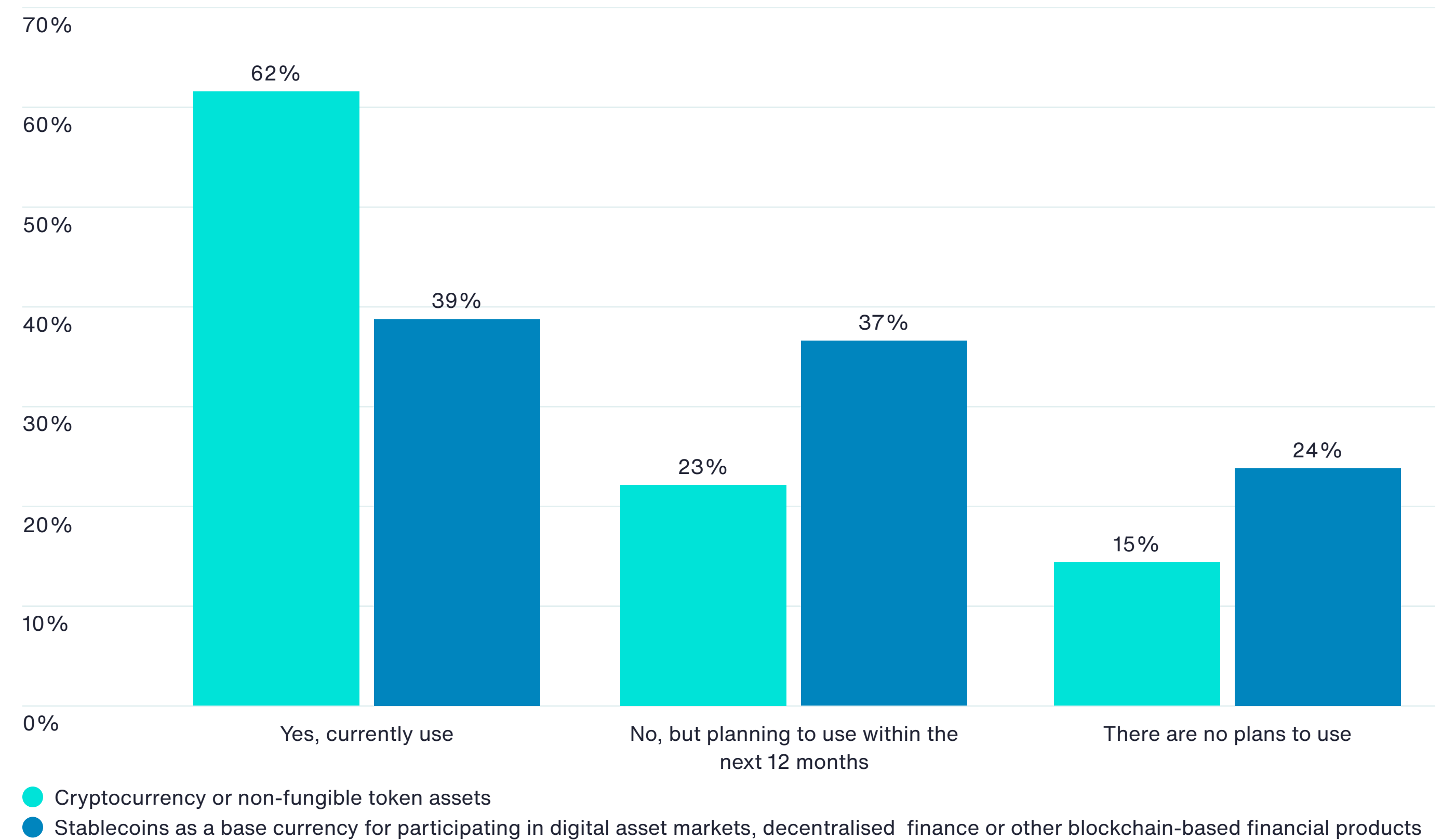
Tangible assets vs. Intangible assets for S&P 500 companies, 1975 - 2025



5 Largest Global Companies by Market Cap	• IBM	• IBM	• GE	• GE	• NVIDIA
	• Exxon Mobil	• Exxon Mobil	• Exxon Mobil	• Exxon Mobil	• Apple
	• Procter & Gamble	• GE	• Coca-Cola	• Microsoft	• Microsoft
	• GE	• Schlumberger	• Altria	• Citigroup	• Amazon
	• 3M	• Chevron	• Walmart	• Walmart	• Alphabet

Use of Cryptocurrency, Non-Fungible Token Assets and Stablecoins

The uncertain and evolving legal liability environment in the wake of the March 2026 verdicts against Meta and Google add additional complexity.³ Furthermore, the Delaware Superior Court ruled that Meta’s insurers owe no duty to defend on claims alleging harm done to children, which raises the importance of insurance implications.⁴ The report therefore evaluates the financial implications of these risks, including their probable maximum loss (PML), likelihood of occurrence, and the adequacy of existing risk transfer mechanisms such as intellectual property, crypto, artificial intelligence, quantum computing and cyber insurance.⁵



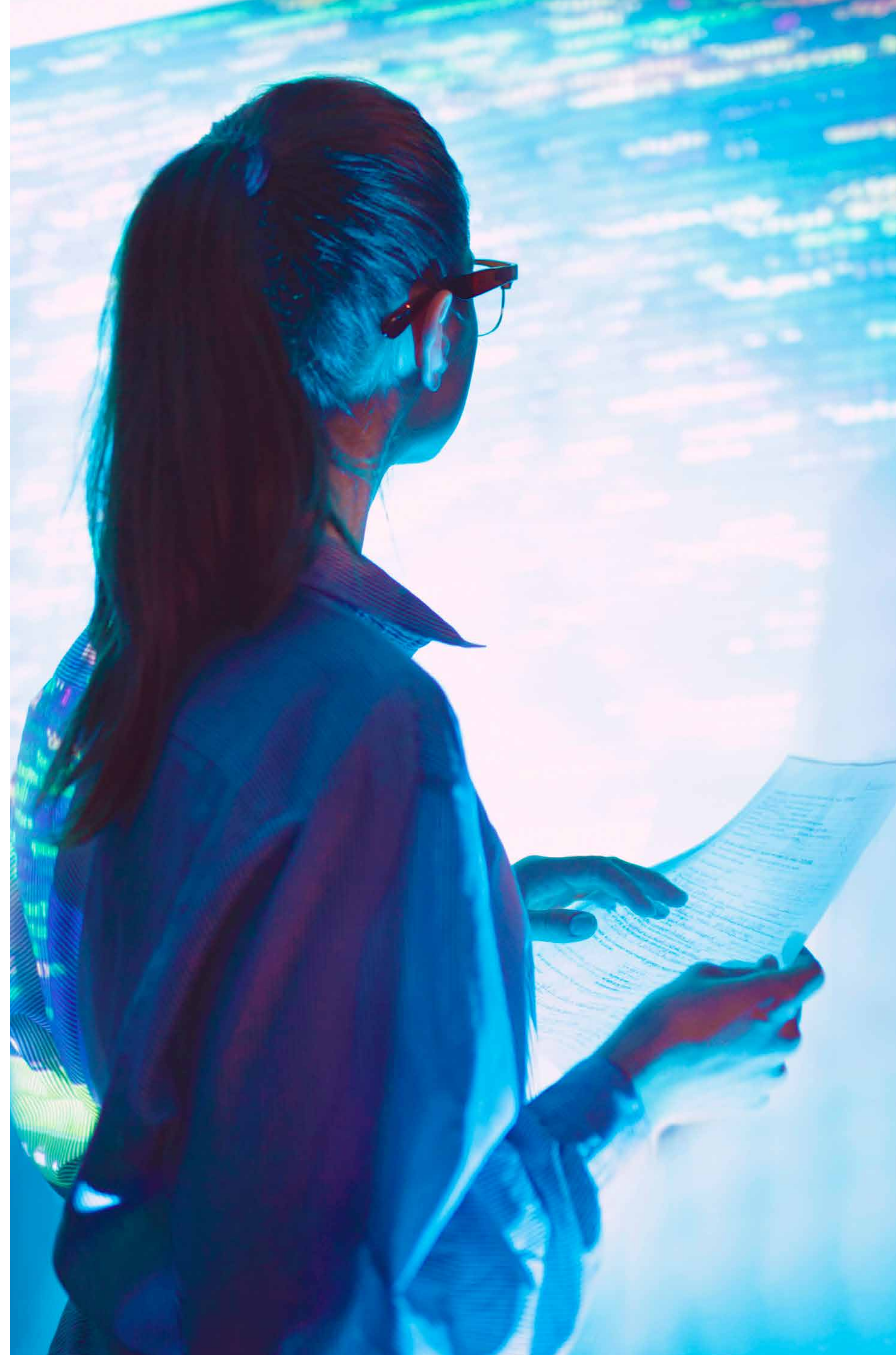
³ [US jury verdicts against Meta, Google tee up fight over tech liability shield](#)

⁴ [What are the insurance implications of Meta’s massive liability lawsuit?](#)

⁵ [On Aon Podcast: The New Risk Capital Playbook for Today’s Business Leaders; Private equity and capital providers to expand reinsurance presence via AI-linked securities: EY – Artemis.bm](#)

AI technology, products and services have developed much faster than AI risk management. As a result, to the extent that evolving AI perils might be covered by existing insurance policies, such coverage falls over ninety percent (90%) under “Silent AI” insurance. Silent AI coverage means that the underlying policy neither affirmatively covers AI nor excludes AI — the policies don’t mention AI. Therefore, we are in a similar position to that of cyber perils in the early 2000’s whereby insureds attempted to fit cyber losses into property, general liability, professional liability, employment practices liability, crime, etc. policies — none of which mentioned cyber (“Silent Cyber” insurance). Insurers responded by adding specific language to legacy policies to clarify that most cyber perils were not intended to be covered, which led to the birth of standalone cyber insurance policies. It took the Lloyd’s of London Market Association eighteen (18) years of coverage ambiguity to finally mandate that all policies must either affirmatively specify cyber coverage grants or include specific cyber exclusions (no more “Silent Cyber” insurance). If we leverage the lessons learned from cyber, we can expedite the AI risk management learning and execution process. After identifying organisation AI usage, potential liability and implementing risk management best practices, map your organisation’s AI risks to existing insurance while monitoring the growing AI exclusions and sub-limit provisions.⁶

⁶ Aon Risk Capital 2026 AI Fact Sheet: <https://assets.aon.com/-/media/files/aon/reports/2026/aon-ai-fact-sheet-2026.pdf>



“

With AI adding complexity to traditional operating models, leaders need forward-looking, actionable insights to understand their exposures and take effective action to manage their risks, protect their balance sheets and grow amidst the volatility.

Greg Case
CEO, Aon

“

Data centers are growing rapidly in scale and complexity as artificial intelligence adoption accelerates, creating both a new challenge and a defining opportunity for the insurance industry as risk and capital increasingly converge.

Joe Peiser
Aon Risk Capital CEO

AI Insurance Coverage and Gaps

Legacy Perils	Peril	Media Liability	Tech E&O, MPL, PI	General Liability	Intellectual Property	Cyber	Crime	D&O	EPL	AI Specific
	Professional Services/technology errors, omissions or negligent acts	Limited to Media orgs								
	Copyright (Output) or Trademark		Can be added	Except media orgs		Requires cyber trigger				
	Patent Infringement and Trade Secrets	Not in base form								
	Discrimination and Bias (employment related – AI Deployer)									
	Defamation, Libel, Slander		Can be added	Except media orgs						
	Bodily Injury		Base forms exclude	Products only		Contingent BI can be added				By special endorsement
	Tangible Property Damage		Base forms exclude	Products only		Contingent PD can be added				By special endorsement
	Privacy and Security breaches liability									
	Loss of Financial Assets/Market Manipulation									
	Product Liability/Recall									
	Business Interruption		Only when cyber added							
New AI Perils	Copyright (Input AI Training)	Limited to media perils								
	AI Regulation Violations		Can be added			Only for privacy/security		Some coverage for FTC/SEC, etc.		To extent allowable by law
	Breach of AI Warranty/Performance Guaranty		Only if due to negligence,	Only via customisation						Varies by solution
	Breach of D&O duties (AI Washing)									Partially included
	Discrimination and Bias (AI Provider)					Requires cyber trigger			Not for non-EPLI	
	Autonomous Vehicles/Robotics/IoT		Requires bespoke			Requires cyber trigger				
	Deepfake	Limited to media perils	Excludes funds transfers			Excludes funds transfers	For funds transfers			Excludes funds transfers
	Hallucinations	Limited to media perils				Limited to privacy/security				

■ Affirmative AI coverage ■ Available, but silent as to AI ■ Ambiguous, unless specifically added ■ Excluded

By comparing tangible and intangible risk exposures and examining evolving technological and regulatory environments,⁷ the report provides insight into how organisations can better align enterprise risk management strategies with the realities of an increasingly digital economy.⁸

The study reveals that intangible assets are now central to organisational value and risk exposure. On average, surveyed organisations report information assets valued at approximately **\$1.49 billion**, slightly exceeding the **\$1.40 billion** average value of tangible assets such as PP&E. Correspondingly, the estimated **probable maximum loss (PML)** from the theft or destruction of information assets averages **\$1.14 billion**, marginally higher than the **\$1.04 billion** estimated PML for physical asset damage or destruction.

⁷ [Titration of Artificial Intelligence Risk Management to Accelerate AI Growth; U.S. Senate Committee Hearing on “Guardrails and Growth: AI’s Role in Capital and Insurance Markets”.](#)

[Policy Alert: New U.S. Executive Order on Artificial Intelligence – Aon Tips for Better Risk Capital Decisions.](#)

⁸ [Aon Risk Capital 2026 AI Fact Sheet: <https://assets.aon.com/-/media/files/aon/reports/2026/aon-ai-fact-sheet-2026.pdf>.](#)

⁹ [Hyperscalers a level of opportunity we haven’t seen before: Aon CEO Greg Case; Aon designed & placed world’s first data centre reinsurance treaty, says CEO Case - Reinsurance News](#); Aon expands Data Center Lifecycle Insurance Program to \$2.5 billion, strengthening resilience for AI-driving digital infrastructure - Jan 14, 2026.

¹⁰ [Where Cyber Meets Physical: Rethinking Risk in the AI Age.](#)

¹¹ [Aon leads peers on AI strategy, TD Cowen says | Insurance Business.](#)

¹² [Aon’s Resilience Quotient](#) is an analytical framework and a tool that integrates Aon’s proprietary Risk Capital and Human Capital data together with sentiment analysis from Gallup, which provides a structured way to understand how risk compounds across systems, how resilience is built and activated and where targeted actions can most effectively influence performance. <https://www.aon.com/en/insights/reports/aon-resilience-quotient>.

¹³ [Cost of a data breach 2025 | IBM.](#)

Cyber risk continues to escalate globally.⁹ Sixty-three percent of surveyed organisations experienced at least one material or disruptive security exploit or data breach within the past two years, with an average financial impact of approximately **\$5.75 million** per incident. Human error and negligence remain the most common cause of these events, followed by cyberattacks that disrupt IT and business operations. As a result, two-thirds of respondents expect their organisation’s cyber risk exposure to increase over the next two years.

Despite growing risk awareness, many organisations remain underinsured. Only **35 percent** report having cyber insurance coverage, and many policies do not fully cover key risks such as negligence or ransomware related costs.¹⁰ Coverage gaps are also evident in emerging areas such as AI-related losses, with 63 percent of respondents indicating their existing insurance policies do not cover AI-related threats. At the same time, interest in new risk transfer solutions—including standalone cyber or AI liability policies—is increasing.¹¹

¹⁴ [Aon’s Resilience Quotient](#) is an analytical framework and a tool that integrates Aon’s proprietary Risk Capital and Human Capital data together with sentiment analysis from Gallup, which provides a structured way to understand how risk compounds across systems, how resilience is built and activated and where targeted actions can most effectively influence performance. <https://www.aon.com/en/insights/reports/aon-resilience-quotient>.

Intellectual property assets represent another major area of exposure. The average value of IP assets has risen to **\$787 million**, representing about **44 percent of total organisational assets**, yet fewer organisations report having formal enterprise risk management strategies for IP protection. Additionally, 45 percent of organisations report experiencing a material IP-related incident within the past two years, most commonly involving trade secrets or infringement of organisational rights.

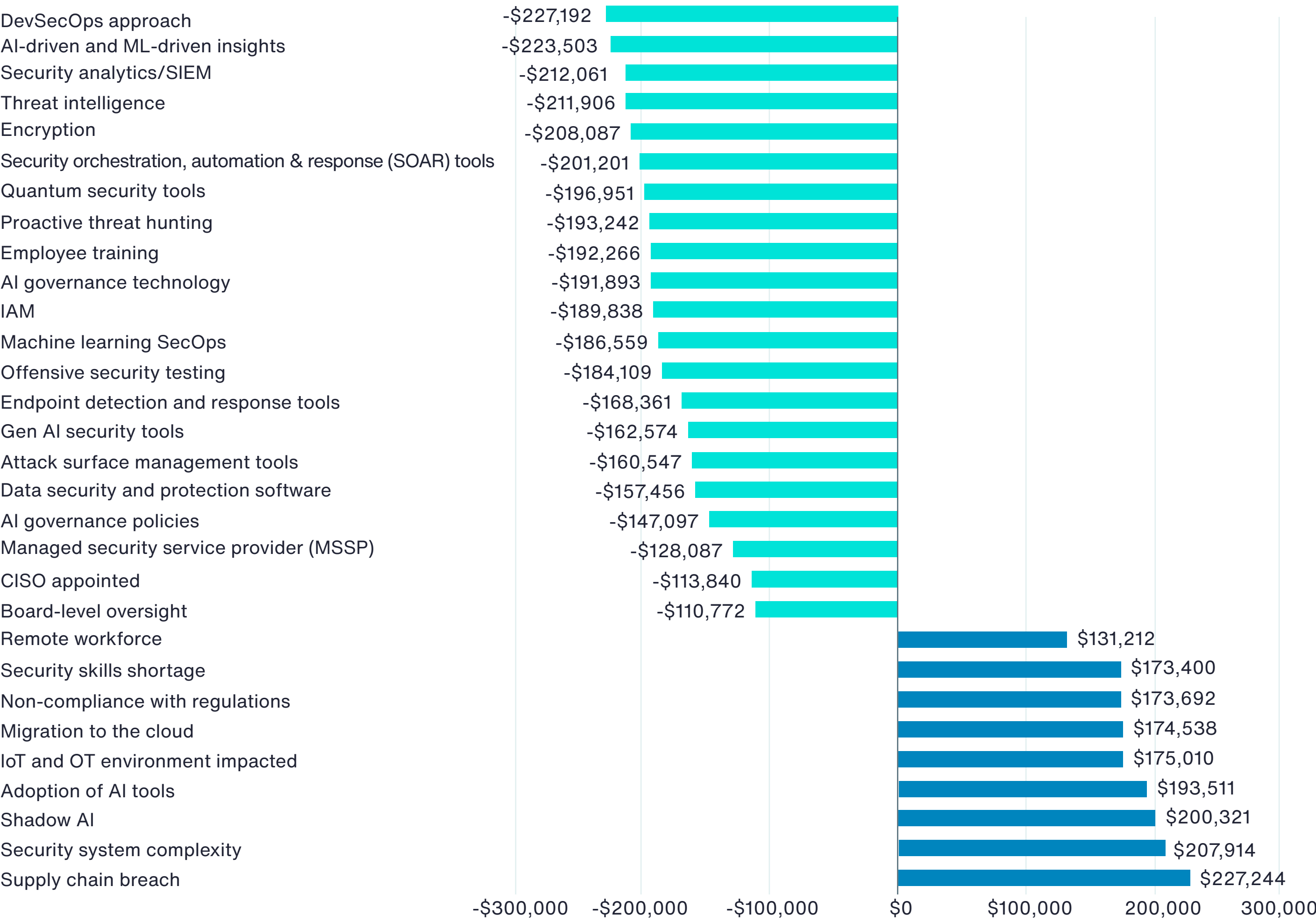
The research also highlights the rapid adoption of artificial intelligence and digital assets. Sixty-eight percent of organisations already use AI technologies, and most respondents consider AI either critical to core operations or a significant driver of innovation.¹² However, the potential PML associated with inadequate AI security tools is estimated at **\$1.57 billion**, underscoring the financial stakes associated with AI governance and security.¹³ In addition to AI financial statement perils, AI is also having a growing material impact on human capital.¹⁴

IBM “Cost of a Data Breach Report 2025: The AI Oversight Gap” (measured in USD)

Can we quantify the frequency and severity of intangible risks exposures and implement risk management best practices to lower the Total Cost of Risk while increasing the Return on Investment of intangible assets? Weighing each AI risk factor is an evolving process since AI perils are dynamic and fluid. In order to provide relative coefficients for each AI risk factor, Aon is building a database of AI claims, based on AI-enabled Bayesian frequency and severity actuarial modelling. For example, a recent IBM report includes the following weights associated with AI factors that increase or decrease costs from a data breach:

Incident response plan and testing

Factors that decrease/increase the total cost of a data breach²⁰



Thus, as the insurance industry collects more AI frequency and severity loss data, we will be in a better position to provide weights to each AI risk factor. Thereafter, we can use analytics to allocate resources appropriately to maximise ROI while lowering the Total Cost of Risk.

Overall, the findings demonstrate that organisations face increasing exposure to intangible risks driven by digital transformation, cyber threats, and emerging technologies.¹⁴ To address these challenges, organisations must strengthen cyber resilience, integrate intangible asset risks into enterprise risk management frameworks, and evaluate more comprehensive insurance¹⁵ and governance strategies¹⁶ to mitigate potentially catastrophic financial losses.¹⁷

“

Data is the foundation, and AI sits below that, feeding off the data foundation. Next is analytics, which we break into three areas: analyzers, which are forward-looking; benchmarks, which help clients compare themselves to others, both within industry and across industry; and diagnostics, which help to isolate problems and make recommendations on how to improve results.

Mindy Simon
COO, Aon

¹⁵ [Cost of data breach 2025 | IBM](#)

¹⁶ [AI Risk 2026: What Business Leaders Need to Know](#)

¹⁷ [Alternative capital hits \\$124bn. Consistent investor appetite to drive it higher still: Aon: https://www.artemis.bm/news/alternative-capital-hits-124bn-consistent-investor-appetite-to-drive-it-higher-still-aon/?utm_source=rss&utm_medium=rss&utm_campaign=alternative-capital-hits-124bn-consistent-investor-appetite-to-drive-it-higher-still-aon](https://www.artemis.bm/news/alternative-capital-hits-124bn-consistent-investor-appetite-to-drive-it-higher-still-aon/?utm_source=rss&utm_medium=rss&utm_campaign=alternative-capital-hits-124bn-consistent-investor-appetite-to-drive-it-higher-still-aon)

Part 1. A High-level Overview of the Consolidated Global Findings

The Use of AI to Reduce Cyber Risks

AI is important in supporting efficiency, process improvement or innovation. Sixty-eight percent of respondents currently use AI and another 23 percent intend to use AI products or services. Thirty percent of respondents say AI is a significant driver of efficiency, process improvement or innovation. Twenty-five percent say AI is critical to the success of core products, services and/or operations. Only 21 percent say AI is used but has a negligible impact on their business.

Organisations are vulnerable to the financial consequences of an AI-generated attack. The average value of the largest loss (PML) that could be caused by the lack of AI tools to secure information assets over the next 12 months is \$1,673 million. An average of 49 percent of the potential loss is covered by insurance, including captives reinsured but not including captives not reinsured.

Sixty-five percent of respondents say their companies' existing insurance policies or a separate standalone AI liability policy do not cover the risks of an AI-generated attack and 14 percent of respondents are unsure. Of these respondents, 28 percent of respondents are very interested, and 39 percent of respondents are interested in purchasing an AI liability policy. Only 14 percent of respondents are not interested.

There is a lack of awareness of the economic and legal consequences resulting from non-compliance with AI regulations in other countries. Only 29 percent of respondents say they are fully aware of the consequences of non-compliance which can result in substantial fines up to 7 percent of an organisation's worldwide revenue.

The use of cryptocurrency or non-fungible token assets and stablecoins are expected to increase. Sixty percent of respondents say their organisations currently use and 29 percent say they plan to use cryptocurrency or non-fungible token assets within the next 12 months. Thirty-four percent of respondents say their organisations use stablecoins as a base currency for participating in digital asset markets, decentralised finance (DeFi) or other blockchain-based financial products and 46 percent plan to use in the next 12 months.

The Valuation of PP&E, Information Assets and Probable Maximum Loss (PML)

The value of Probable Maximum Loss (PML) from stolen or destroyed information assets is higher than for damaged or destroyed PP&E. Organisations estimate the average PML resulting from stolen or destroyed information assets averages \$1,168 million. The average value of the largest loss that could result from damage or destruction of PP&E averages \$987 million. Business disruption has a slightly greater impact on information assets (\$288 million) than on PP&E (\$215 million).

Organisations value PP&E higher than information assets. The average total value of PP&E is approximately \$1,474 million for the organisations represented in this research. The average total value of information assets is lower at \$1,168 million.

The likelihood of a loss to information assets totalling 100 percent has increased from 3.2 percent in 2024 to 5.1 percent in 2026. Organisations estimate the likelihood that they will sustain a loss relating to information assets totalling no more than 50 percent of PML over the next 12 months at 5 percent and 100 percent of PML at 5.1 percent. The likelihood of a loss relating to PP&E totalling no more than 50 percent of PML over the next 12 months is an average of 2.1 percent and at 100 percent of PML it is 0.66 percent.

Twenty-eight percent of respondents believe it is not necessary to disclose a material loss to information assets not covered by insurance. In contrast, only 13 percent of respondents say no disclosure is necessary for a material loss to PP&E assets not covered by insurance. Thirty-nine percent of respondents say their organisation would disclose a material loss to information assets not covered by insurance in the footnotes of its financial statements and 38 percent of respondents say their organisation would disclose a material loss to PPE in the footnotes.

Twenty-six percent of respondents say their organisations would disclose a material loss to PP&E as a contingent liability on the balance sheet (FASB 5). Fifteen percent of respondents say a loss of information assets would be reported as a contingent liability.

There is a significant difference between insurance and self-insured coverage of PP&E and information assets. On average, approximately 53 percent of PP&E assets are covered by insurance and only 36 percent of PP&E assets are self-insured. In contrast, 59 percent of information assets are self-insured. Only 19 percent of the potential loss to information assets are covered by insurance.

Cyber Risk Exposure Continues to Increase

Most organisations believe their cyber risk is increasing. Sixty-nine percent of respondents believe their organisation’s exposure to cyber risk will increase and 18 percent of respondents say it will stay the same. Only 13 percent of respondents expect it to decrease.

In 2026, more organisations had at least one material or significantly disruptive security exploit or data breach in past two years. In 2026, 59 percent of respondents say their organisations had a material or significantly disruptive security exploit or data breach one or more times in the past two years, an increase from 54 percent in 2024. The average total financial impact of these incidents in 2026 was \$4.5 million, a decrease from \$5.6 million in 2024.

Seventy-two percent of these respondents say the incident increased their organisation’s concerns over cyber liability and 69 percent of respondents in 2024 said their worries increased. Only 12 percent of respondents are less concerned.

Sixty-six percent of respondents say responsibility for cyber risk management mostly resides with the CISO (35 percent) and the CIO (31 percent).

Data breaches and security exploits caused by negligence or mistakes and system or business process failures increase significantly. Fifty-nine percent of respondents say their organisation had a data breach or security incident. Seventy-five percent of respondents say the breach or security exploit was caused by negligence or mistakes that resulted in the loss of business confidential information and 61 percent of respondents say it was caused by system or business process failures that caused disruption to business failures such as software updates.

More organisations are becoming aware of the economic and legal consequences from an international data breach or security exploit. Fifty-two percent of respondents are fully aware, and 34 percent of respondents are aware or somewhat aware of the consequences that could result from a data breach or security exploit in other countries in which their organisation operates. Only 14 percent of respondents say they are not aware of the consequences.

Informal internal assessments to determine the level of cyber risk have significantly increased from 18 percent in 2024 to 26 percent in 2026. Twenty-nine percent of respondents say they use third parties to assess cyber risk. Only 13 percent of respondents say the level of cyber risk was based on intuition or gut feel.

The likelihood of a PML event involving information assets is highest for an AI/cyber IT disruption at a supply chain provider (41 percent of respondents). The most severe event to information assets is caused by a Software as a Service (SaaS) provider interruption (40 percent of respondents).

Most organisations are postponing the purchase of a standalone cyber insurance policy. Only 29 percent of respondents plan to purchase standalone cyber insurance in the next 12 months. Forty-six percent plan to purchase cyber insurance in the next 24 months (21 percent of respondents) or in more than 24 months (25 percent of respondents).

Twenty-five percent of respondents say their organisation has no plan to purchase standalone cyber insurance. The main reasons are coverage is inadequate based on their exposure (49 percent of respondents), premiums are too expensive (42 percent of respondents) and property and casualty policies are sufficient (35 percent of respondents).

Forty-five percent of respondents say that an external, cyber, IP or AI-related incident can become a “Black Swan”. A Black Swan is an event that is an “outlier” as it lies outside the realm of regular expectations. According to the research, 48 percent of respondents say preparation for a Black Swan event is part of the enterprise risk management approach.

The Use of Cyber Insurance to Mitigate the Financial Consequences of Data Breaches and Security Exploits

Since 2019 fewer organisations believe their cyber insurance coverage is sufficient. Despite the extent of cyber risk, only 33 percent of respondents say their organisations currently have cyber insurance coverage, including within a technology E&O, standalone cyber policy or similar policy not including Property, General Liability or Crime policy.

with an average limit of \$13 million. Only respondents in organisations with cyber insurance participated in this section of the research.

Fifty-four percent of these respondents believe their cyber insurance is sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security, a significant decline from 62 percent of respondents in 2019.

Cyber and IP risks rank in the top 5 of all business risks facing organisations. Fifty-five percent of respondents rank the risk to their organisation's intellectual property (IP) among the top 5 of all business risks (23 percent + 32 percent). Seventy percent of respondents consider cyber as the number 1 or 2 business risk (27 percent) or among the top 5 (43 percent).

Coverage for system or business failures and human error increases significantly. Seventy-five percent of respondents say their cyber insurance covers external attacks by cyber criminals, including ransomware and 69 percent of respondents say it covers malicious or criminal insiders. More respondents say cyber insurance covers system or business process failures (61 percent of respondents vs. 34 percent of respondents in 2024). Fifty-nine percent of respondents say it covers human error, mistakes and negligence, including AI, an increase from 31 percent of respondents in 2024.

The use of formal risk assessments by a third party to determine the adequacy of cyber insurance coverage increases from 21 percent of respondents in 2024 to 27 percent of respondents in 2026. The adequacy of cyber insurance coverage is determined mainly by a formal risk assessment by a third party (27 percent of respondents) or a formal risk assessment by in-house staff (21 percent of respondents).

Few cyber insurance policies cover ransomware payments and costs to recover from the attack. The top three reimbursements and services are forensics and investigative costs, replacement of lost or damaged equipment and notification costs to data breach victims, (68 percent, 60 percent and 60 percent of respondents respectively). Only 36 percent of respondents say their insurance reimburses costs related to ransomware.

Access to cyber security forensic experts is still the number one service offered (76 percent of respondents). Another primary service provided by the insurer are access to legal and regulatory experts (69 percent of respondents). This is followed by assistance in the remediation of the incident and access to specialised technologies and tools.

The Vulnerability of IP Assets

The average total value of organisations IP assets such as trademarks, patents, copyrights, trade secrets and know-how is \$928 million and represents an average of 41 percent of total company's assets, an increase from \$638 million in 2024. In 2024, IP assets averaged 47 percent of total assets. Less than half of respondents (49 percent) say their enterprise risk management activities include risks to their IP.

Forty-seven percent of respondents say their organisation experienced a material IP event in the past 24 months. The IP asset most often involved in a material IP event in the past 24 months was a trade secret (39 percent of respondents) followed by copyright, trademark or service mark (30 percent of respondents). However, only 49 percent of respondents say their organisation's enterprise risk management activities include risks to IP such as trademarks and brand, patents, copyrights and trade secrets as well as liability risks relating to third-party IP.

Most organisations say their existing insurance policy

covers IP events. Only 34 percent of respondents say their existing policy does not cover IP events. Forty-one percent of respondents say it covers a challenge to their company's IP assets. Forty-nine percent of respondents report that their policy covers third-party infringement of their organisation's IP assets.

Most often IP security exploits involve the infringement of an organisation's rights. The IP material event can be best described as an infringement of the organisation's rights (49 percent of respondents), challenge to the organisation's rights (40 percent of respondents) or an allegation of an organisation's infringement of third-party rights (11 percent of respondents).

As a supplement to a cyber risk policy, few organisations have a trade secret theft insurance policy. Only 25 percent of respondents say they have a trade secret theft insurance policy and 41 percent of respondents have an intellectual property liability policy.

Fifty percent of respondents are very interested or interested in purchasing a trade secret insurance policy and 68 percent say their organisations would purchase an intellectual property liability policy.



2

Key Findings



Part 2. Key findings

This report features the EMEA findings. A total of 599 respondents participated in the 2026 research. The audited findings are presented in the Appendix of this report.

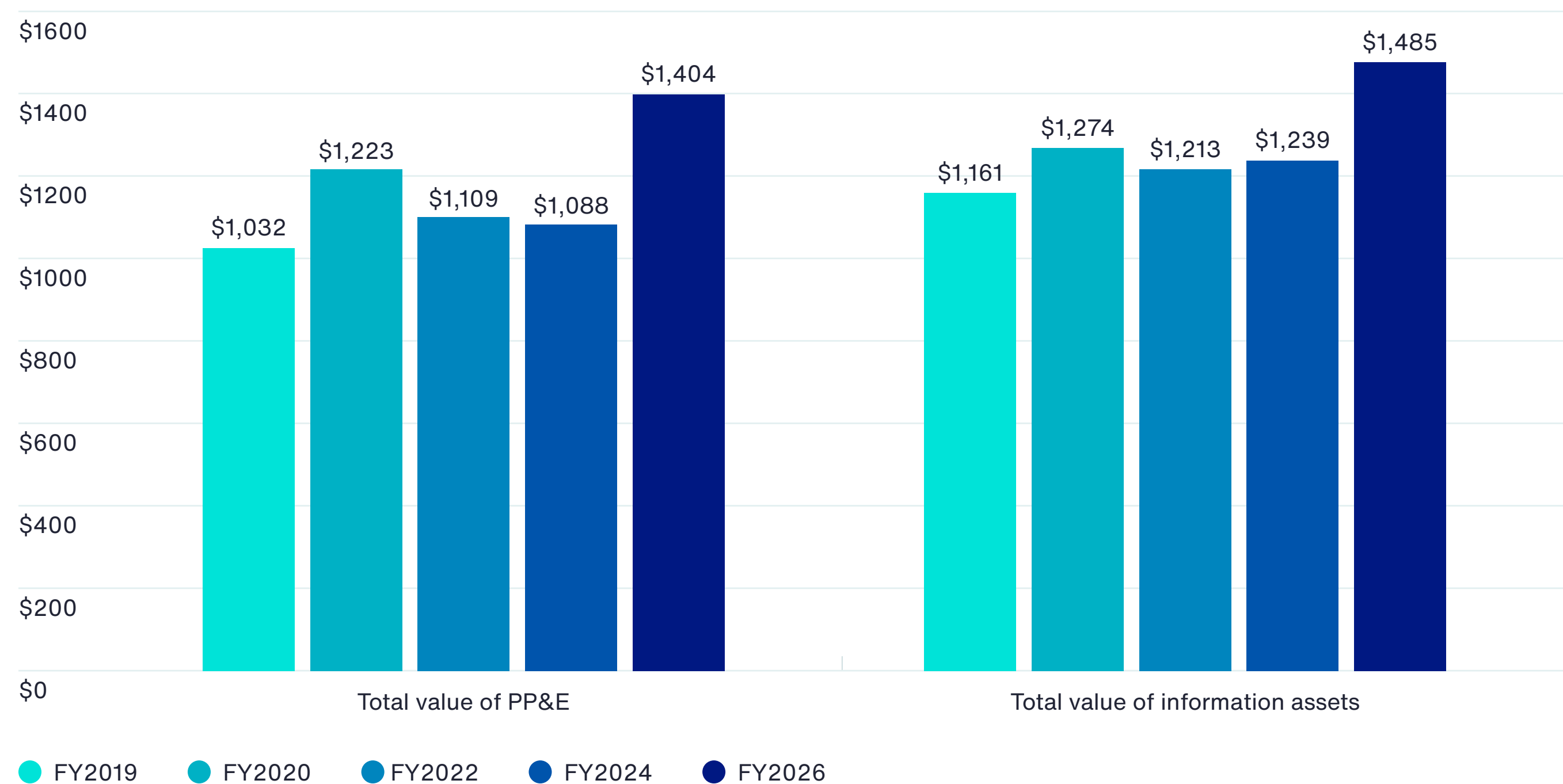
All respondents are familiar with the cyber risks facing their organisation. In the context of this research, cyber risk means any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems. We have organised the report according to the following topics:

- The Valuation of PP&E, Information Assets and Probable Maximum Loss (PML)
- Cyber Risk Exposures Increase
- The Use of Cyber Insurance to Mitigate the Financial Consequences of Data Breaches and Security Exploits
- The Vulnerability of IP Assets
- The Use of AI to Reduce Cyber Risks

The Valuation of PP&E, Information Assets and Probable Maximum Loss (PML)

Figure 1. The total value of PP&E and information assets

Extrapolated value (\$ millions)

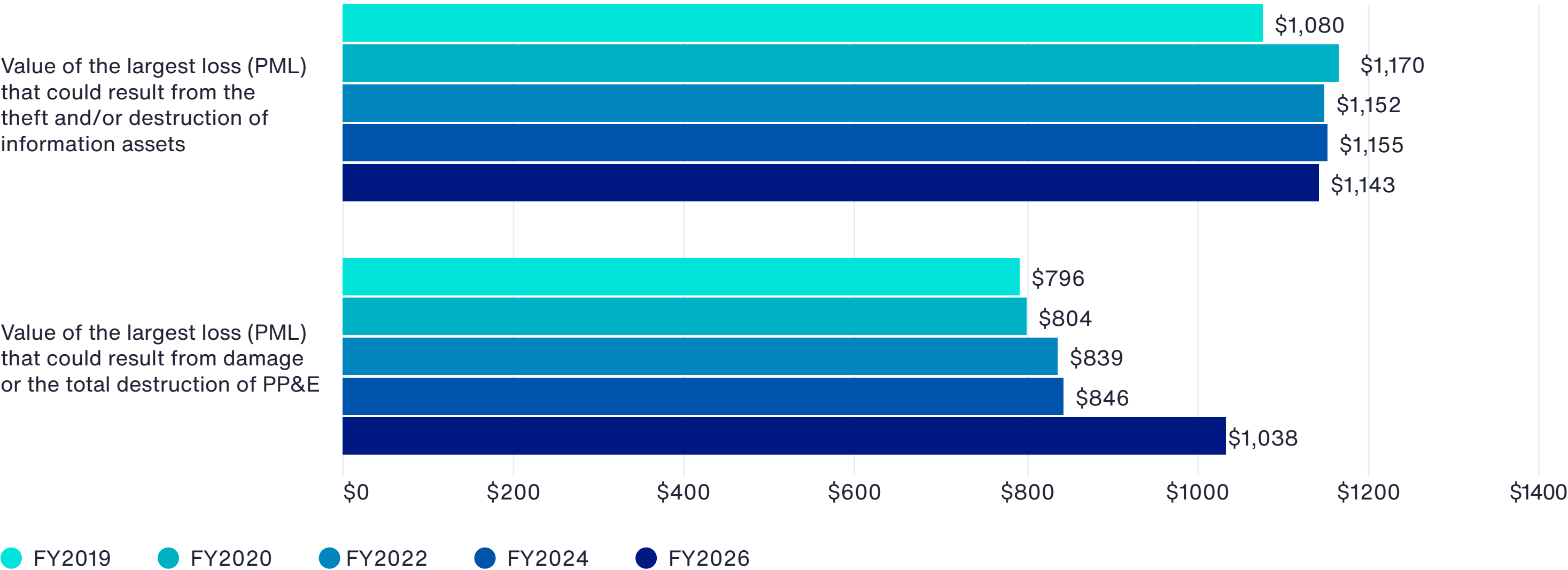


Organisations value information assets slightly higher than they do PP&E. According to Figure 1, on average, the total value of PP&E, including all fixed assets plus SCADA and industrial control systems averages \$1,474 million for the organisations represented in this research. The average total value of information assets, which includes customer records, employee records, financial reports, analytical data, source code, models, methods and other intellectual properties, is lower at \$1,168 million.

In contrast, the value of the largest loss that could result from damage or destruction of PP&E is, on average, approximately \$987 million. This also assumes the normal functioning of passive protective features such as firewalls, non-flammable materials, proper functioning of active suppression systems, fire sprinklers, raised flooring and more.

Figure 2. The PML value for PP&E and information assets Q9a,2a

Extrapolated value (\$ millions)



“

The United States has a disproportionate frequency and severity of litigation. The 2026 Ponemon/Aon Intangible Risks Report highlights that U.S. organisations must realign capital and insurance to where their true exposures now sit -- organisations can no longer treat physical and information assets as separate risk questions.

Christine Williams
Aon Co-Head of U.S.

Respondents were asked to rate the likelihood that their organisations would have a PML event involving information assets due to certain risks. According to Figure 3, AI/cyber-IT disruptions are more likely to occur (41 percent) than Software as a Service (SaaS) provider interruption (32 percent).

As shown in Figure 4, 40 percent of respondents say a SaaS interruption can be more severe than percent AI/ cyber IT disruptions (37 percent of respondents) and Power/Telco/Internet/Cloud infrastructure interruption (31 percent of respondents).

Figure 3. The likelihood of a PML event involving information assets due to certain security incidents Q10a,b,c

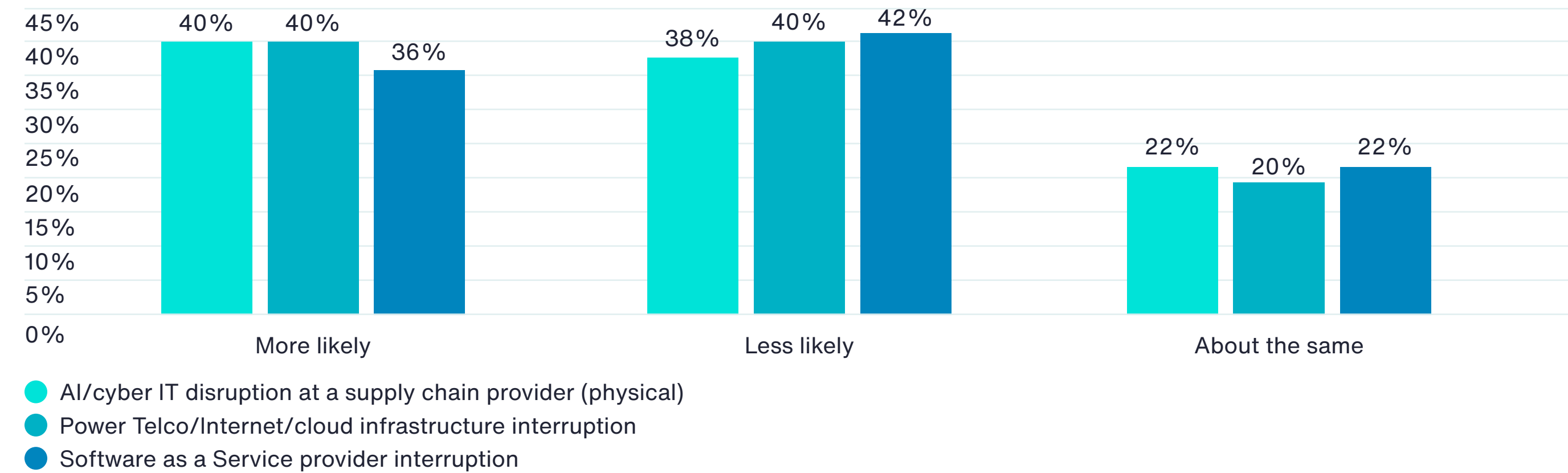
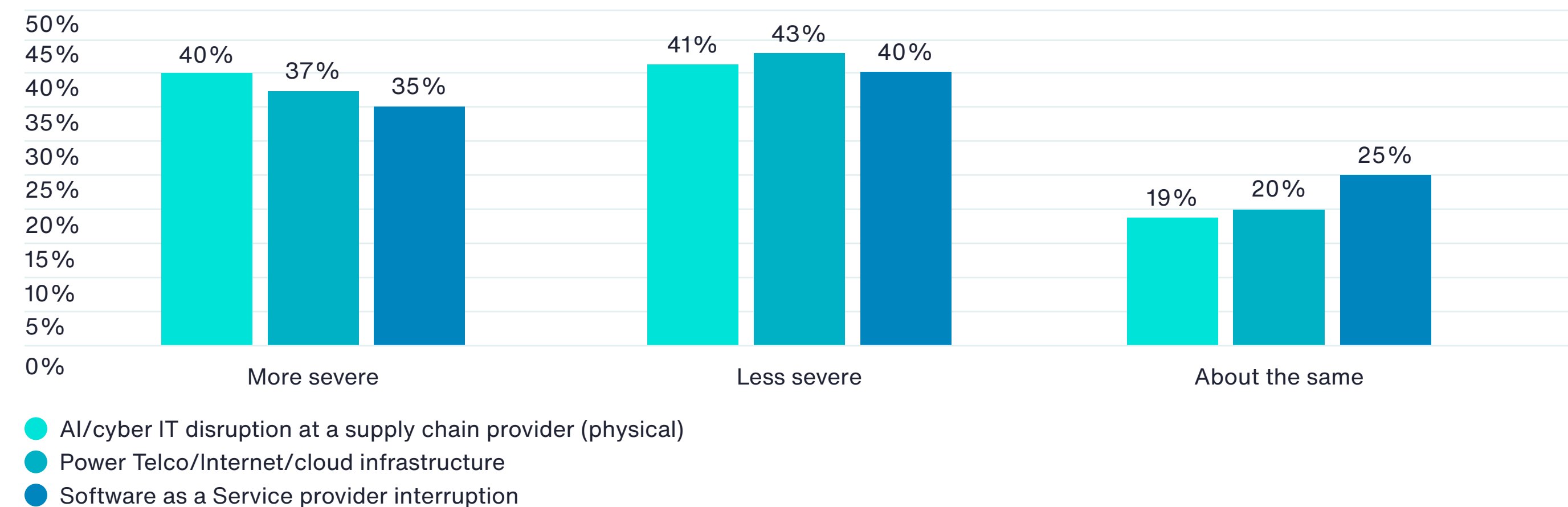
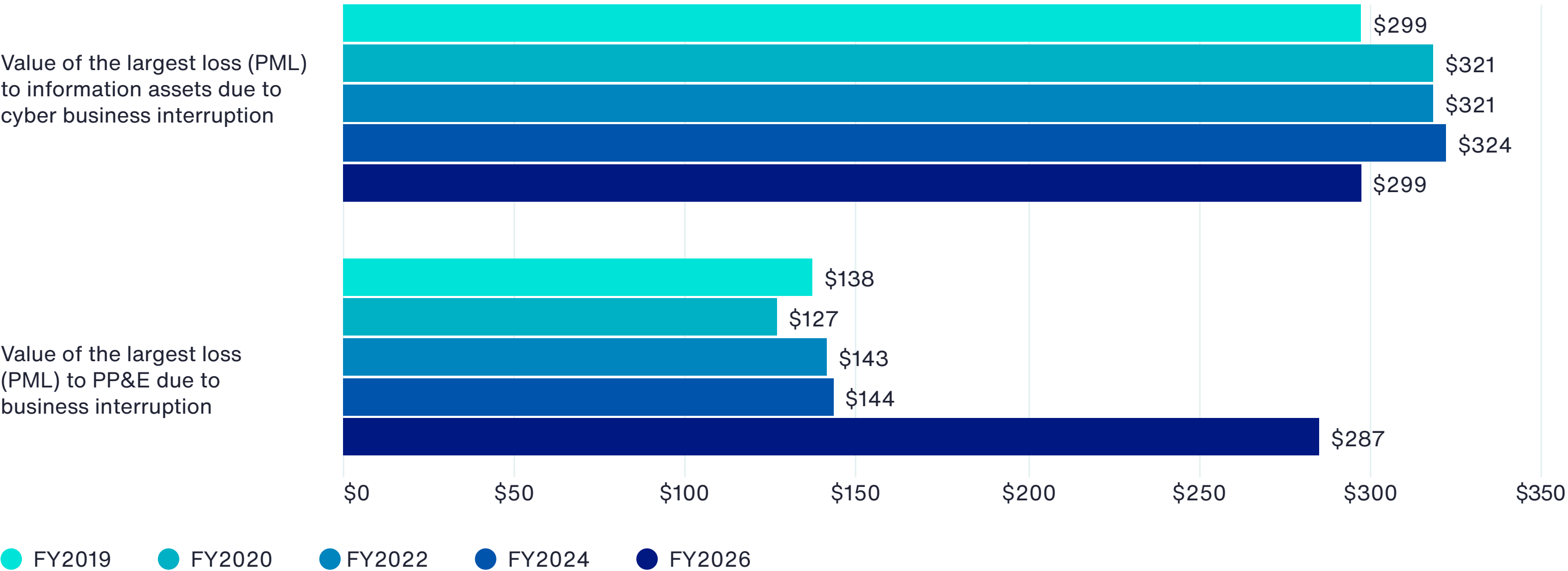


Figure 4. The severity of a PML event involving information assets Q11a,b,c



The loss to PP&E due to business interruption has increased significantly since 2024. . According to Figure 5, since 2024 the value of a PML of a PP&E due to business disruption has increased from \$171 million to \$215 million. The value of the largest loss to information assets due to business interruption averages \$288 million.

Figure 5. The value of the largest loss (PML) due to business and cyber disruption Q9b, 2b
Extrapolated value (\$ millions)



The likelihood of a loss to information assets totalling 100 percent has increased from 3.2 percent in 2024 to 5.1 percent in 2026. Organisations estimate the likelihood that they will sustain a loss relating to information assets totalling no more than 50 percent of PML over the next 12 months and 100 percent of PML at 5 and 5.1 percent, respectively as shown in Figure 6. The likelihood of a loss relating to PP&E totalling no more than 50 percent of PML over the next 12 months is an average of 2.1 percent and at 100 percent of PML it is 0.66 percent.



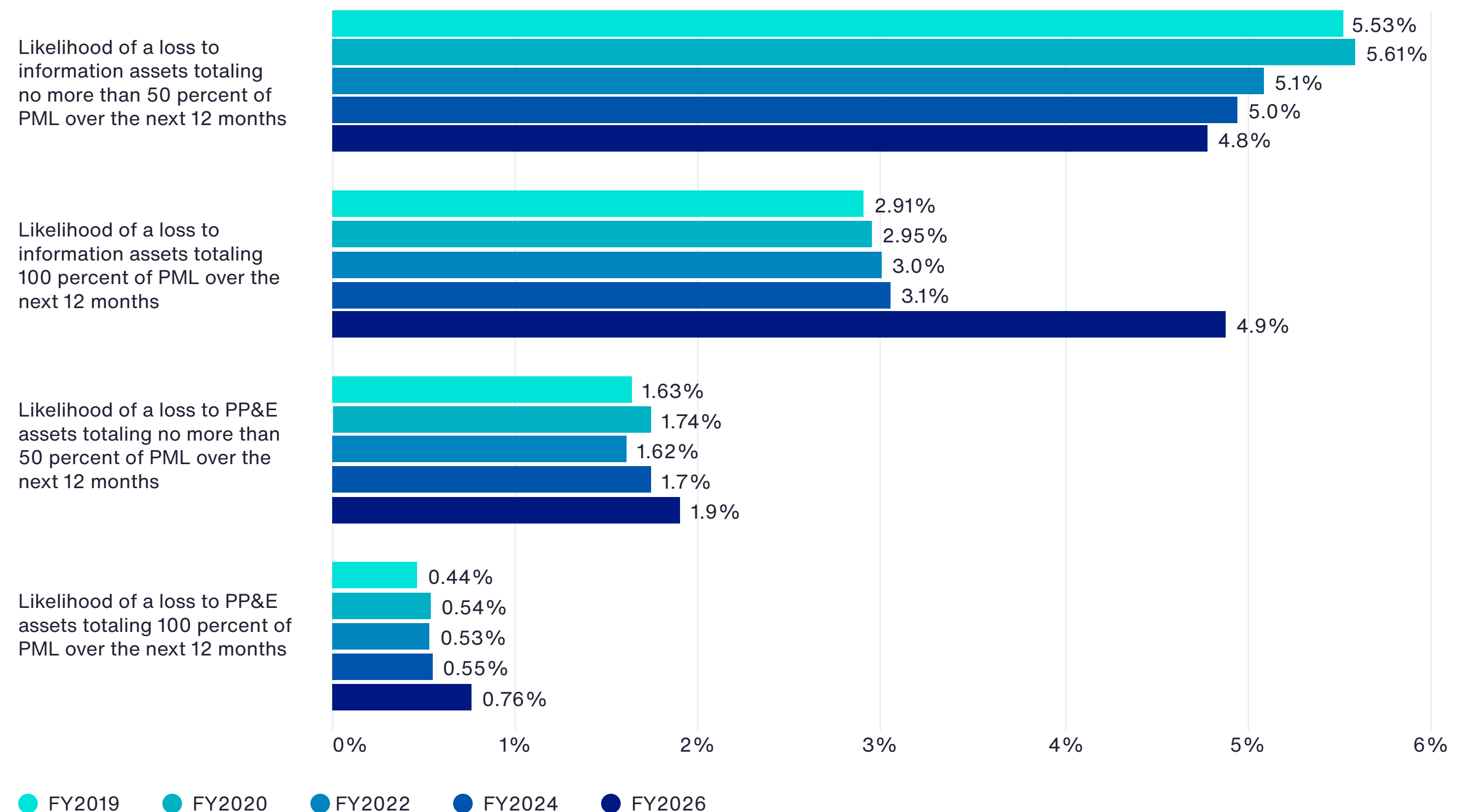
Artificial intelligence is accelerating investment in physical assets such as data centers and energy infrastructure. As a result, tangible risks are being concentrated and reshaped by intangible ones, not replaced. An effective AI strategy now depends on managing physical and digital risks as a single, integrated enterprise exposure.

Anne Corona

North America CEO, Aon

Figure 6. Likelihood of loss to PP&E and information assets totalling more than 50 percent and 100 percent of PML over the next 12 months Q12,13

Extrapolated percentage

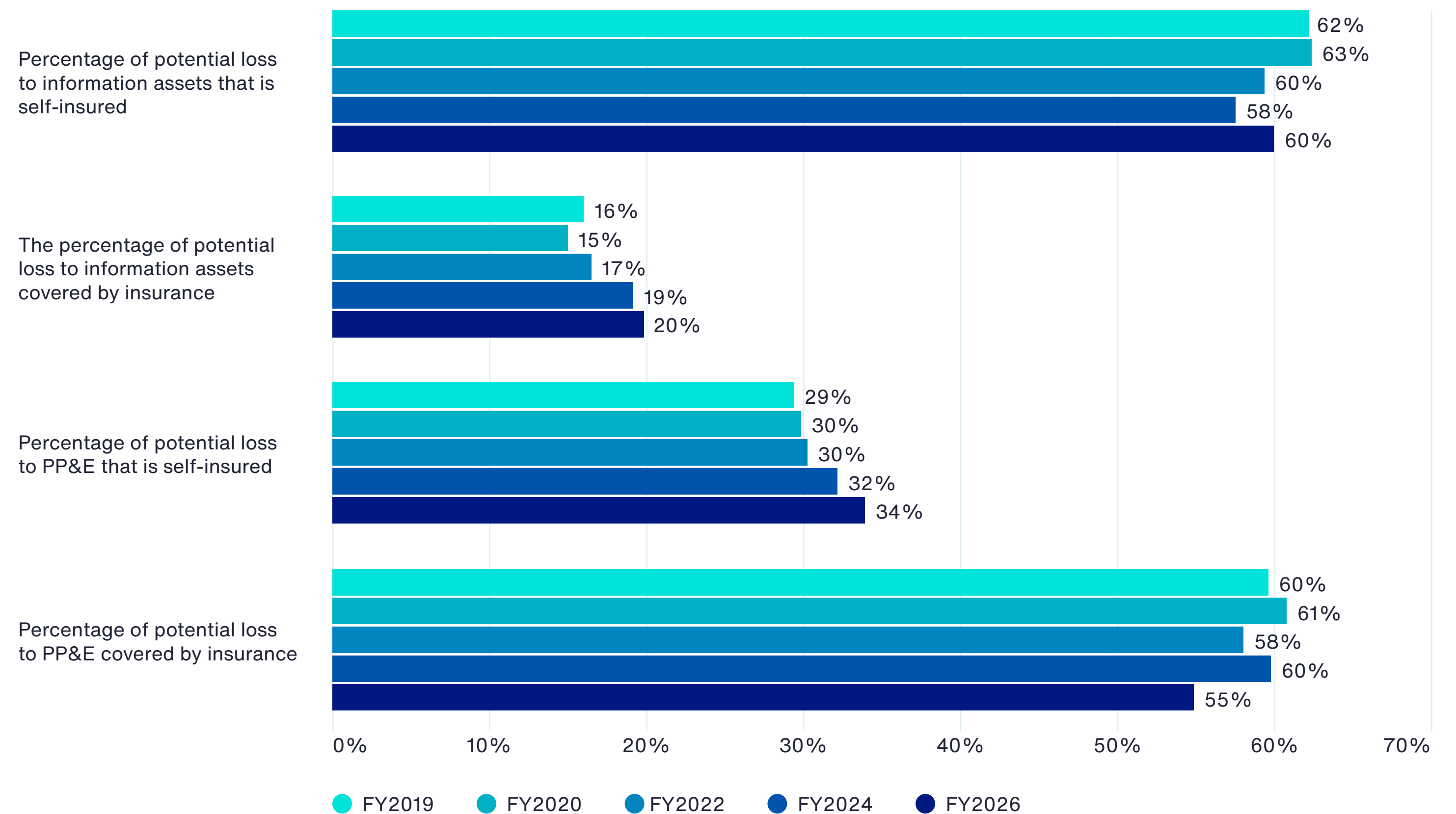


There is a significant difference between insurance coverage and self-insured coverage of PP&E and information assets. On average, approximately 53 percent of the potential loss to PP&E assets is covered by insurance, including captives reinsured but not including captives not reinsured. Only 36 percent of the potential loss to PP&E assets is self-insured, including captives not reinsured (Figure 7). A significant decrease from 60 percent of respondents in 2024.

In contrast, an average of 19 percent of the potential loss to information assets is covered by insurance, including captives reinsured but not including captives not reinsured and an average of 59 percent of the potential loss to information assets is self-insured, including captives not reinsured.

Figure 7. Percentage of PP&E: and information assets covered by insurance and self-insured Only Q3,4

Extrapolated percentage

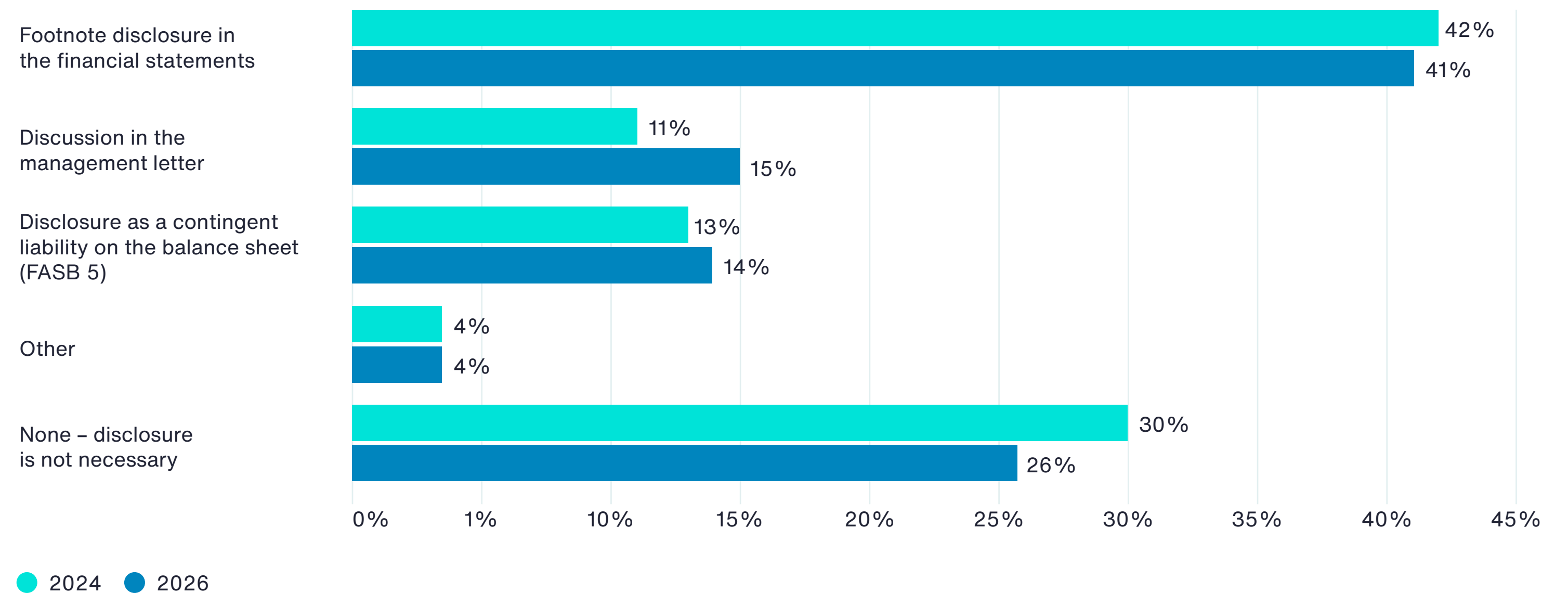


Twenty-eight percent of respondents believe it is not necessary to disclose a material loss to information assets not covered by insurance. In contrast, only 13 percent of respondents say no disclosure is necessary for a material loss to PP&E assets not covered by insurance.

Figure 8 focuses on how organisations would disclose a material loss. Thirty-eight percent of respondents say their organisation would disclose a material loss to PPE in the footnotes. Twenty-six percent of respondents say their organisations would disclose a material loss to PP&E as a contingent liability on the balance sheet (FASB 5).

Figure 8. How would your organisation disclose a material loss to PP&E and information assets not covered by insurance? Q7,14

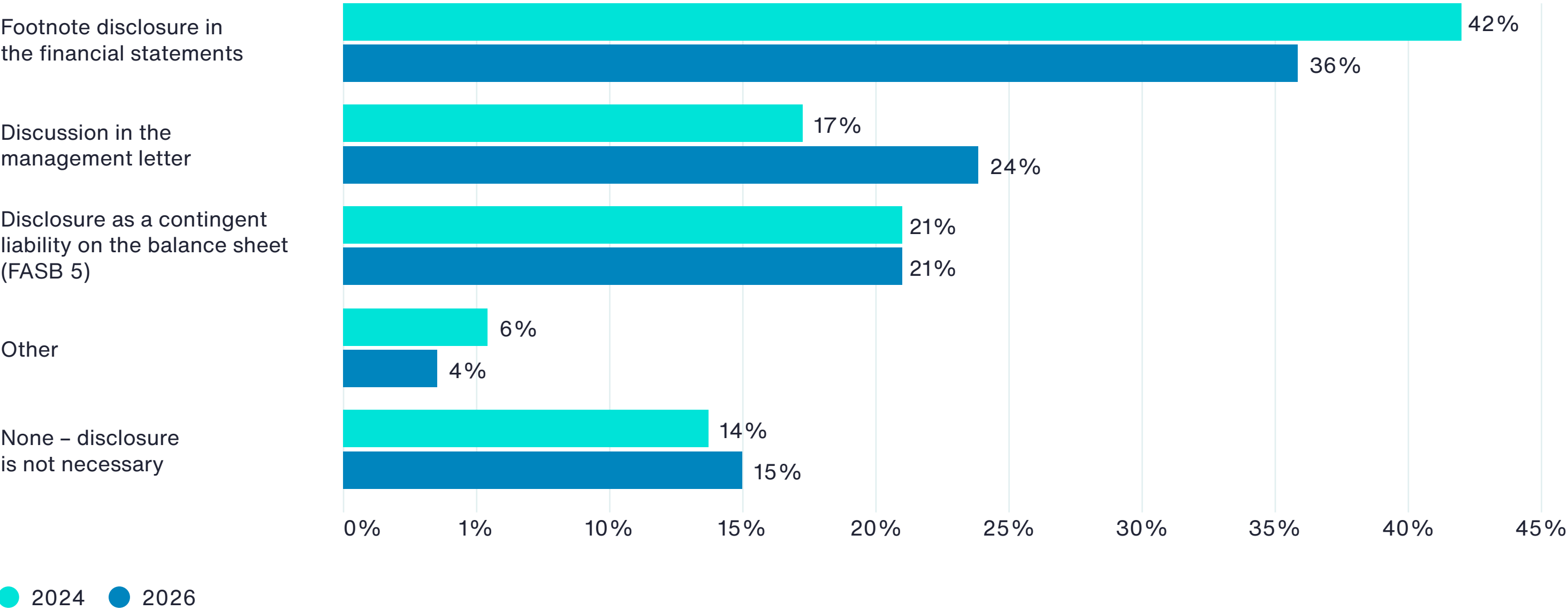
Methods to disclose a material loss to information assets not covered by insurance



Thirty-nine percent of respondents say their organisation would disclose a material loss to information assets not covered by insurance in the footnotes of its financial statements.

Fifteen percent of respondents say a loss of information assets would be reported as a contingent liability.

Methods to disclose a material loss to PP&E assets not covered by insurance



Cyber Risk Exposures Continue to Increase

Concerns about cyber incidents continue to increase.

Fifty-nine percent of respondents say their organisations had a material or significantly disruptive security exploit or data breach one or more times in the past 24 months. The average total financial impact of these incidents was \$4.5 million. In 2024, 54 percent of respondents said their organisation had a cyber incident and financial impact averaged \$5.6 million. According to Figure 9, 72 percent of these respondents say the incident increased their organisation's concerns over cyber liability.

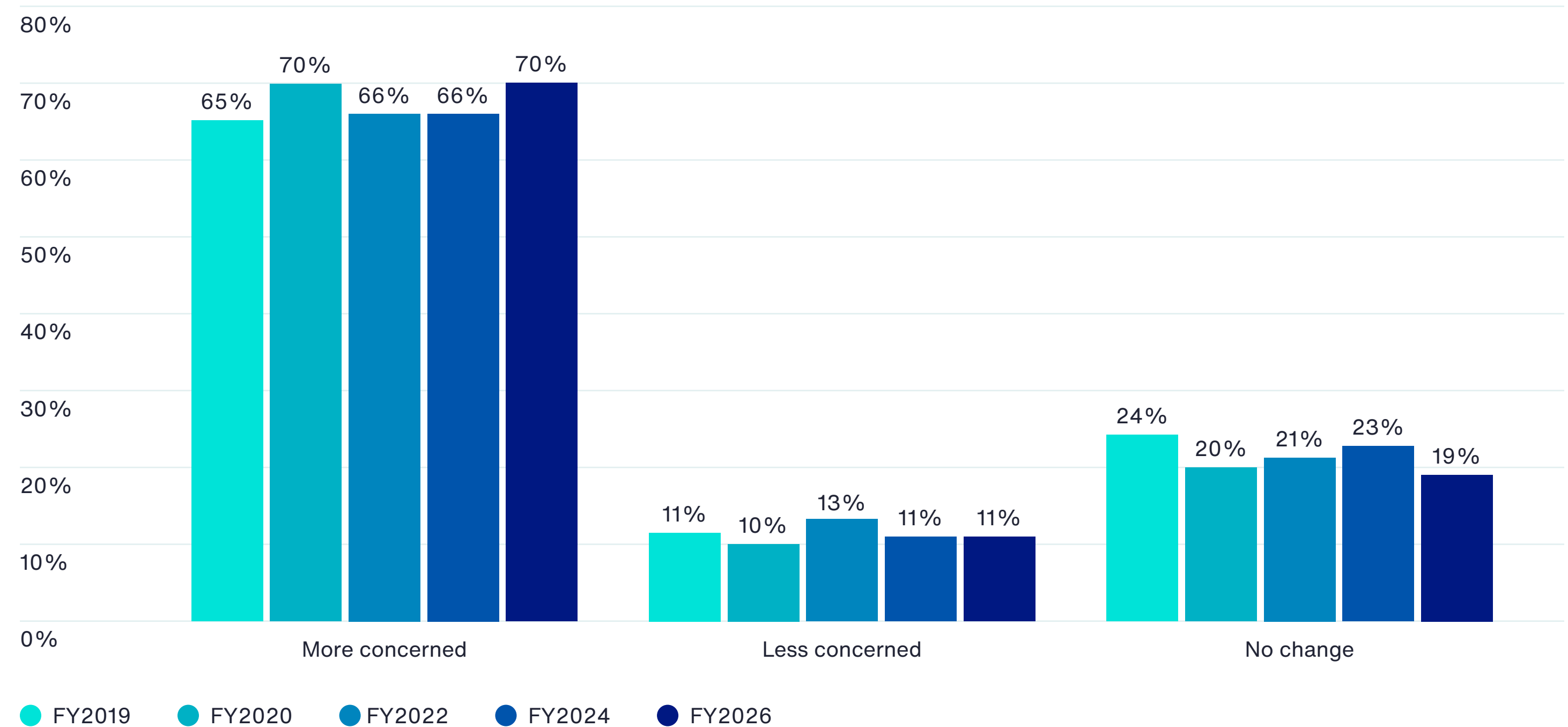
“

Artificial intelligence is growing in importance as both a threat, and a mitigation mechanism, with respect to cyber IT Security resilience — but nothing will ever completely replace the importance of human collaboration.

Ariel Weintraub

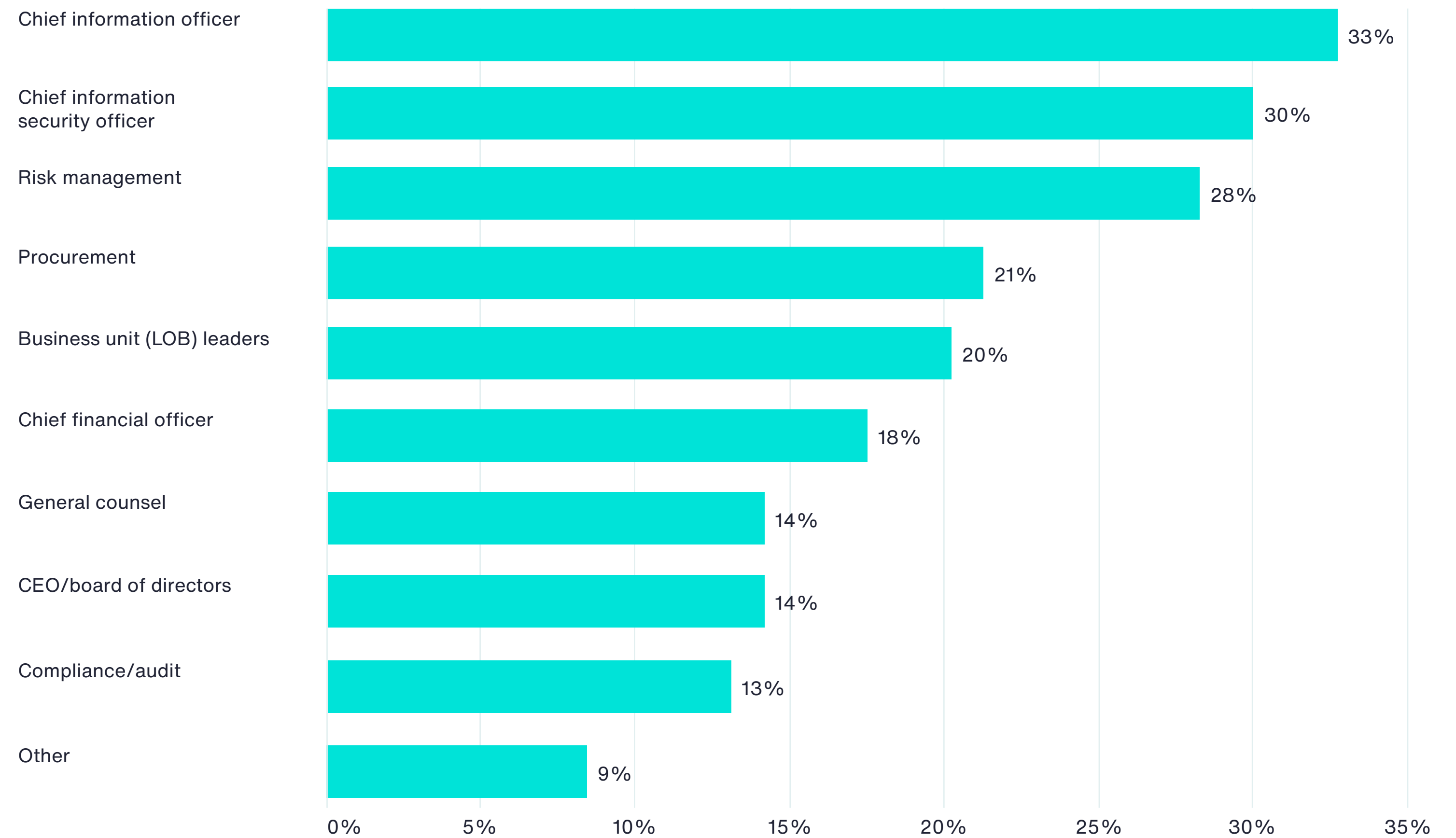
Chief Security Officer, Aon

Figure 9. How did the security exploit or data breach affect your organisation's concerns over cyber liability? Q16d



Sixty-six percent of respondents say responsibility for cyber risk management mostly resides with the CISO (35 percent), and the CIO (31 percent). As shown in Figure 10, 25 percent of respondents say risk management is responsible for cyber risk management.

Figure 10. Who is most responsible for cyber risk management? Q27

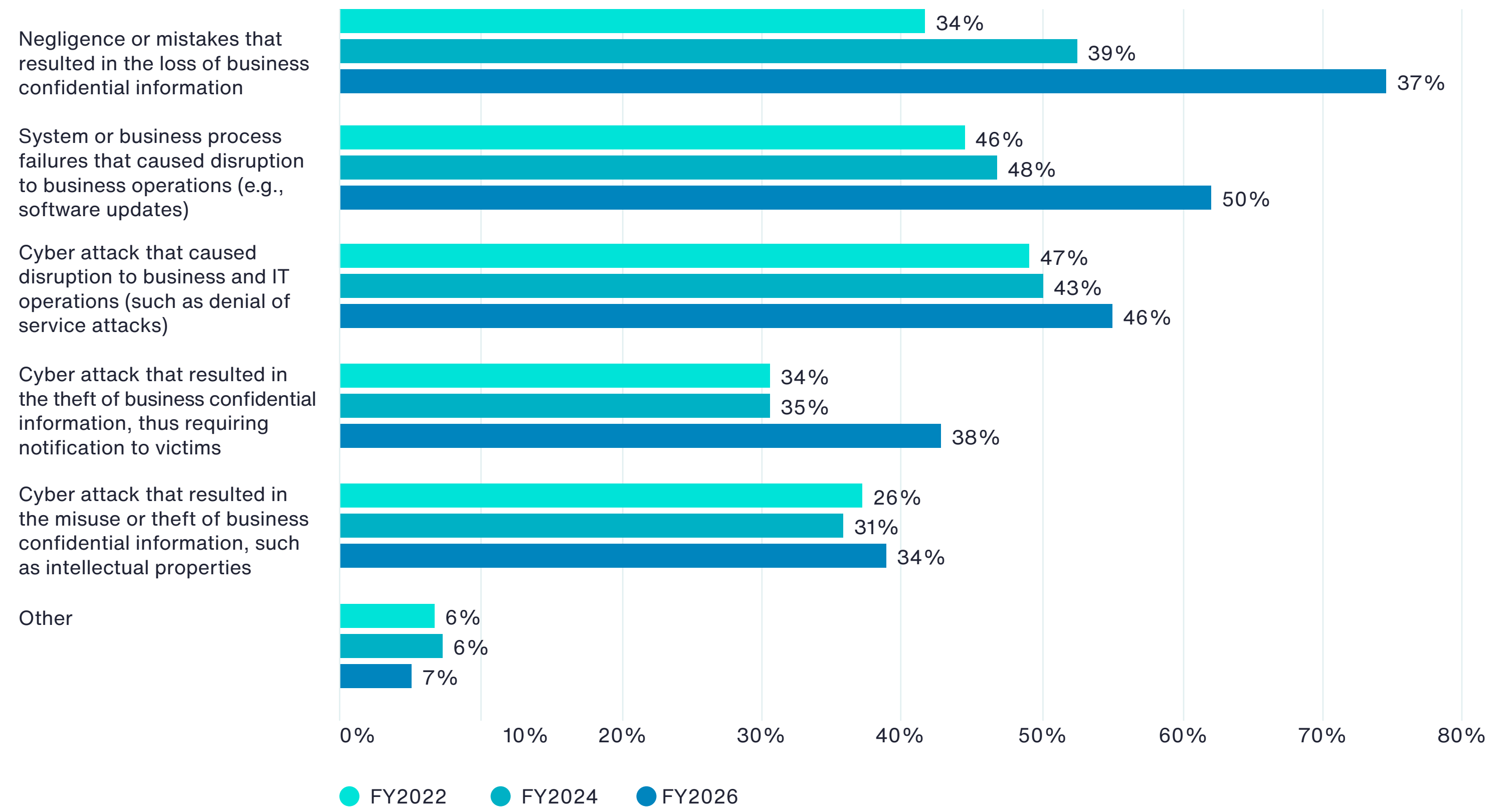


Data breaches and security exploits caused by negligence or mistakes and system or business process failures increase significantly. Figure 11 lists the security incidents that 59 percent of the organisations in this research experienced. The most frequent type of incident was one that was caused by negligence or mistakes that resulted in the loss of confidential business information (75 percent of respondents), a significant increase from 49 percent of respondents in 2024.

Sixty-one percent of respondents say a system or business process failure caused disruption to business operations, an increase from 44 percent of respondents in 2024. Fifty-three percent of respondents say it was a cyberattack that caused disruption to business and IT operations, such as denial-of-service attacks.

Figure 11. What type of data breach or security exploit did your organisation experience? Q16b

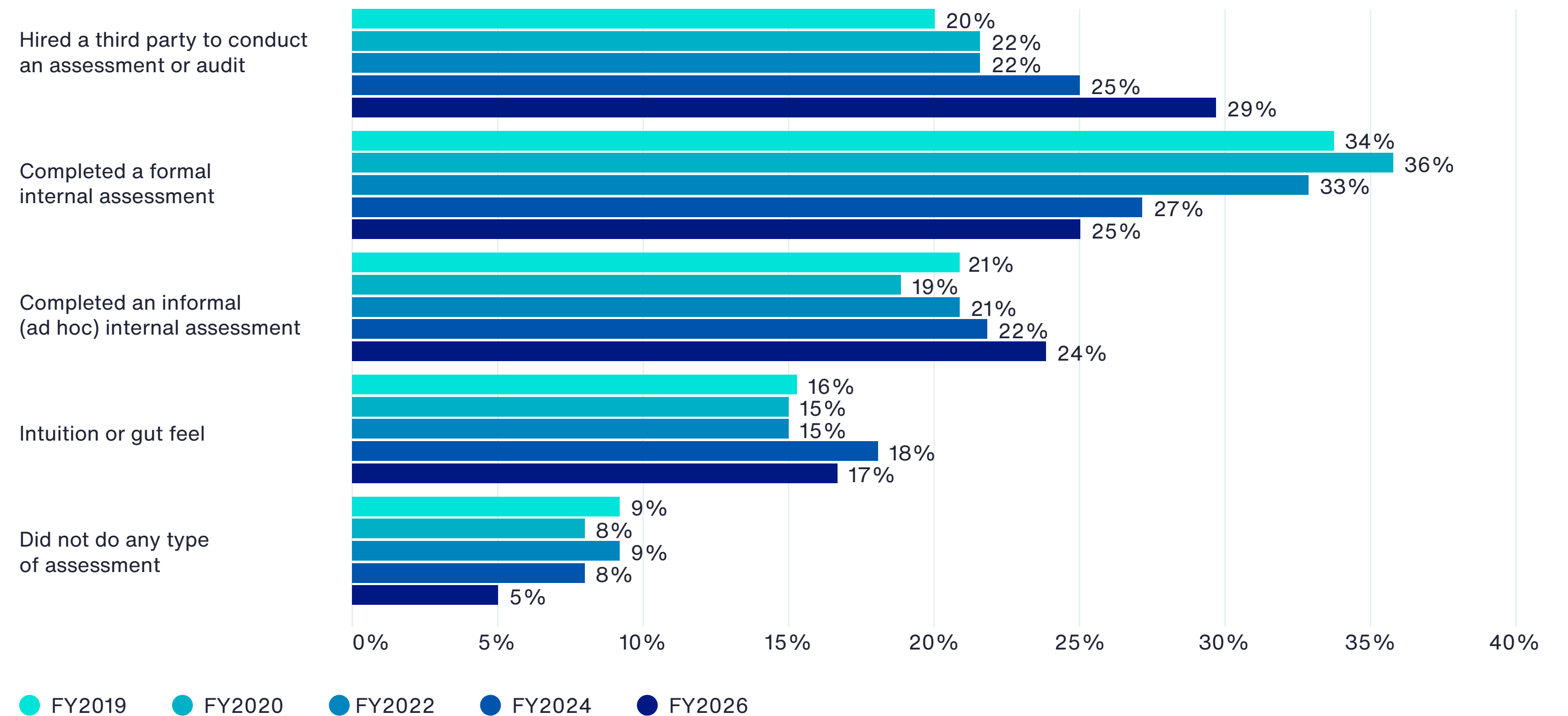
More than one response permitted



Informal internal assessments increase significantly and third-party audits decrease. According to Figure 12, to determine the cyber risk to their organisation, 26 percent of respondents say their organisations did an informal (ad hoc) internal assessment, an increase from 18 percent of respondents in 2024.

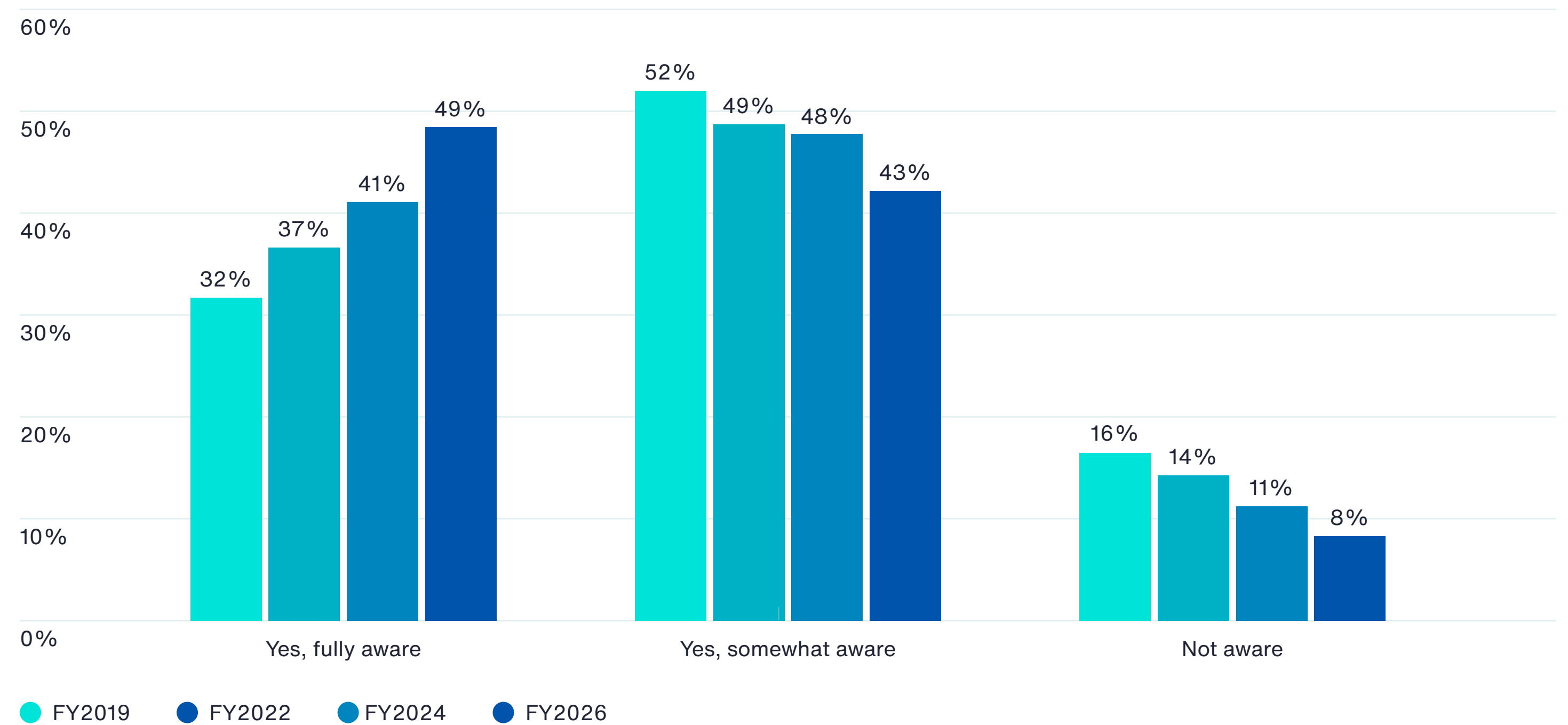
Twenty-nine percent of respondents say the organisation hired a third party to conduct an assessment or audit, a decrease from 35 percent of respondents in 2024. Twenty-eight percent of respondents say they conduct formal internal assessments. Only 13 percent of respondents say it was based on intuition or gut feel.

Figure 12. How did you determine the level of cyber risk to your organisation? Q19



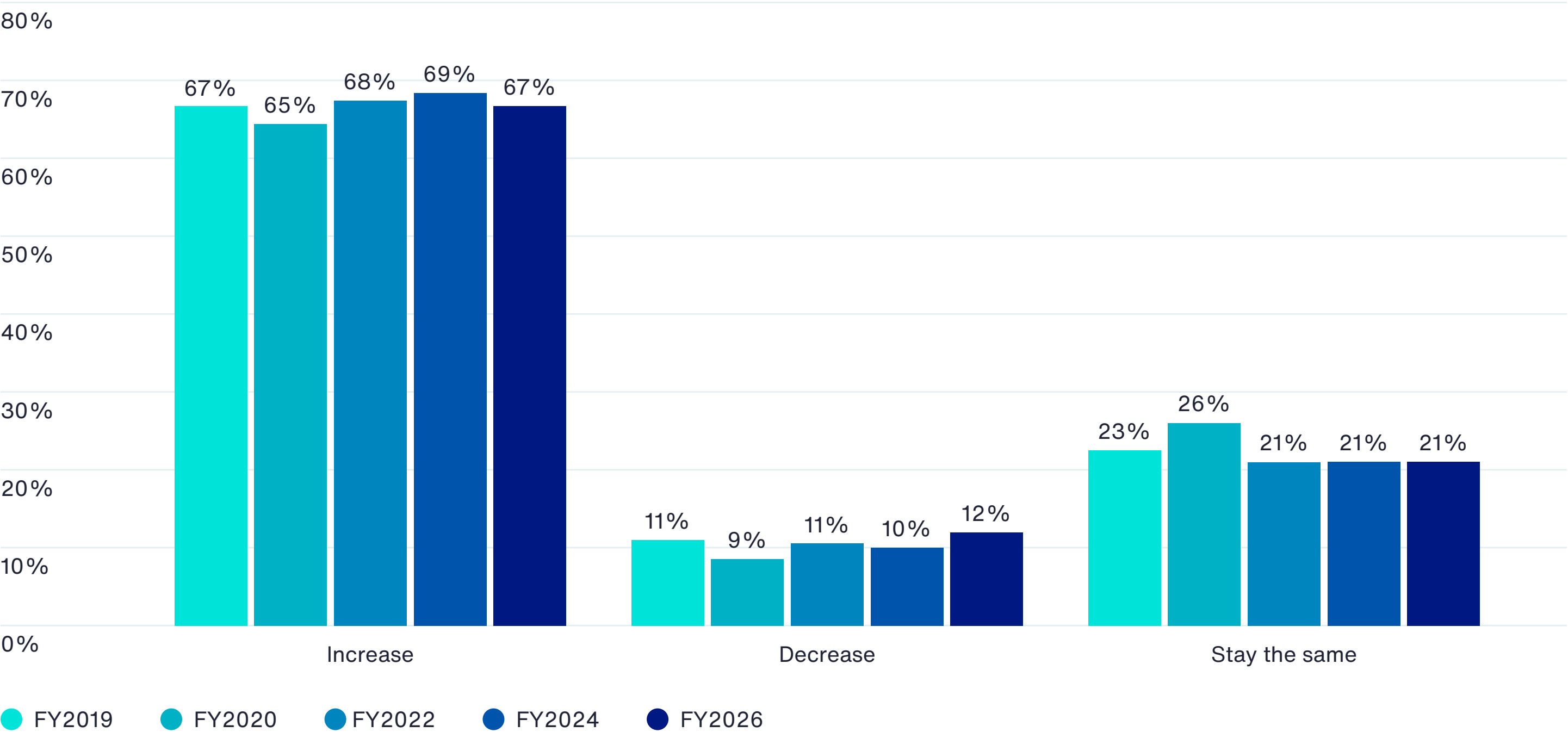
More organisations are becoming fully aware of the economic and legal consequences from an international data breach or security exploit. As revealed in Figure 13, 52 percent of respondents vs. 41 percent of respondents in 2024 are fully aware of the consequences that could result from a data breach or security exploit in other countries in which their organisation operates. Only somewhat aware decreased from 50 percent of respondents to 34 percent of respondents in 2026. Only 14 percent of respondents say they are not aware of the consequences.

Figure 13. Awareness of the economic and legal consequences from an international data breach or security exploit Q15



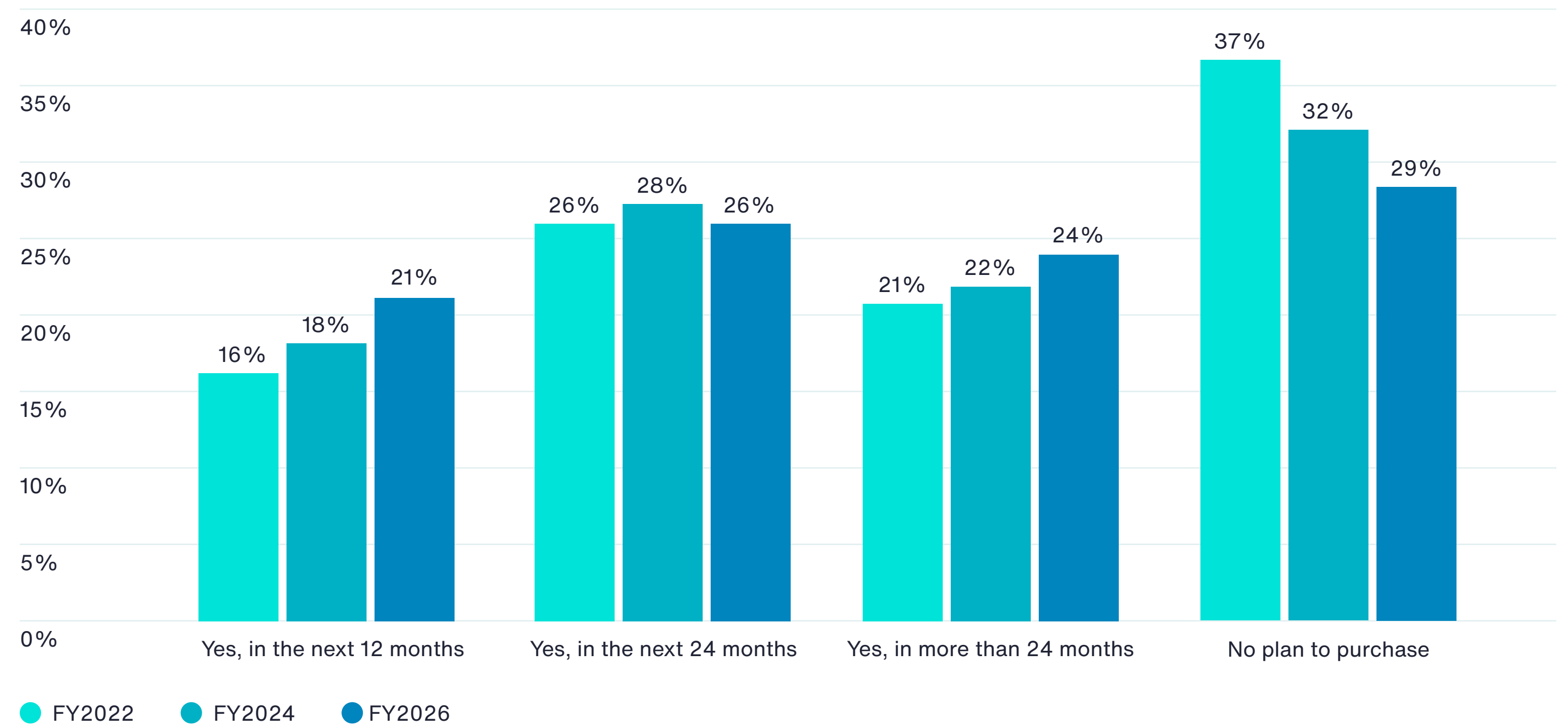
Most organisations believe their exposure to cyber risk is increasing. According to Figure 14, 69 percent of respondents believe their organisation’s exposure to cyber risk will increase and 18 percent of respondents say it will stay the same. Only 13 percent of respondents expect it to decrease.

Figure 14. Will your organisation’s cyber risk exposure increase, decrease or stay the same over the next 24 months? Q17



Fifty percent of respondents are postponing the purchase of a standalone cyber insurance policy for more than 24 months (25 percent) or have no plans to purchase (25 percent). The other 50 percent say they will purchase standalone cyber insurance in the next 12 months (29 percent) or in the next 24 months (21 percent), as shown in Figure 15.

Figure 15. Does your company plan to purchase standalone cyber insurance? Q26a

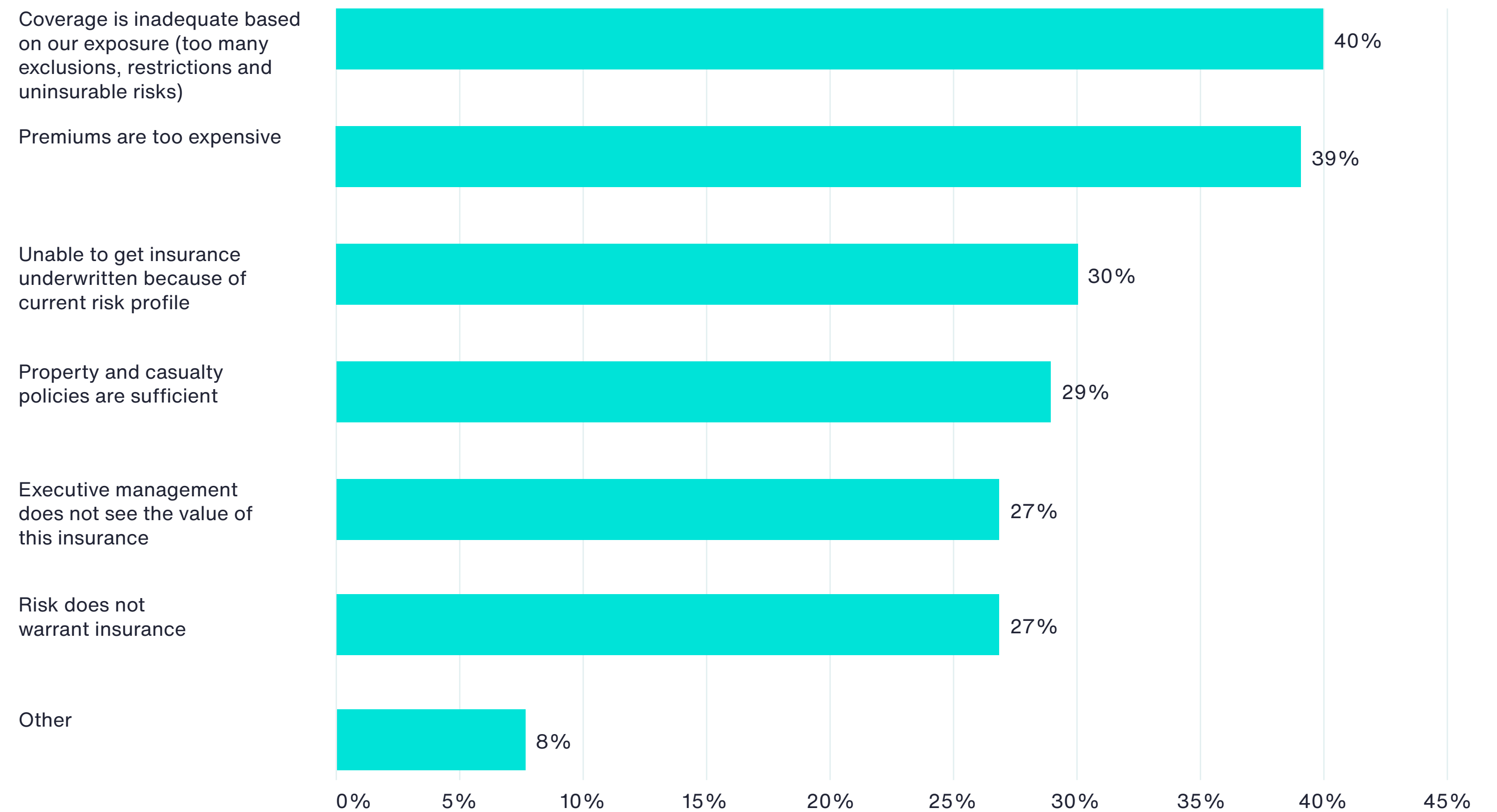


Inadequate coverage and cost are the main reasons for not purchasing standalone cyber security insurance.

According to Figure 16, more organisations are not purchasing a standalone cyber security insurance policy because coverage is inadequate based on their exposure (49 percent of respondents) or premiums are too expensive (42 percent of respondents).

Figure 16. What are the main reasons why your organisation will not purchase standalone cyber security insurance? Q26b

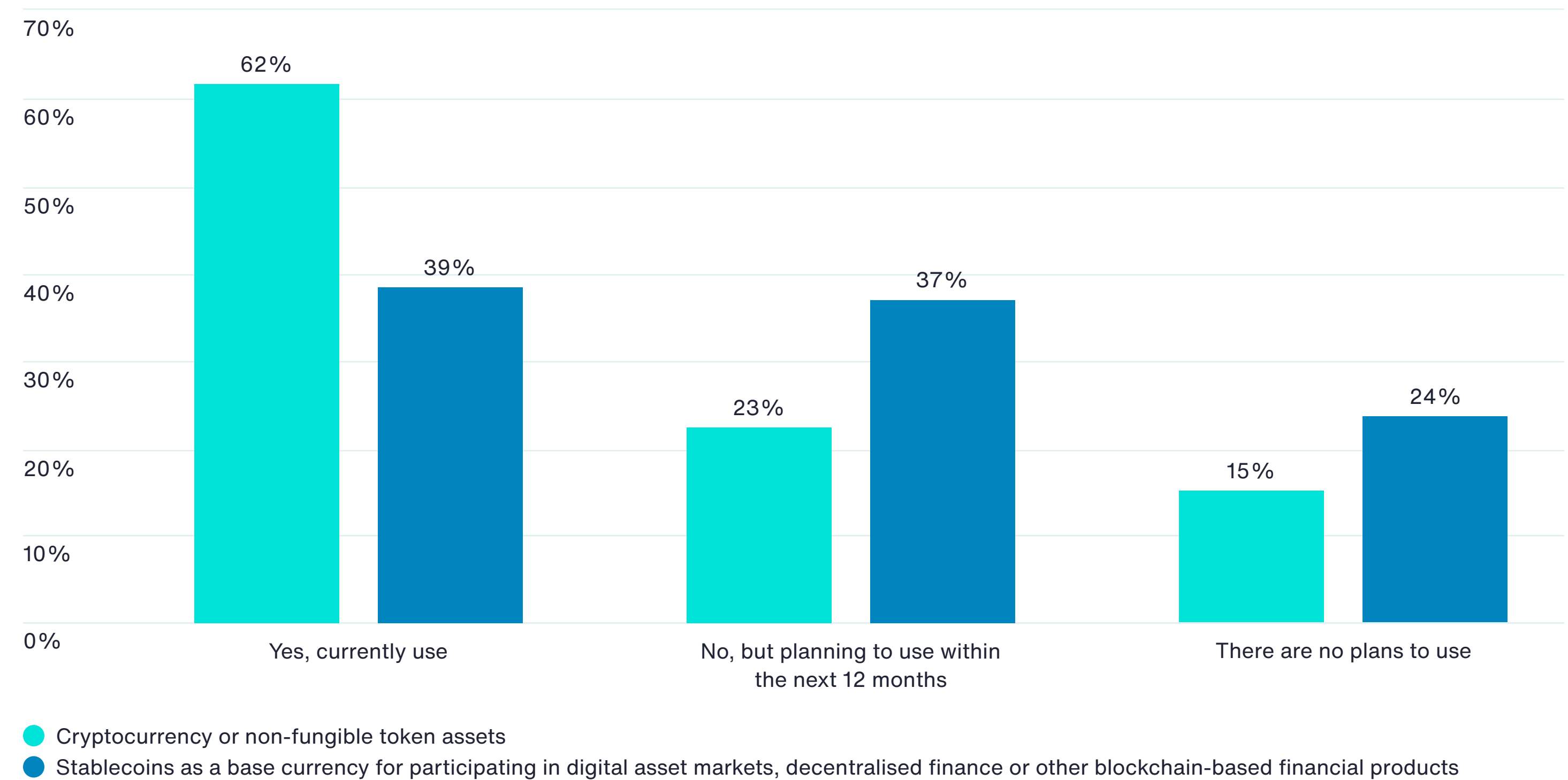
More than one response permitted



Cryptocurrency and non-fungible token assets are widely used. Eighty-nine percent of respondents say they currently use (60 percent) or plan to use cryptocurrency and non-fungible token assets in the next 12 months (29 percent).

Eighty percent of respondents currently use stablecoins as a base currency (34 percent) or plan to use within the next 12 months (46 percent). Stablecoins are cryptocurrencies designed to maintain a stable value, usually by being “pegged” to a stable asset like the U.S. dollar, gold, or other cryptocurrencies, acting as a bridge between volatile crypto markets and traditional finance. They achieve stability through reserves (fiat-backed, commodity-backed) or algorithms, offering a reliable medium for transactions, payments, and DeFi applications, reducing the price volatility seen in assets like Bitcoin.

Figure 17. Does your organisation use or plan to use cryptocurrency/non-fungible token assets and stablecoins as a base currency for participating in digital asset markets, decentralised finance or other blockchain-based financial products? Q28,29



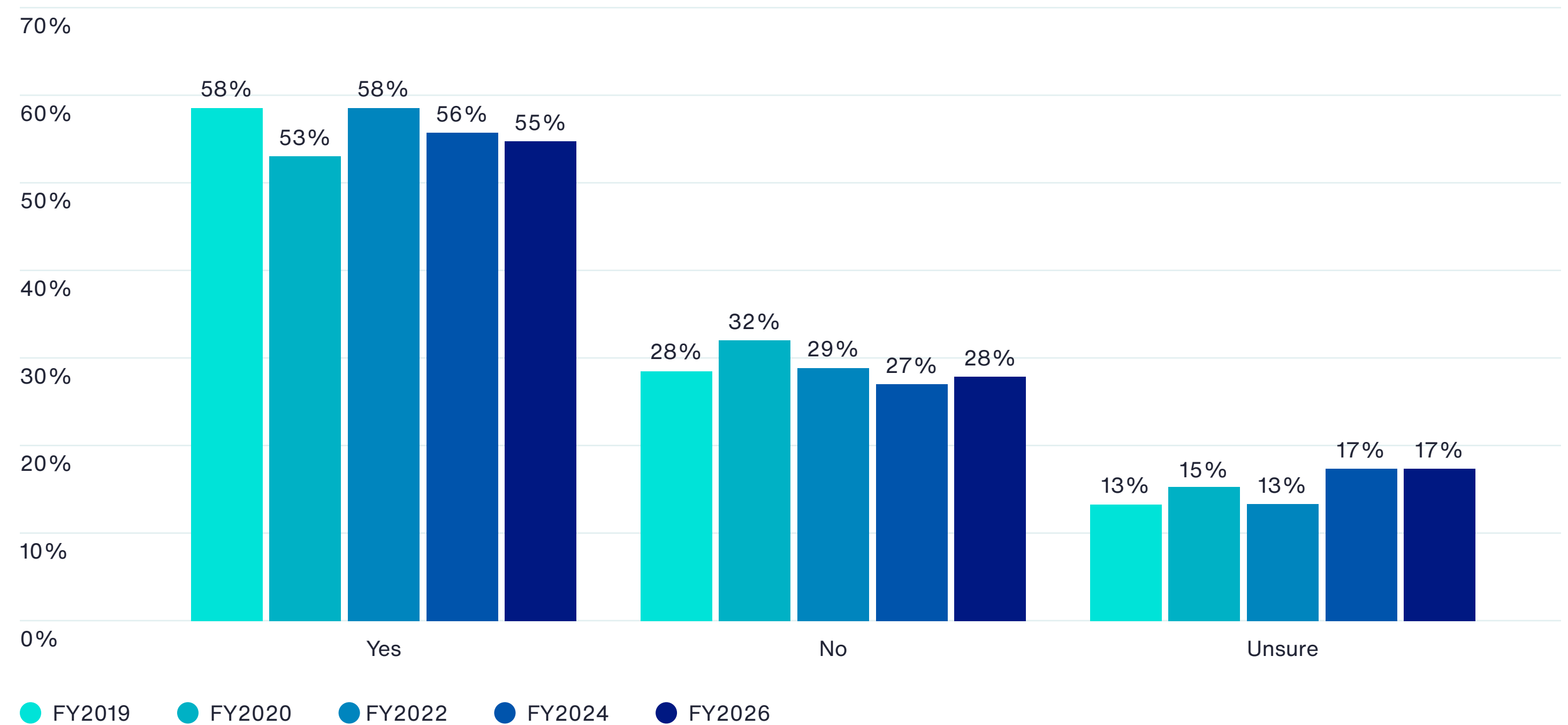
The Use of Cyber Insurance to Mitigate the Financial Consequences of Data Breaches and Security Exploits

Thirty-three percent of respondents say their organisations have cyber insurance coverage, including within a Technology Errors & Omission or similar policy not including Property, General Liability or Crime policy. Only respondents with these policies participated in this section of the research.

Since 2019 fewer organisations believe their cyber insurance coverage is sufficient. Despite the extent of cyber risk, only 33 percent of respondents say their organisations currently have cyber insurance coverage with an average limit of \$13 million.

As Figure 18 reveals, 54 percent of these respondents believe their cyber insurance is sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security, a significant decline from 62 percent in 2019.¹⁸

Figure 18. Is your organisation's cyber insurance coverage sufficient? Q21

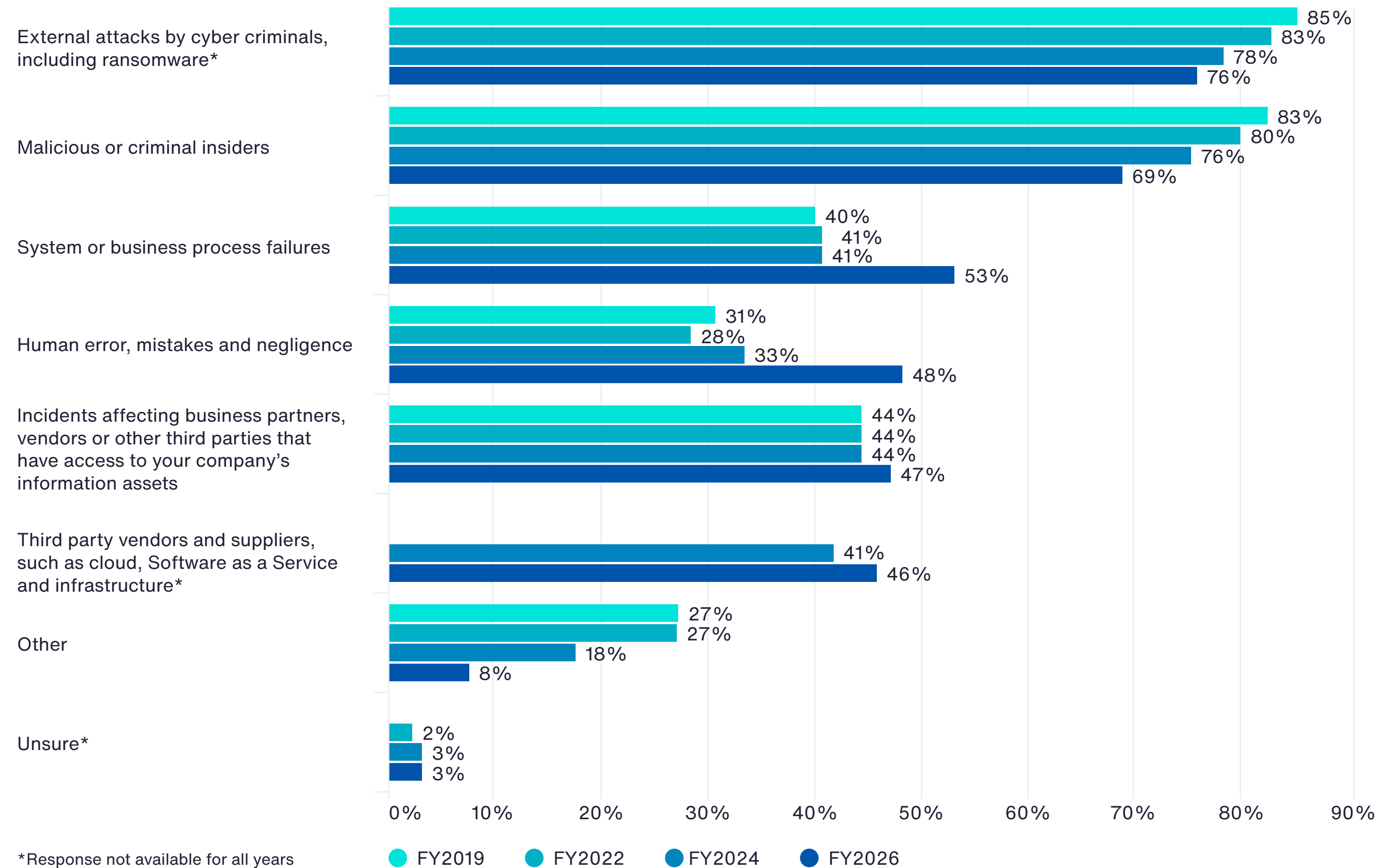


¹⁸ The Future of Insurance to Address Cyber Perils. Insurance Thought Leadership.
<http://insurancethoughtleadership.com/future-of-insurance-to-address-cyber-perils/>

Coverage for system or business failures and human error increases significantly. Figure 19 lists the types of incidents organisations' cyber insurance covers. As shown, 75 percent of respondents say it covers external attacks by cyber criminals, including ransomware and 69 percent of respondents say it covers malicious or criminal insiders. More respondents say cyber insurance covers system or business process failures (61 percent of respondents vs. 34 percent of respondents in 2024). Fifty-nine percent of respondents say it covers human error, mistakes and negligence, including AI, an increase from 31 percent of respondents in 2024.

Figure 19. What types of incidents does your organisation's cyber insurance cover? Q23

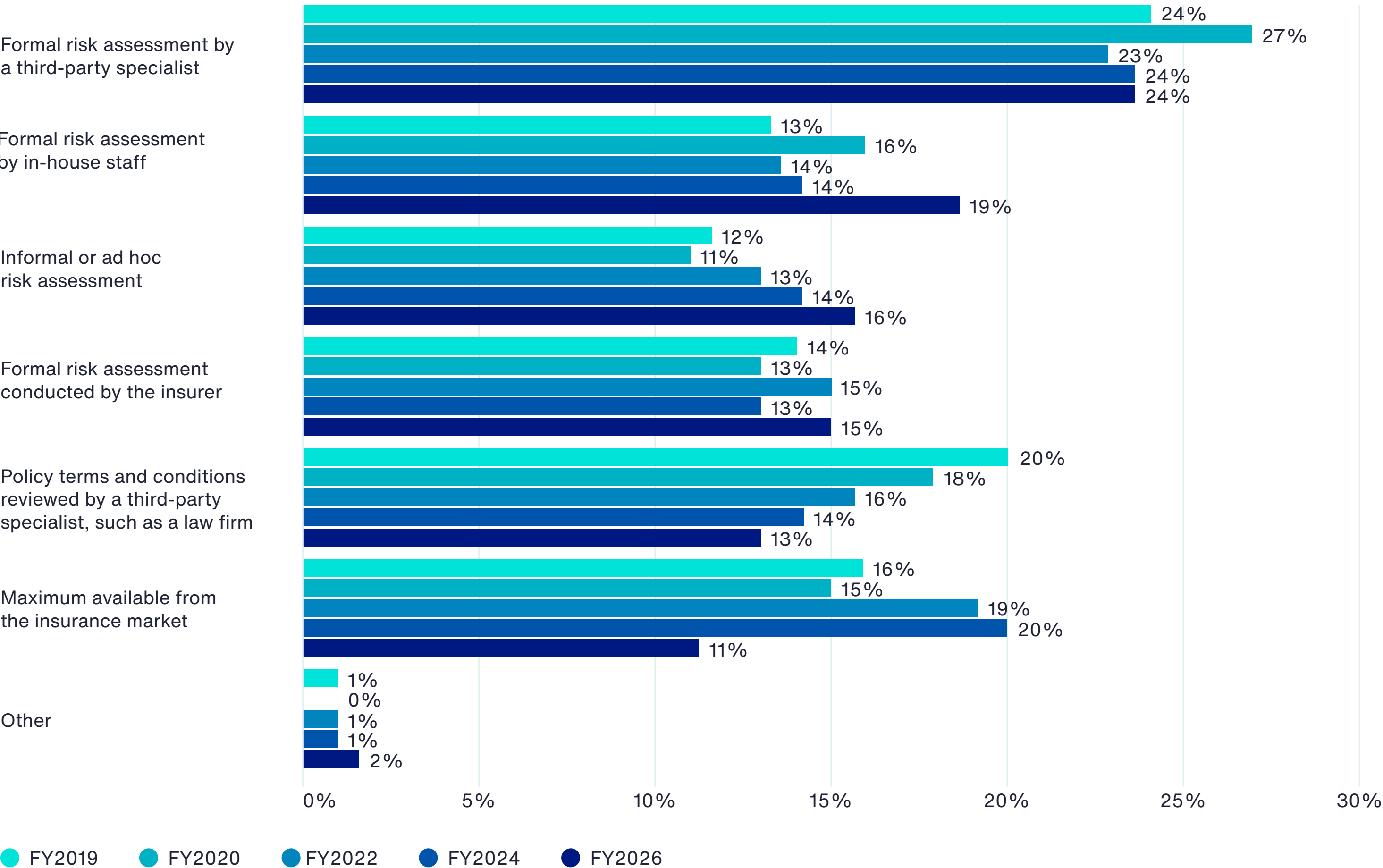
More than one response permitted



The use of formal risk assessments by a third party to determine the adequacy of cyber insurance coverage increases from 21 percent of respondents in 2024 to 27 percent of respondents in 2026. According to Figure 20, the adequacy of cyber insurance coverage is determined mainly by a formal risk assessment by a third party (27 percent of respondents) or a formal risk assessment by in-house staff (21 percent of respondents).

Figure 20. How organisations determine the adequacy of cyber insurance coverage Q22

Only one choice permitted

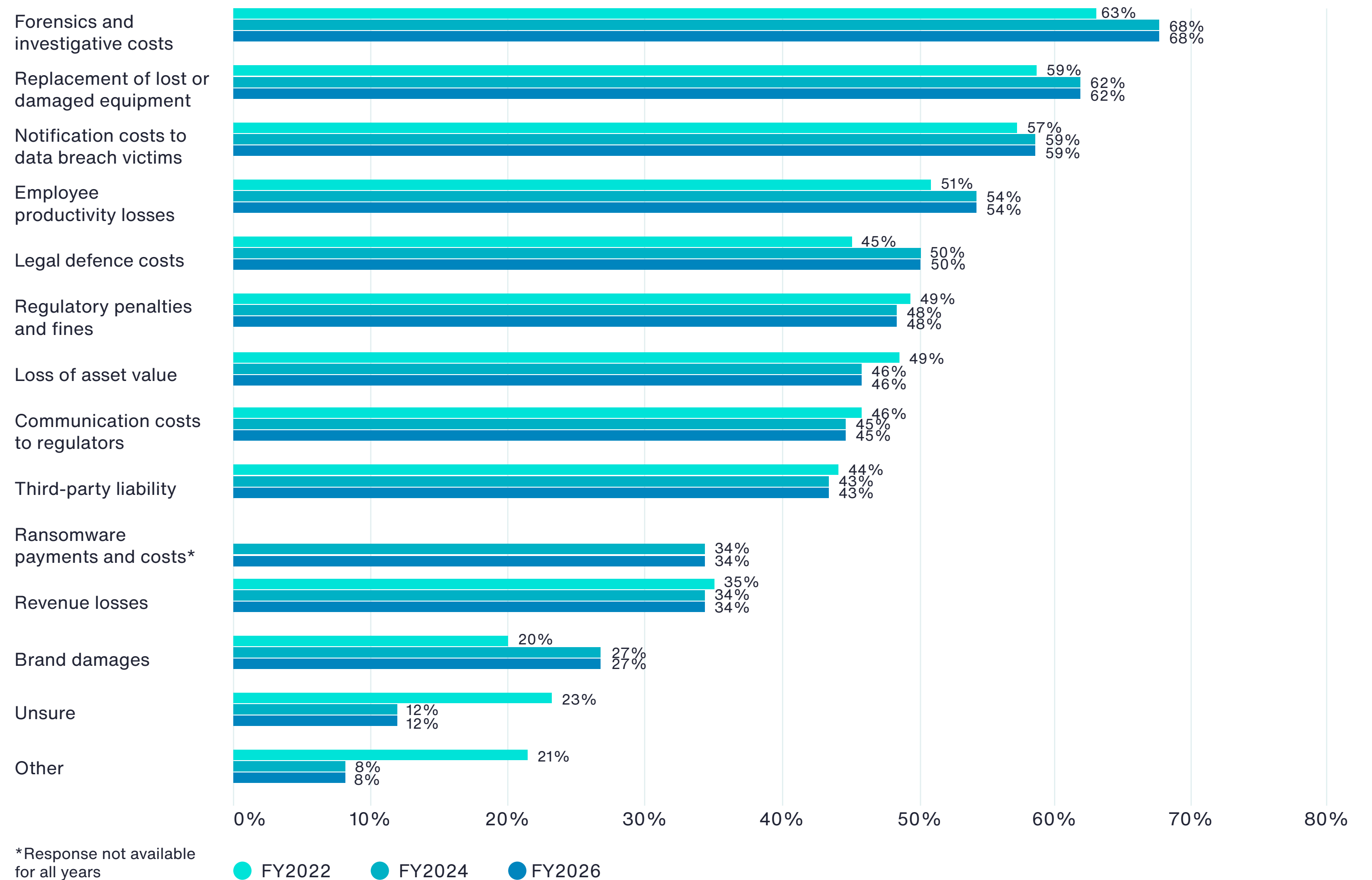


The top three reimbursements and services continue to be forensics and investigative costs, replacement of lost or damaged equipment and notification costs to data breach victims. Figure 21 lists the various reimbursements and services insurance organisations offer.

The top three are forensics and investigative costs, replacement of lost or damaged equipment and notification costs to data breach victims, 68 percent, 60 percent and 60 percent of respondents respectively. Only 36 percent of respondents say ransomware costs are covered. Reimbursements for loss of asset value have declined from 50 percent of respondents in 2022 to 39 percent of respondents in 2026.

Figure 21. The reimbursements and services from insurance providers? Q24

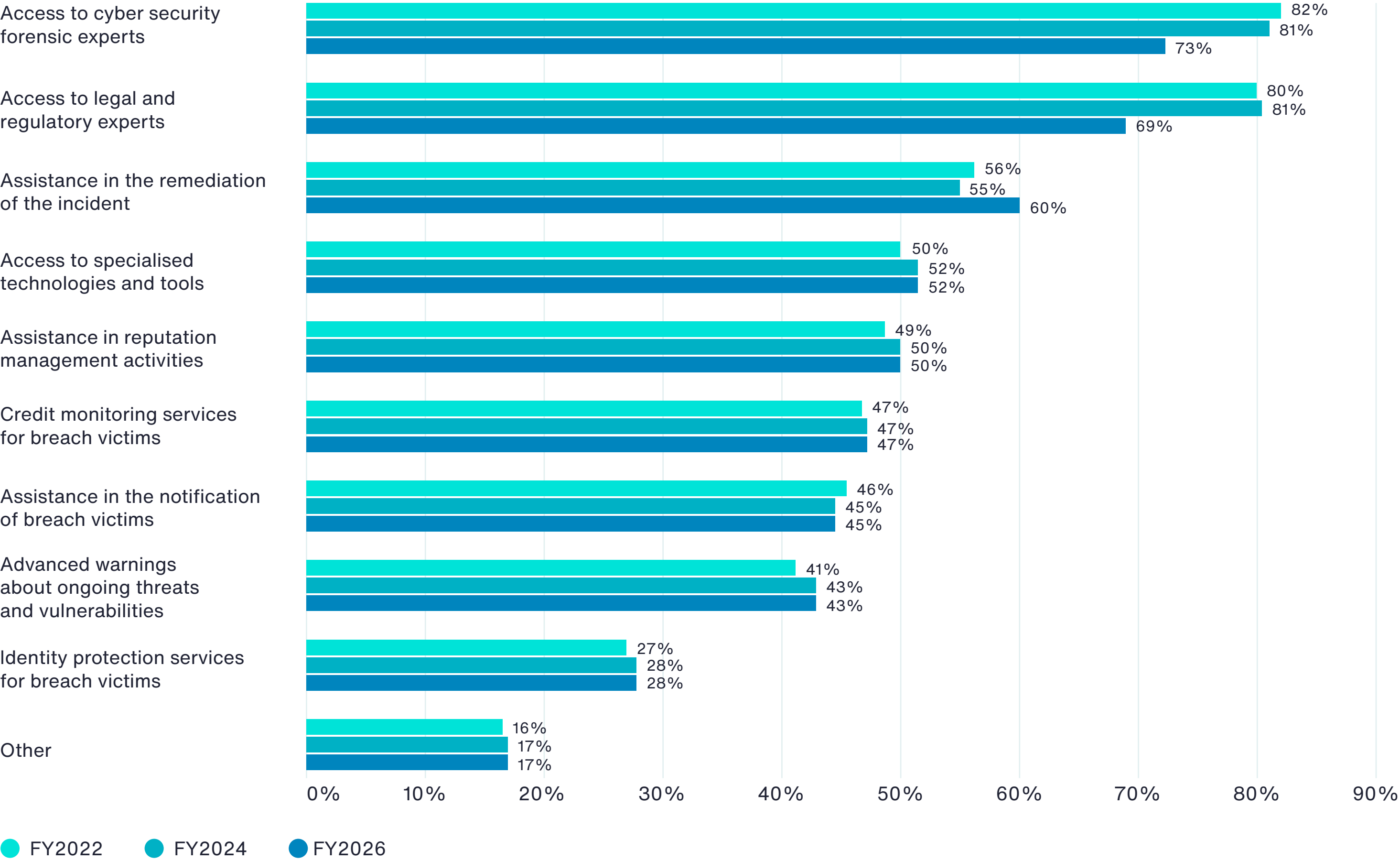
More than one response permitted



Access to cyber security forensic, legal and regulatory experts continues to be the services most often provided by cyber insurance policies. According to Figure 22, the primary services provided by the insurer are access to cyber security forensic experts and legal and regulatory experts (76 percent of respondents and 69 percent of respondents, respectively). This is followed by assistance in the remediation of the incident and access to specialised technologies and tools (both 53 percent of respondents). Only 19 percent of respondents say their organisations provide identity protection services for breach victims.

Figure 22. Other services included in cyber insurance policies Q25

More than one response permitted



The Vulnerability of IP Assets

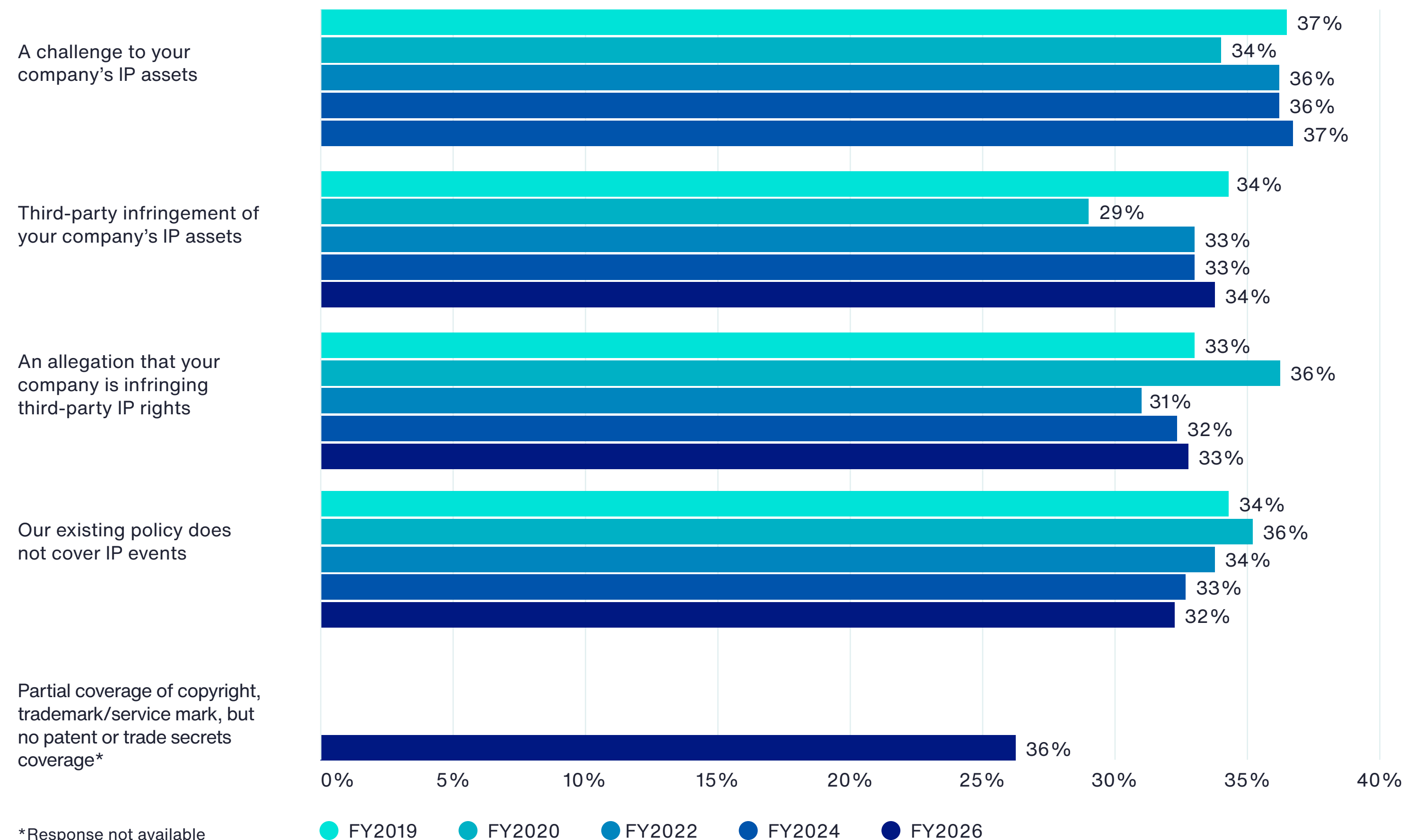
The average total value of organisations' IP assets such as trademarks, patents, copyrights, trade secrets and know-how is \$928 million and represents an average of 41 percent of total company's assets, a significant increase from \$638 million in 2024. In 2024, IP assets averaged 47 percent of total assets.

In this year's research, 47 percent of respondents say their organisation had a material IP event. In 2024, 56 percent of respondents said their organisation had a material IP event.

According to Figure 23, 49 percent of respondents say organisation's insurance policy covers third-party infringement of their IP assets and 42 percent say it provides partial coverage of copyright, trademark/service mark, but no patent or trade secrets coverage. Forty-one percent of respondents say it covers a challenge to their company's IP assets.

Figure 23. Does your organisation's existing insurance policy cover any of the following IP events? Q42

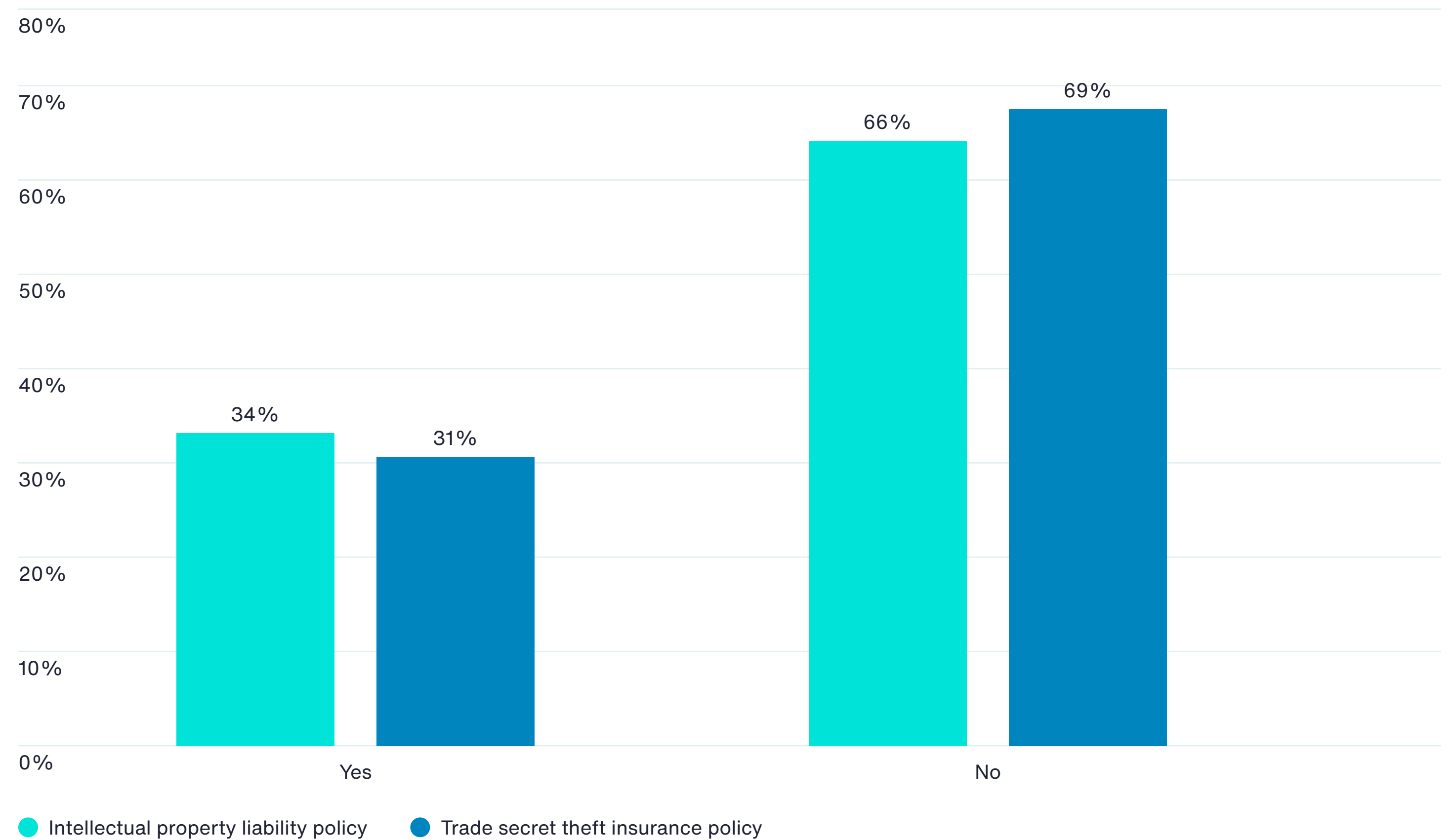
More than one response permitted



*Response not available for all years

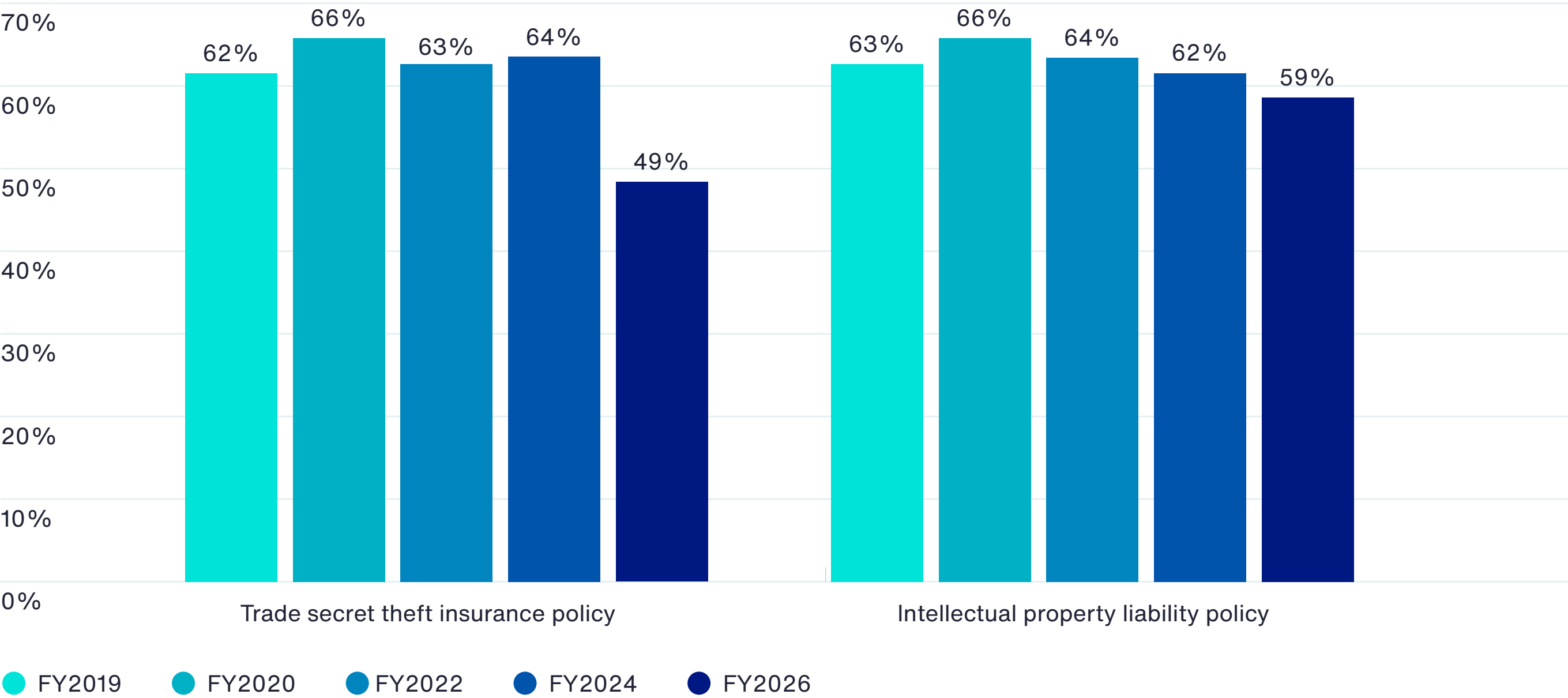
Organisations are more likely to have an IP liability policy than a trade secret policy. As shown in Figure 24, only 25 percent of respondents say they have a trade secret theft insurance policy and 41 percent of respondents say they have an intellectual property liability policy.

Figure 24. Does your organisation have a trade secret and/or IP liability policy? 43a



More organisations are interested in purchasing an IP liability policy. According to Figure 25, only 50 percent of respondents are very interested or interested in purchasing a trade secret insurance policy, a decrease from 64 percent in 2024. Similar to 2024, 68 percent of respondents say their organisations would purchase an intellectual property liability policy.

Figure 25. If no, what is your organisation’s level of interest in purchasing a trade secret theft insurance policy and/or an IP liability policy? Q43b, Q44b
Very interested and Interested responses combined



Cyber and IP risks rank in the top 5 of all business risks facing organisations. According to Figure 26, 55 percent of respondents rate the risk to their organisation's intellectual property (IP) among the top 5 of all business risks (23 percent + 32 percent). Seventy percent of respondents consider cyber risk as the number one or two business risk (27 percent of respondents) and among the top five (43 percent of respondents).

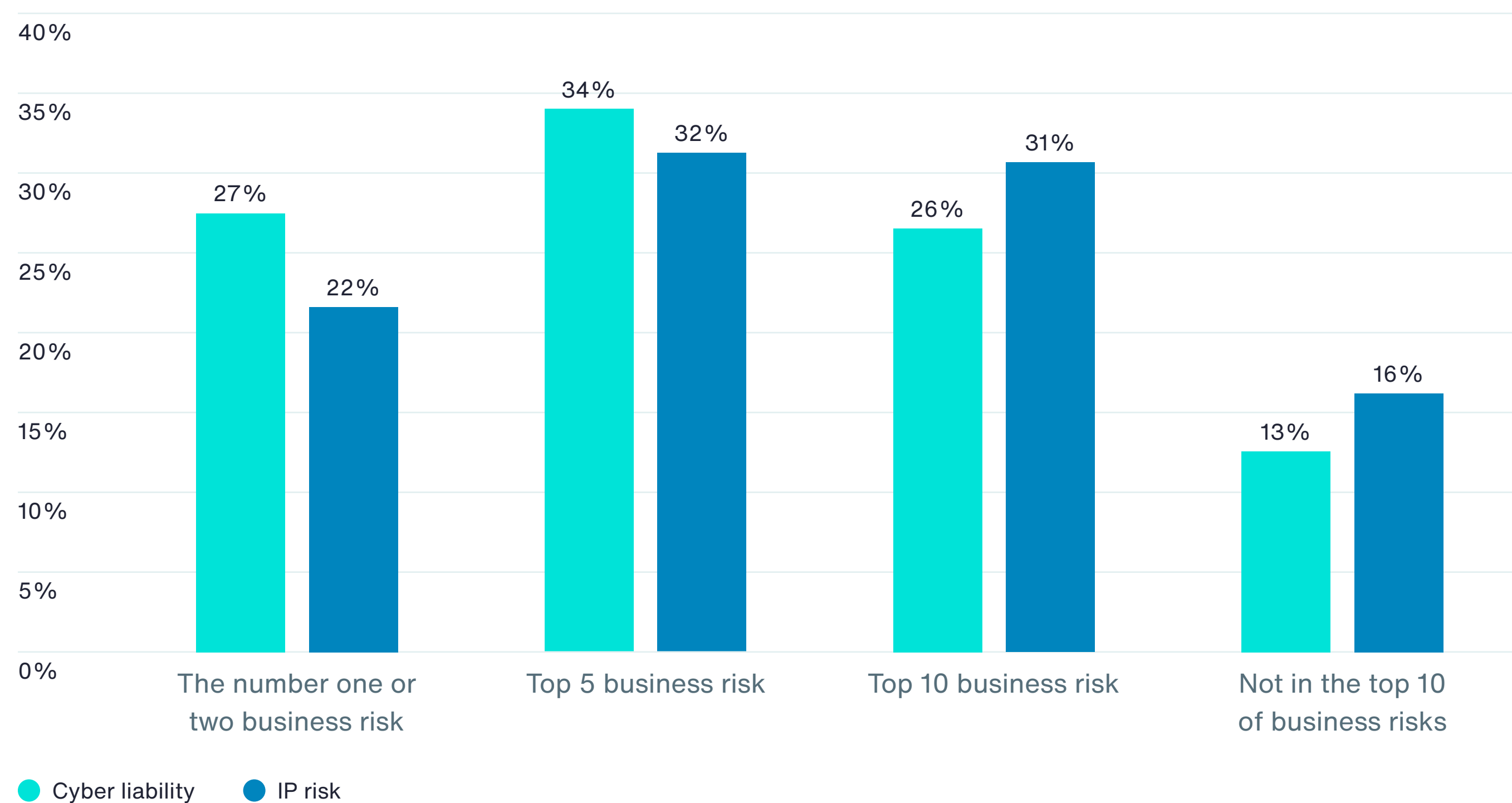
“

International access to London and Bermuda market capital enables positive insurance premium arbitrage and helps to optimize terms and conditions throughout the tower. Furthermore, Aon's tailored MGA facilities based in London can provide discreet and accretive capital to that available in the open market.

Beverley Alderson

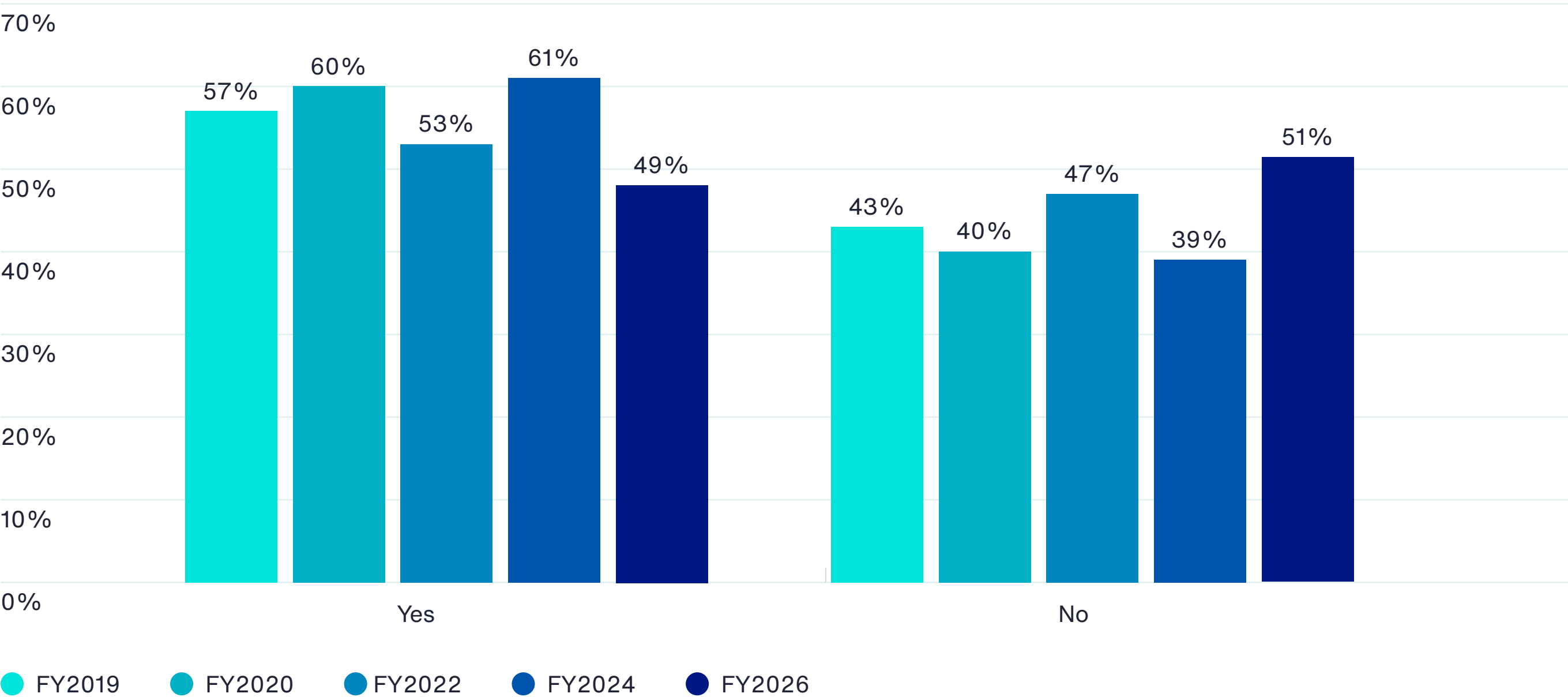
Global Broking Center — London
Aon

Figure 26. How do cyber and IP risks compare to other business risks? Q18,41



The value of company’s IP assets increased significantly but risk management activities involving risks to IP decreases. The value of IP assets has increased from \$638 million in 2024 to \$928 million in 2026. However, the percentage of respondents that say their organisations have a strategy to manage risks to IP has decreased. As shown in Figure 27, 49 percent of respondents say their enterprise risk management activities include risks to their IP, a significant decrease from 67 percent of respondents in 2024.

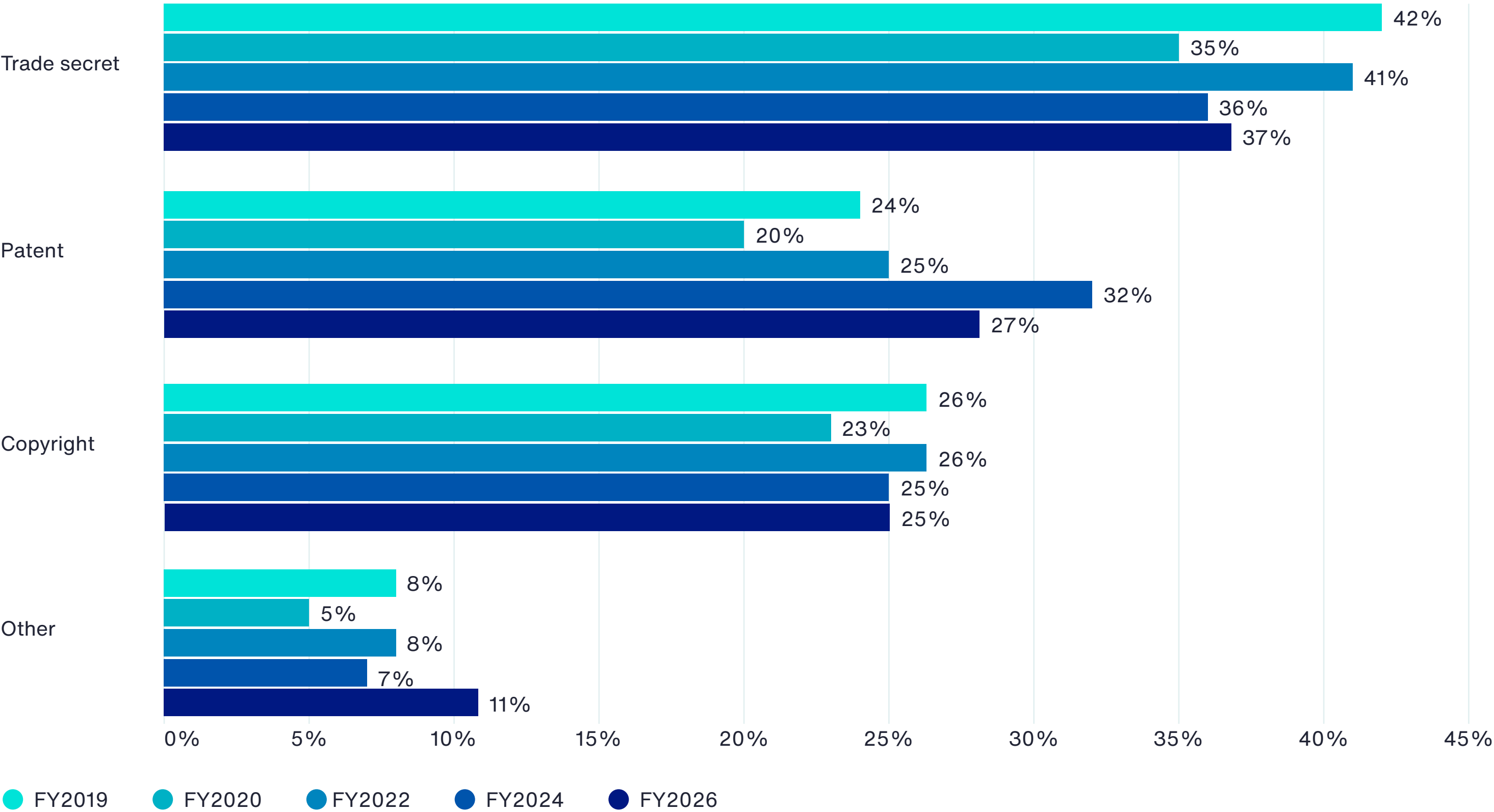
Figure 27. Do your organisation’s enterprise risk management activities include risks to IP? Q37



Fewer organisations experienced a material IP event in the past two years. In 2024, 51 percent of respondents said they experienced a material IP event. In 2026, 48 percent of respondents say their organisation experienced a material IP event.

According to Figure 28, in 2026 39 percent of respondents say the material IP security exploits involved trade secrets and 24 percent say it involved patents. In 2024, 32 percent of respondents said the incident involved trade secrets and 30 percent said it involved patents.

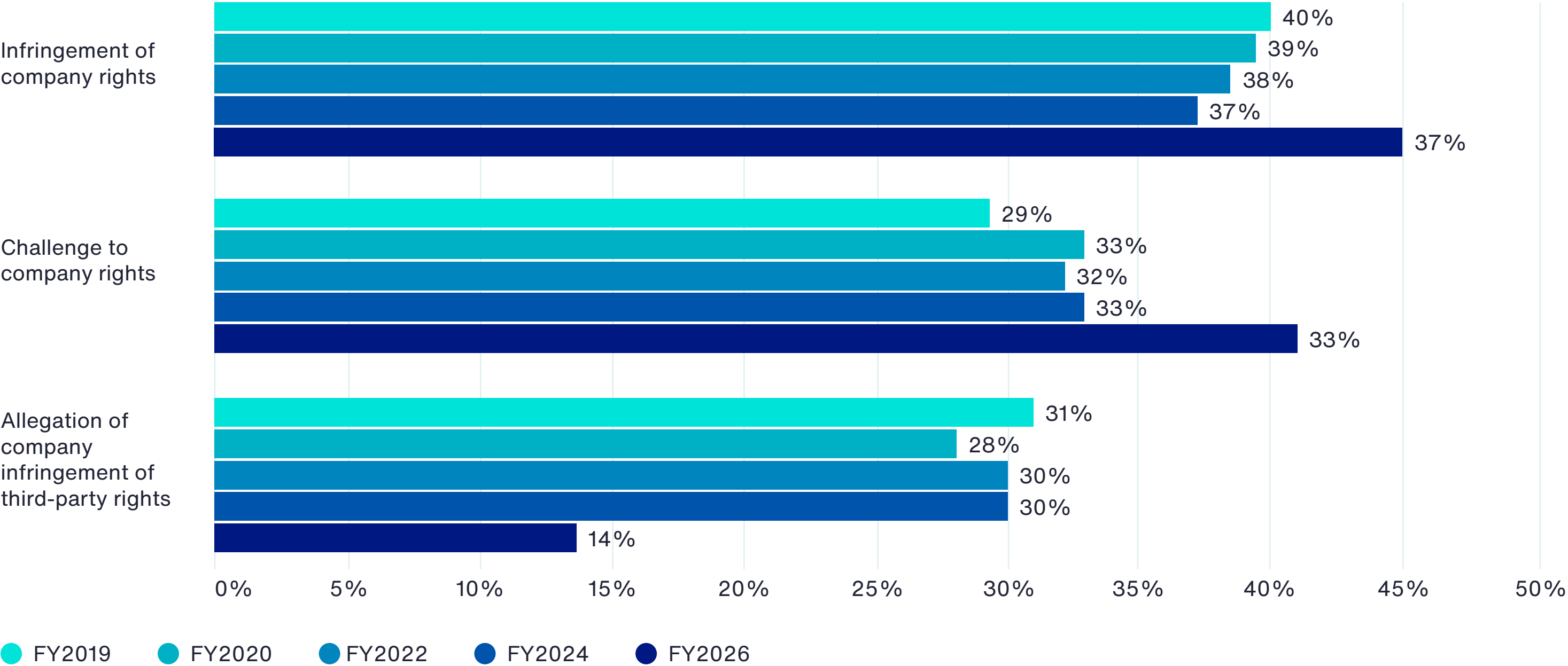
Figure 28. What type of IP assets were involved in a material IP event? Q40b
Only one choice permitted



Most incidents involved the Infringement of company rights. According to Figure 29, 49 percent say the incident involved the Infringement to company rights. Forty percent of respondents say it was a challenge to company rights.

Figure 29. What best describes the IP material event? Q40c

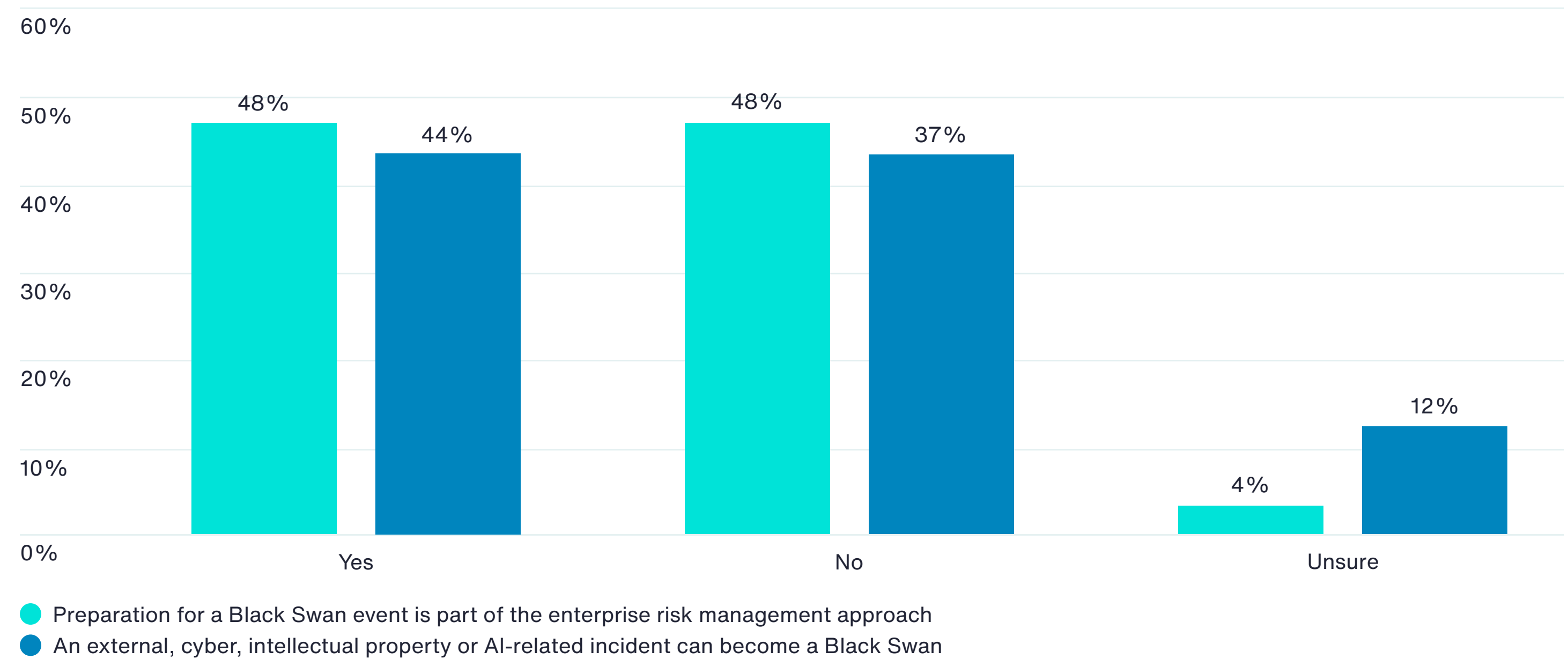
Only one response permitted



Forty-five percent of respondents say that an external, cyber, IP or AI-related incident can become a Black Swan incident for their firm. A Black Swan is an unpredictable or unforeseen event typically one with extreme consequences such as the SolarWinds attack in 2020, Log4Shell in 2021 or WannaCry in 2017. However, less than half (48 percent) of respondents are preparing for such an event and making it part of their enterprise risk management approach, as shown in Figure 30.

Figure 30. Managing a Black Swan event Q45,46

Only one response permitted



The use of AI to reduce cyber risks

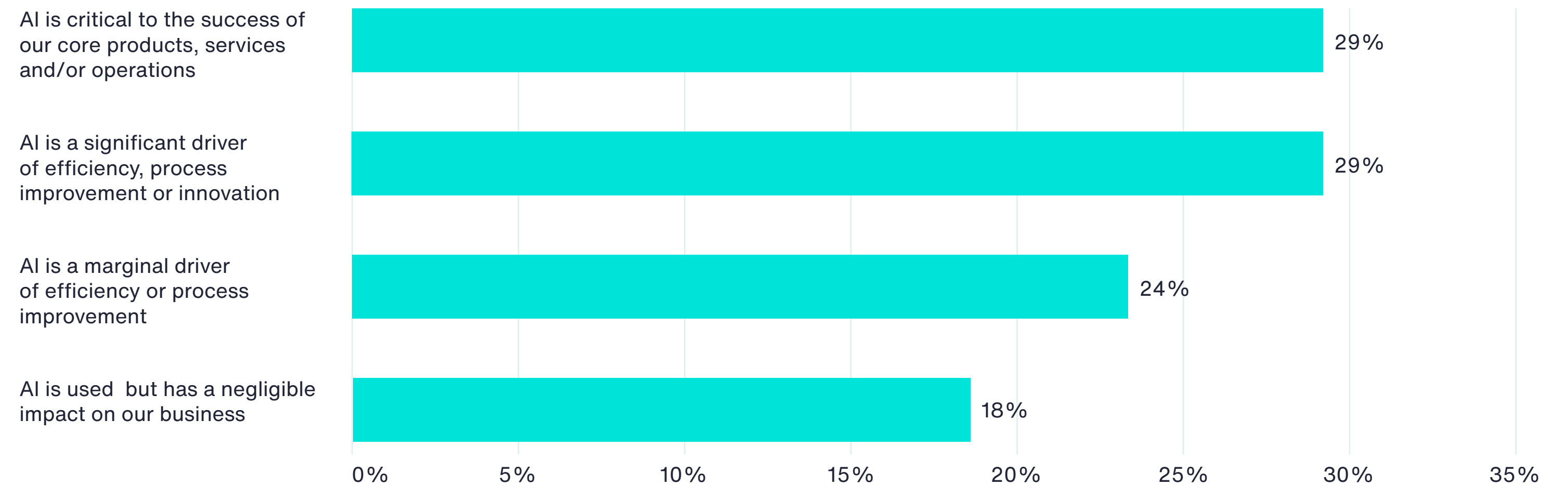
Most respondents believe AI is important in supporting the success of operations and innovation.

Sixty-eight percent of respondents currently use artificial intelligence products or services and 23 percent plan to use AI within the next 12 months.

Respondents were asked to select the one statement that best describes what AI means to their organisations. According to Figure 31, only 21 percent say AI has a negligible impact on their business. Thirty percent of respondents say AI is a significant driver of efficiency, process improvement or innovation and 25 percent of respondents say AI is critical to the success of their core products, services and/or operations.

Figure 31. How would you describe the pervasiveness and role of AI within your organisation? Q31

More than one response permitted

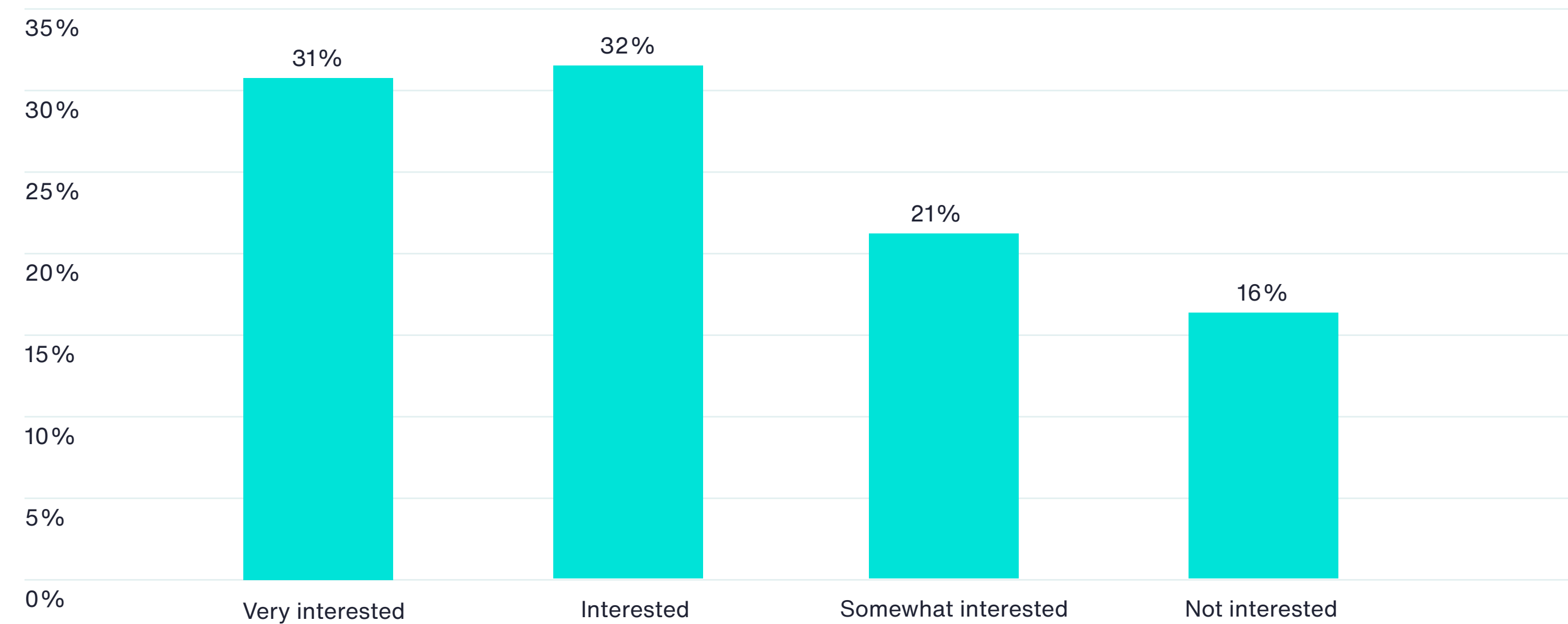


Organisations are vulnerable to the financial consequences of an AI-generated attack. The average value of the largest loss (PML) that could be caused by the lack of AI tools to secure information assets over the next 12 months is \$1,673 million. An average of 49 percent of the potential loss is covered by insurance, including captives reinsured but not including captives and not reinsured.

Sixty-five percent of respondents say their companies' existing insurance policies or a separate standalone AI liability policy **do not** cover the risks of an AI-generated attack and 14 percent of respondents are unsure.

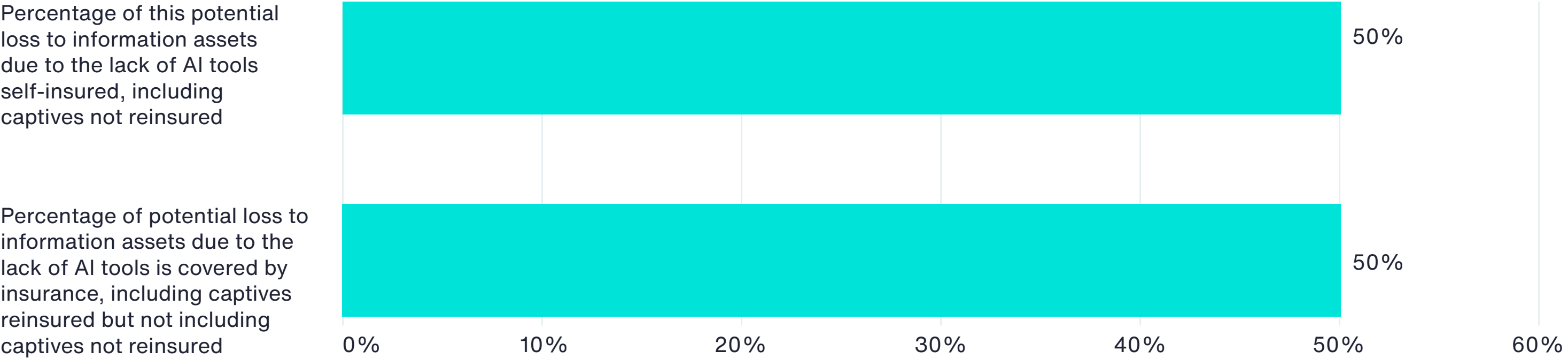
As shown in Figure 32, many organisations are very interested (28 percent) or interested (39 percent) in purchasing an AI liability policy. Only 14 percent of respondents say they are not interested.

Figure 32. How interested is your organisation in purchasing an AI liability policy? Q36b



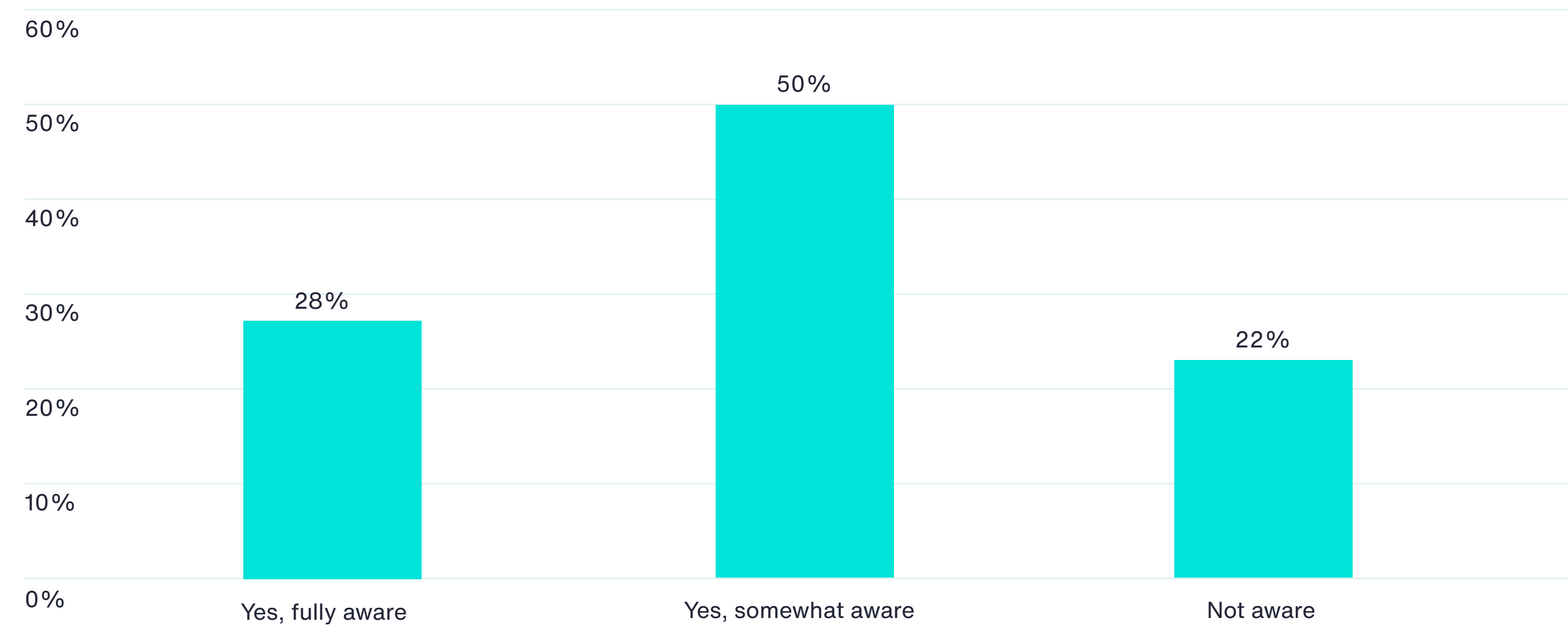
Interest in purchasing an AI liability policy is high because of awareness of the potential loss. The percentage of potential loss to information assets due to the lack of AI tools is 49 percent for insured and 50 percent for self-insured, as shown in Figure 33.

Figure 33. The average percentage of potential loss to information assets and self-insured Q33,34
Extrapolated average presented



Awareness is low of the economic and legal consequences resulting from non-compliance with AI regulations in other countries in which their company operates, such as the EU's AI Act. According to Figure 34, only 29 percent of respondents say they are fully aware of the consequences which can result in substantial fines up to 7 percent of an organisation's worldwide revenue. Fifty-two percent of respondents say they are somewhat aware.

Figure 34. Awareness about the economic and legal consequences resulting from non-compliance with AI regulations in other countries Q35



3

Methods

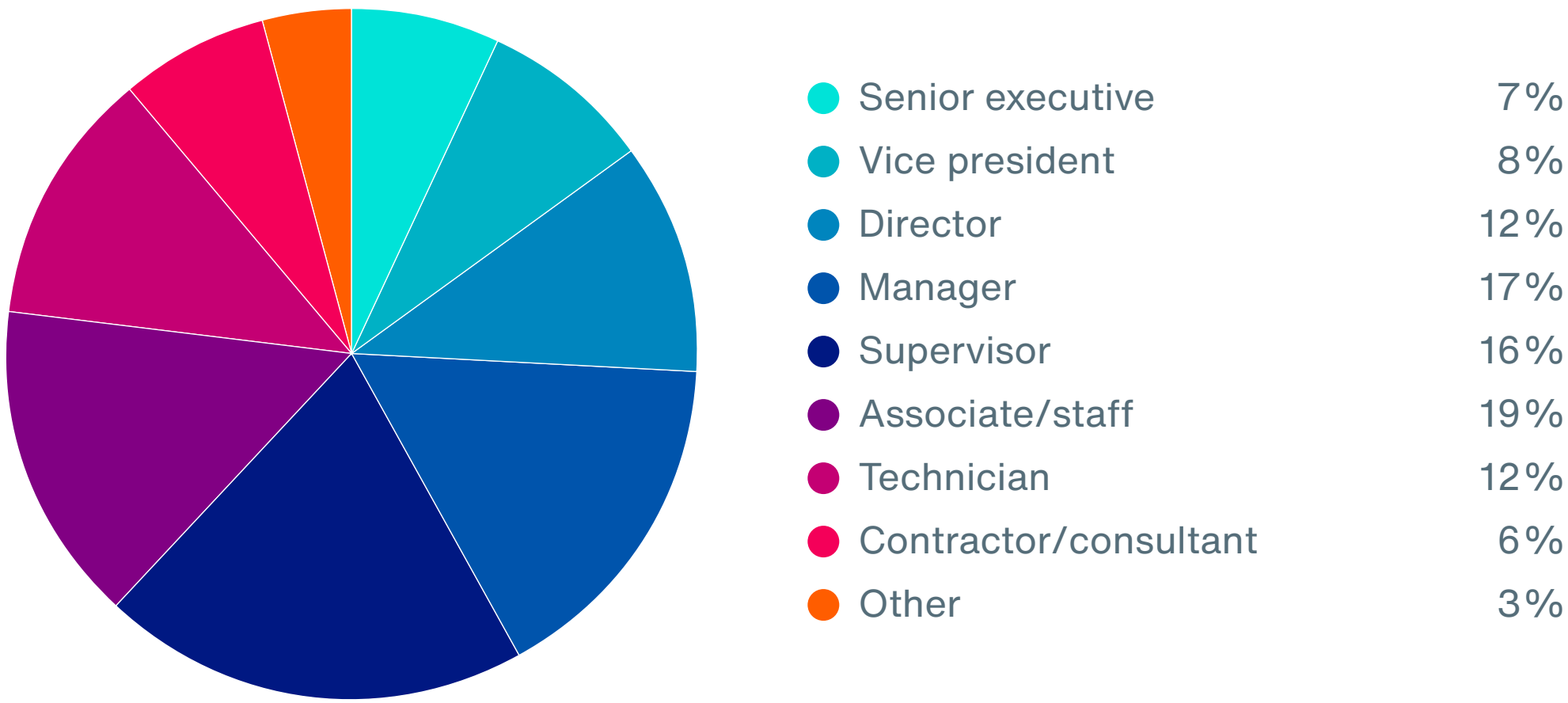


The EMEA sampling frame is composed of 16,405 individuals. Respondents are involved in their organisation’s cyber risk management as well as enterprise risk management activities. As Table 1 shows, 701 respondents completed the survey, of which 102 were rejected for reliability issues. The final sample consisted of 599 surveys, a 3.7 per cent response rate.

Table 1. Sample response	Freq	Pct%
Total sampling frame	16,405	100.0%
Total returns	701	4.3%
Rejected or screened surveys	102	0.6%
Final sample	599	3.7%

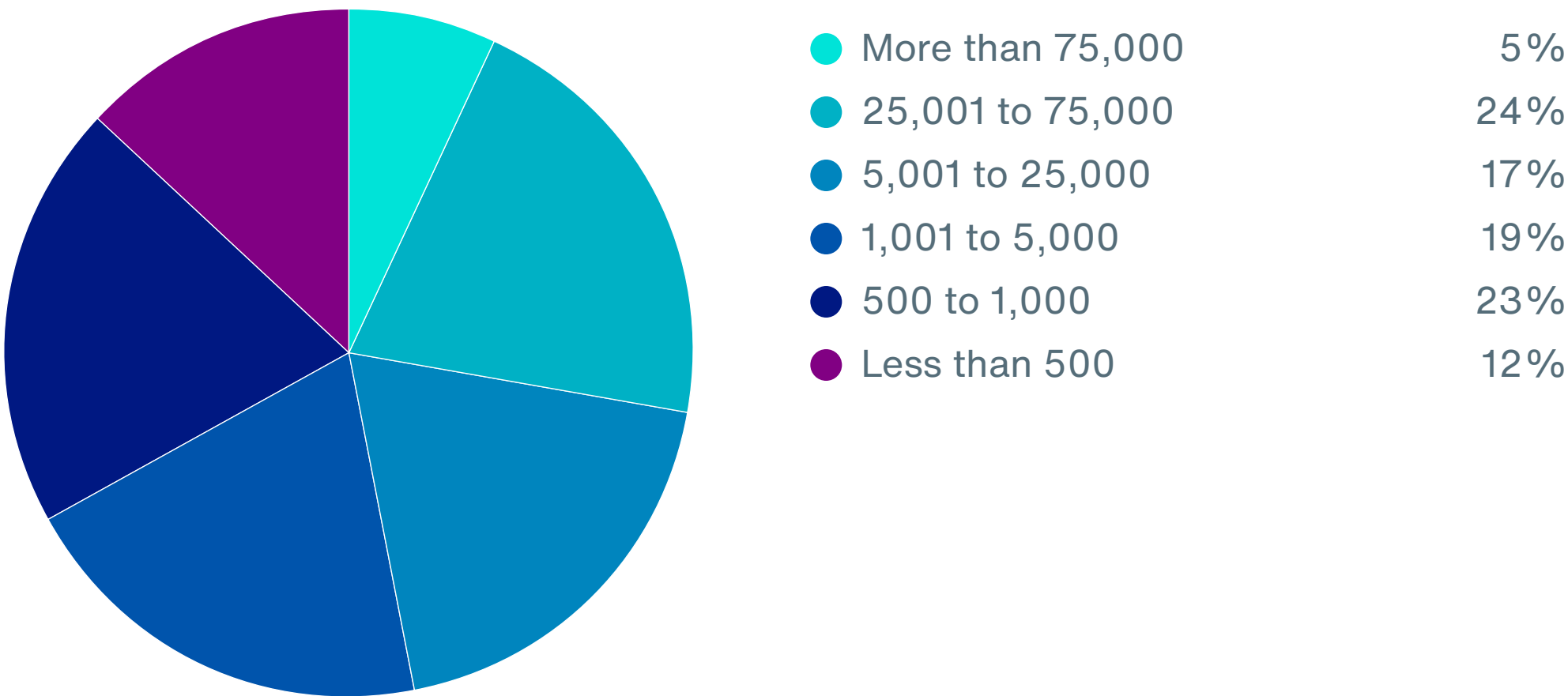
Pie Chart 1 reports the current position or organisational level of the respondents. More than half (62 percent) of the respondents reported their current position as supervisory level or above.

Pie Chart 1. Current position or organisational level



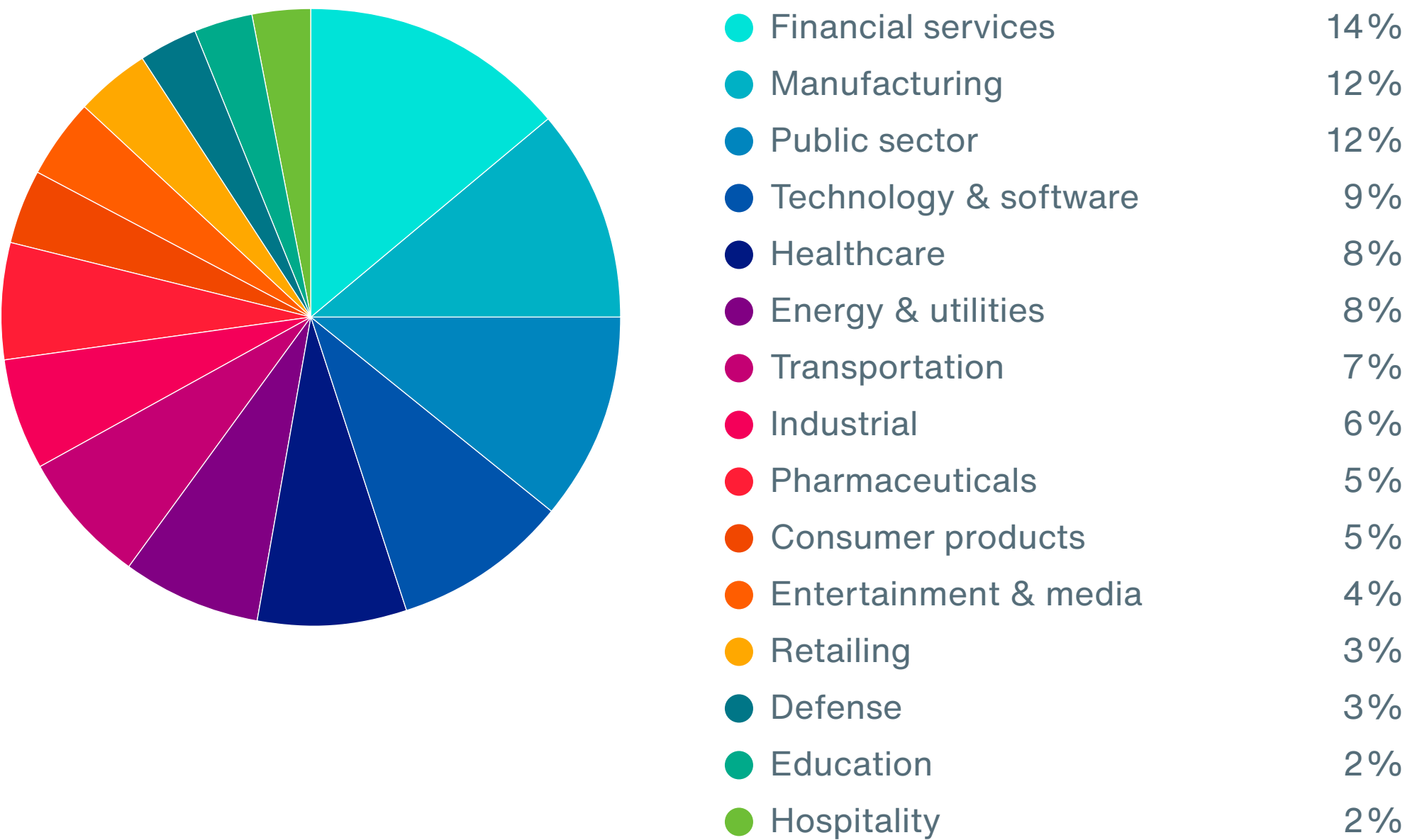
As Pie Chart 2 reveals, 65 per cent of the respondents are from organisations with a global headcount of more than 1,000 employees.

Pie Chart 2. Worldwide headcount of the organization



Pie Chart 3 reports the primary industry classification of respondents' organisations. This chart identifies financial services (14 per cent of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by manufacturing (12 per cent of respondents), public sector (12 per cent of respondents), healthcare (9 per cent of respondents), industrial (8 per cent of respondents), technology and software (8 per cent of respondents), and energy and utilities (each at 7 per cent of respondents).

Pie Chart 3. Primary industry focus



4

Caveats



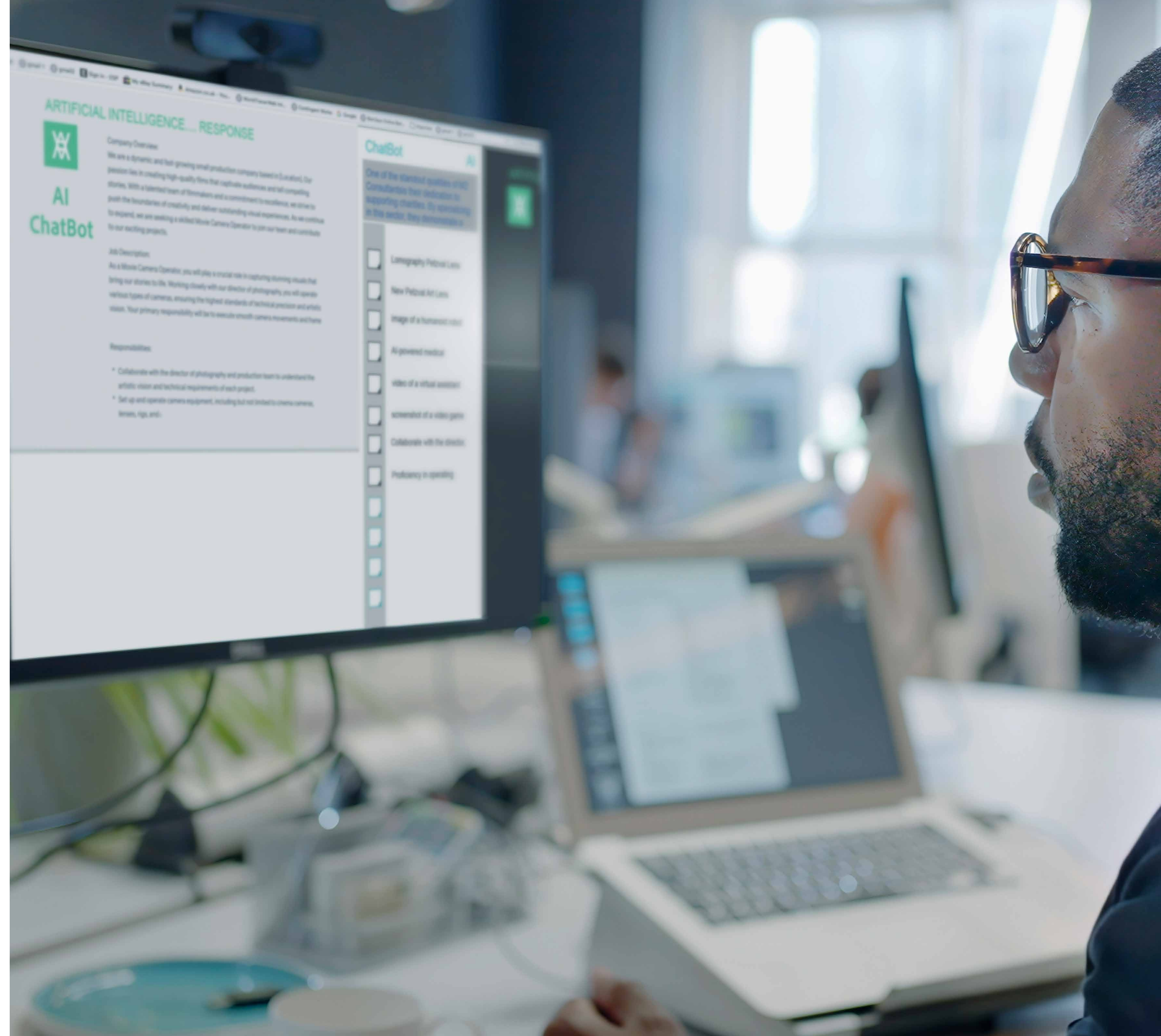
Part 4. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are involved in their organisations' cyber and enterprise risk management. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.



5

Appendix 2



5

Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in November and December 2025.

Survey response	EMEA 2026
Sampling frame*	16,405
Total returns	701
Rejected surveys	102
Final sample	599
Response rate	3.7%

*The sampling frame is a consolidation of four regions: EMEA, APAC, LATAM and North America.

Screening questions

S1. How familiar are you with cyber risks facing your company today?	EMEA 2026
Very familiar	26%
Familiar	31%
Somewhat familiar	28%
Not familiar	15%
No knowledge (stop)	0%
Total	100%

S2. Are you involved in your company’s cyber risk management activities?	EMEA 2026
Yes, significant involvement	36%
Yes, some involvement	64%
No involvement (stop)	0%
Total	100%

S3. What best defines your role?	EMEA 2026
Risk management	28%
Finance, treasury & accounting	33%
Corporate compliance/audit	18%
Security/information security	9%
General management	5%
Legal (OGC)	7%
None of the above (stop)	0%
Total	100%

S4. Are you involved in your company’s enterprise risk management activities?	EMEA 2026
Yes, significant involvement	43%
Yes, some involvement	57%
No involvement (stop)	0%
Total	100%

The following questions pertain to your company’s property, plant and equipment (PP&E)
Part 1. Sizing the economic impact

Q1. What is the total value of your company’s PP&E, including all fixed assets plus SCADA and industrial control systems? Please exclude and assume a value based on full replacement cost (and not historic cost).	EMEA 2026
Less than \$1 million	5%
\$1 to 10 million	11%
\$11 to 50 million	13%
\$51 to 100 million	11%
\$101 to 500 million	23%
\$501 to 1 billion	19%
\$1 to 10 billion	13%
More than \$10 billion	5%
Total	100%
Extrapolated value (US\$ millions)	\$1,474.37

Q2a. What is the value of the largest loss (PML) that could result from damage or the total destruction of PP&E. Please assume the normal functioning of passive protective features – such as firewalls, nonflammable materials, proper functioning of active suppression systems, fire sprinklers, raised flooring and more.	EMEA 2026
Less than \$1 million	3%
\$1 to 10 million	9%
\$11 to 50 million	14%
\$51 to 100 million	20%
\$101 to 500 million	29%
\$501 to 1 billion	12%
\$1 to 10 billion	11%
More than \$10 billion	2%
Total	100%
Extrapolated value (US\$ millions)	\$986.79

Q2b. What is the value of your largest loss (PML) due to business interruption? Please assume the normal functioning of passive protective features – such as firewalls, nonflammable materials, proper functioning of active suppression systems, fire sprinklers, raised flooring and more.	
	FY2026
Less than \$1 million	11%
\$1 to 10 million	24%
\$11 to 50 million	23%
\$51 to 100 million	20%
\$101 to 500 million	13%
\$501 to 1 billion	7%
\$1 to 10 billion	2%
More than \$10 billion	0%
Total	100%
Extrapolated value (US\$ millions)	\$214.93

Q3. What percentage of this potential loss to PP&E assets is covered by insurance, including captives reinsured but not including captives not reinsured?	
	EMEA 2026
Less than 5%	3%
5% to 10%	7%
11% to 20%	8%
21% to 30%	8%
31% to 40%	9%
41% to 50%	8%
51% to 60%	12%
61% to 70%	10%
71% to 80%	13%
81% to 90%	13%
91% to 100%	9%
Total	100%
Extrapolated value	53%

Q4. What percentage of this potential loss to PP&E assets is self-insured, including captives not reinsured?	EMEA 2026
Less than 5 %	10 %
5 % to 10 %	12 %
11 % to 20 %	13 %
21 % to 30 %	9 %
31 % to 40 %	14 %
41 % to 50 %	13 %
51 % to 60 %	9 %
61 % to 70 %	8 %
71 % to 80 %	6 %
81 % to 90 %	2 %
91 % to 100 %	4 %
Total	100 %
Extrapolated value	36 %

Q5. What is the likelihood that your company will sustain a loss to PP&E assets totaling no more than 50 percent of PML over the next 12 months?	EMEA 2026
Less than 0.1%	20%
0.1% to 0.5%	12%
0.6% to 1.0%	16%
1.1% to 2.0%	12%
2.1% to 3.0%	15%
3.1% to 4.0%	10%
4.1% to 5.0%	8%
5.5% to 10.0%	4%
More than 10.0%	3%
Total	100%
Extrapolated value	2.1%

Q6. What is the likelihood that your company will sustain a loss to PP&E assets totaling 100 percent of PML over the next 12 months?	EMEA 2026
Less than 0.1%	64%
0.1% to 0.5%	14%
0.6% to 1.0%	8%
1.1% to 2.0%	6%
2.1% to 3.0%	2%
3.1% to 4.0%	1%
4.1% to 5.0%	2%
5.1% to 10.0%	3%
More than 10.0%	0%
Total	100%
Extrapolated value	0.66%

Q7. In your opinion, how would your company disclose a material loss to PP&E assets that is not covered by insurance in its financial statements?	EMEA 2026
Disclosure as a contingent liability on the balance sheet (e.g., FASB 5)	26%
Footnote disclosure in the financial statements	38%
Discussion in the management letter	19%
None – disclosure is not necessary	13%
Other	4%
Total	100%

The following questions pertain to your company’s information assets.

Q8. What is the total value of your company’s information assets , including customer records, employee records, financial reports, analytical data, source code, models, methods and other intellectual properties? Please assume a value based on full replacement cost (and not historic cost). Please note this value can be either a precise quantification or estimate.	EMEA 2026
Less than \$1 million	0%
\$1 to 10 million	2%
\$11 to 50 million	10%
\$51 to 100 million	29%
\$101 to 500 million	26%
\$501 to 1 billion	22%
\$1 to 10 billion	6%
More than \$10 billion	5%
Total	100%
Extrapolated value (US\$ millions)	\$1,167.91

Q9a. What is the value of the largest loss (PML) that could result from the theft and/or destruction of information assets. Please assume the normal functioning of passive protective cybersecurity features – such as perimeter controls, data loss prevention tools, data encryption, identity and access management systems and more.	EMEA 2026
Less than \$1 million	5%
\$1 to 10 million	12%
\$11 to 50 million	15%
\$51 to 100 million	21%
\$101 to 500 million	24%
\$501 to 1 billion	10%
\$1 to 10 billion	8%
More than \$10 billion	5%
Total	100%
Extrapolated value (US\$ millions)	\$1,168

Q9b. What is the value of your largest loss (PML) due to cyber business interruption? Please assume the normal functioning of passive protective features – such as perimeter controls, data loss prevention tools, data encryption, identity and access management systems and more.		EMEA 2026
Less than \$1 million		15 %
\$1 to 10 million		23 %
\$11 to 50 million		20 %
\$51 to 100 million		16 %
\$101 to 500 million		12 %
\$501 to 1 billion		11 %
\$1 to 10 billion		3 %
More than \$10 billion		0 %
Total		100 %
Extrapolated value (US\$ millions)		\$288.0

Q10. For each of the following external risk scenarios, is the likelihood of a PML event more likely, less likely or about the same as a similar event caused by internal risks to your information assets?	
Q10a. Software as a Service (SaaS) provider interruption:	EMEA 2026
More likely	32 %
Less likely	42 %
About the same	26 %
Total	100 %

Q10b. AI/cyber IT disruption at a supply chain provider (physical):	EMEA 2026
More likely	41 %
Less likely	39 %
About the same	20 %
Total	100 %

Q10c. Power/Telco/Internet/cloud infrastructure interruption:	EMEA 2026
More likely	39 %
Less likely	42 %
About the same	19 %
Total	100 %

Q11. For each of the following external risk scenarios, would the severity of a PML event be more severe, less severe or about the same as a similar event caused by internal risks to your information assets?	
Q11a. Software as a Service (SaaS) provider interruption:	EMEA 2026
More severe	40%
Less severe	44%
About the same	16%
Total	100%
Q11b. AI/cyber IT disruption at a supply chain provider (physical):	EMEA 2026
More severe	37%
Less severe	44%
About the same	19%
Total	100%
Q11c. Power/Telco/Internet/cloud infrastructure interruption:	EMEA 2026
More severe	31%
Less severe	48%
About the same	21%
Total	100%

Q12. What is the likelihood your company will sustain a loss to information assets totaling no more than 50 percent of PML over the next 12 months?	EMEA 2026
Less than 0.1%	5%
0.1% to 0.5%	2%
0.6% to 1.0%	8%
1.1% to 2.0%	10%
2.1% to 3.0%	11%
3.1% to 4.0%	14%
4.1% to 5.0%	15%
5.1% to 10.0%	16%
More than 10.0%	19%
Total	100%
Extrapolated value	5.0%

Q13. What is the likelihood your company will sustain a loss to information assets totaling 100 percent of PML over the next 12 months?		EMEA 2026
Less than 0.1%		3%
0.1% to 0.5%		2%
0.6% to 1.0%		8%
1.1% to 2.0%		10%
2.1% to 3.0%		9%
3.1% to 4.0%		14%
4.1% to 5.0%		19%
5.1% to 10.0%		16%
More than 10.0%		19%
Total		100%
Extrapolated value		5.1%

Q14. In your opinion, how would your company disclose a material loss to information assets that is not covered by insurance in its financial statements?		EMEA 2026
Disclosure as a contingent liability on the balance sheet (FASB 5)		15%
Footnote disclosure in the financial statements		39%
Discussion in the management letter		13%
None – disclosure is not necessary		28%
Other		5%
Total		100%

Part 2. Other Questions

Q15. Are you aware of the economic and legal consequences resulting from a data breach or security exploit in other countries in which your company operates, such as the European Union’s General Data Protection Regulation (GDPR), which may issue a fine of up to 4 percent of an organisation’s worldwide revenue?		EMEA 2026
Yes, fully aware		52%
Yes, somewhat aware		34%
Not aware		14%
Total		100%

Q16a. Has your company experienced a material or significantly disruptive security exploit or data breach one or more times over the past 24 months? Please refer to the definition of materiality provided above.		EMEA 2026
Yes		59%
No [skip to Q17]		41%
Total		100%

Q16b. If yes, what best describes the data breaches or security exploits experienced by your company over the past 24 months? Please select all that apply.		EMEA 2026
Cyber attack that caused disruption to business and IT operations (such as denial of service attacks)		53%
Cyber attack that resulted in the theft of business confidential information, thus requiring notification to victims		43%
Cyber attack that resulted in the misuse or theft of business confidential information, such as intellectual properties		40%
Negligence or mistakes that resulted in the loss of business confidential information		75%
System or business process failures that caused disruption to business operations (e.g., software updates)		61%
Other		6%
Total		278%

Q16c. If yes, what was the total financial impact of security exploits and data breaches experienced by your company over the past 24 months. Please include all costs including out-of-pocket expenditures such as consultant and legal fees, indirect business costs such as productivity losses, diminished revenues, legal actions, customer turnover and reputational damage.		EMEA 2026
Zero		0%
Less than \$10,000		3%
\$10,001 to \$100,000		6%
\$100,001 to \$250,000		18%
\$250,001 to \$500,000		23%
\$500,001 to \$1,000,000		19%
\$1,000,001 to \$5,000,000		12%
\$5,000,001 to \$10,000,000		6%
\$10,000,001 to \$25,000,000		7%
\$25,000,001 to \$50,000,000		6%
\$50,000,001 to \$100,000,000		0%
More than \$100,000,000		0%
Total		100%
Extrapolated value US\$		\$4,548,790

Q16d. If yes, how has the above security exploit or data breach changed your company’s concerns about cyber liability?	EMEA 2026
More concerned	72%
Less concerned	12%
No change	16%
Total	100%

Q17. Do you believe your company’s exposure to cyber risk will increase, decrease or stay the same over the next 24 months?	EMEA 2026
Increase	69%
Decrease	13%
Stay the same	18%
Total	100%

Q18a. From a business risk perspective, how do cyber risks compare to other business risks. Please select one best choice.	EMEA 2026
Cyber liability is the number one or two business risk for my company	27%
Cyber liability is a top 5 business risk for my company	43%
Cyber liability is a top 10 business risk for my company	20%
Cyber liability is not in the top 10 of business risks for my company	10%
Total	100%

Q19. How did you determine the level of cyber risk to your company?	EMEA 2026
Completed a formal internal assessment	28%
Completed an informal (ad hoc) internal assessment	26%
Hired a third party to conduct an assessment or audit	29%
Intuition or gut feel	13%
Did not do any type of assessment	4%
Total	100%

Q20a. Does your company have cyber insurance coverage, including within a technology Errors & Omission, standalone cyber policy or similar policy not including Property, General Liability or Crime policy?	EMEA 2026
Yes	33%
No [please skip to Q26a]	67%
Total	100%

Q20b. If yes, what limits do you purchase	EMEA 2026
Less than \$1 million	12%
\$1 million to \$5 million	34%
\$6 million to \$20 million	45%
\$21 million to \$100 million	8%
More than \$100 million	1%
Total	100%
Extrapolated value (US\$ millions)	\$12.92

Q21. Is your company’s cyber insurance coverage sufficient with respect to coverage terms and conditions, exclusions, retentions, limits and insurance carrier financial security?	EMEA 2026
Yes	54%
No	27%
Unsure	19%
Total	100%

Q22. How does your company determine the level of coverage it deems adequate?	EMEA 2026
Formal risk assessment by in-house staff	21%
Formal risk assessment conducted by the insurer	14%
Formal risk assessment by a third-party specialist*	27%
Informal or ad hoc risk assessment	14%
Policy terms and conditions reviewed by a third-party specialist, such as a law firm*	10%
Maximum available from the insurance market	13%
Other	1%
Total	100%

Q23. What types of incidents does your organisation’s cyber insurance cover? Please select all that apply.		EMEA 2026
External attacks by cyber criminals, including ransomware *		75%
Malicious or criminal insiders		69%
System or business process failures		61%
Human error, mistakes and negligence, including artificial intelligence*		59%
Incidents affecting business partners, vendors or other third parties that have access to your company’s information assets		46%
Third-party vendors and suppliers, such as cloud, Software as a Service and infrastructure		42%
Other		8%
Unsure		3%
Total		363%

Q24. What coverage does this insurance offer your company? Please select all that apply.		EMEA 2026
Forensics and investigative costs		68%
Notification costs to data breach victims		60%
Communication costs to regulators		40%
Employee productivity losses		54%
Replacement of lost or damaged equipment		60%
Revenue losses		31%
Legal defence costs		58%
Loss of asset value		39%
Regulatory penalties and fines		40%
Third-party liability		45%
Brand damages		31%
Ransomware payments and costs		36%
Other		6%
Unsure		10%
Total		578%

Q25. In addition to cost coverage, what other services does the cyber insurer provide your company in the event of a security exploit or data breach? Please check all that apply.		EMEA 2026
Access to cyber security forensic experts		76%
Access to legal and regulatory experts		69%
Access to specialized technologies and tools		53%
Advanced warnings about ongoing threats and vulnerabilities		42%
Assistance in the remediation of the incident		53%
Assistance in the notification of breach victims		29%
Identity protection services for breach victims		19%
Credit monitoring services for breach victims		47%
Assistance in reputation management activities		54%
Other		16%
Total		458%

Q26a. Does your company plan to purchase standalone cyber insurance?	EMEA 2026
Yes, in the next 12 months	29%
Yes, in the next 24 months	21%
Yes, in more than 24 months	25%
No plan to purchase	25%
Total	100%

Q26b. If no, what are the two main reasons why your company is not planning to purchase standalone cyber security insurance? Please select two choices only.		EMEA 2026
Premiums are too expensive		42%
Coverage is inadequate based on our exposure (too many exclusions, restrictions and uninsurable risks)		49%
Risk does not warrant insurance		26%
Property and casualty policies are sufficient		35%
Executive management does not see the value of this insurance		21%
Unable to get insurance underwritten because of current risk profile		21%
Other		6%
Total		200%

Q27. Who in your company is most responsible for cyber risk management? Please select two choices only.		EMEA 2026
CEO/board of directors		15%
Chief financial officer		18%
Business unit (LOB) leaders		19%
Chief information officer		31%
Chief information security officer		35%
Risk management		25%
Procurement		18%
General counsel		15%
Compliance/audit		15%
Other		9%
Total		200%

Q28. Does your organization use or plan to use cryptocurrency or non-fungible token assets?		EMEA 2026
Yes, currently use		60%
No, but planning to use within the next 12 months		29%
There are no plans to use		11%
Total		100%

Q29. Does your organization use or plan to use stablecoins as a base currency for participating in digital asset markets, decentralized finance (DeFi) or other blockchain-based financial products?		EMEA 2026
Yes, currently use		34%
No, but planning to use within the next 12 months		46%
There are no plans to use		20%
Total		100%

Part 3. The use of AI to reduce cyber risks

Q30. Does your organization use or plan to use artificial intelligence products or services?	EMEA 2026
Yes, currently use	68%
No, but planning to use within the next 12 months	23%
There are no plans to use [please skip to Q37]	9%
Total	100%

Q31. How would you describe the pervasiveness and role of AI within your organization? Please select one choice only.	EMEA 2026
AI is critical to the success of our core products, services and/or operations	25%
AI is a significant driver of efficiency, process improvement or innovation	30%
AI is a marginal driver of efficiency or process improvement	24%
AI is used but has a negligible impact on our business	21%
Total	100%

Q32. What is the value of your largest loss (PML) that could be caused by the lack of AI tools to secure information assets to over the next 12 months?	EMEA 2026
Cannot determine	6%
Less than \$1 million	5%
\$1 million to \$10 million	8%
\$11 million to \$50 million	19%
\$51 million to \$100 million	20%
\$101 million to \$500 million	13%
\$501 million to \$1 billion	11%
\$1 billion to \$10 billion	9%
More than \$10 billion	9%
Total	100%
Extrapolated value (\$millions)	\$1,673

Q33. What percentage of this potential loss to information assets due to the lack of AI tools is covered by insurance, including captives reinsured but not including captives not reinsured?	EMEA 2026
Less than 5 %	4 %
5 % to 10 %	5 %
11 % to 20 %	7 %
21 % to 30 %	9 %
31 % to 40 %	13 %
41 % to 50 %	16 %
51 % to 60 %	11 %
61 % to 70 %	10 %
71 % to 80 %	12 %
81 % to 90 %	7 %
91 % to 100 %	6 %
Total	100 %
Extrapolated value	49 %

Q34. What percentage of this potential loss to information assets due to the lack of AI tools is self-insured, including captives not reinsured?	EMEA 2026
Less than 5 %	3 %
5 % to 10 %	4 %
11 % to 20 %	8 %
21 % to 30 %	6 %
31 % to 40 %	11 %
41 % to 50 %	18 %
51 % to 60 %	15 %
61 % to 70 %	10 %
71 % to 80 %	12 %
81 % to 90 %	8 %
91 % to 100 %	5 %
Total	100 %
Extrapolated value	50 %

Q35. Are you aware of the economic and legal consequences resulting from non-compliance with artificial intelligence (AI) regulations in other countries in which your company operates, such as the European Union’s AI Act. The Act may impose substantial fines up to 7 percent of an organisation’s worldwide revenue?		EMEA 2026
Yes, fully aware		29%
Yes, somewhat aware		52%
Not aware		19%
Total		100%

Q36a. Does your company cover the risks of an AI-generated attack in either a combination of existing insurance policies or separate standalone AI liability policy?		EMEA 2026
Yes		21%
No		65%
Unsure		14%
Total		100%

Q36b. If no or unsure, how interested is your organization in purchasing an AI liability policy?		EMEA 2026
Very interested		28%
Interested		39%
Somewhat interested		19%
Not interested		14%
Total		100%

Part 4. IP risks

Q37. Does your company’s enterprise risk management activities include risks to IP such as trademarks and brand, patents, copyrights and trade secrets as well as liability risks relating to third-party IP?		EMEA 2026
Yes		49%
No (Please skip to Part 5)		51%
Total		100%

Q38a. What is the total value of your company’s IP assets such as trademarks, patents, copyrights, trade secrets and know-how?		EMEA 2026
Less than \$1 million		3%
\$1 to 10 million		8%
\$11 to 50 million		15%
\$51 to 100 million		22%
\$101 to 500 million		24%
\$501 to 1 billion		18%
\$1 to 10 billion		6%
More than \$10 billion		4%
Total		100%
Extrapolated value (\$ millions)		\$928

Q39. What is the IP asset percentage value of your company’s total assets (intellectual property includes trademarks, patents, copyrights, trade secrets and know-how)?		EMEA 2026
Less than 5%		6%
5% to 10%		7%
11% to 25%		23%
26% to 50%		27%
51% to 75%		28%
More than 75%		9%
Total		100%
Extrapolated value		41%

Q40a. Did your company experience a material IP event in the past 24 months?		EMEA 2026
Yes		47%
No		53%
Total		100%

Q40b. If yes, what type of IP assets were involved in the event?	EMEA 2026
Patent	24 %
Trade secret	39 %
Copyright, trademark or service mark	30 %
Other	7 %
Total	100 %

Q40c. If yes, what best describes the event?	EMEA 2026
Challenge to company rights	40 %
Infringement of company rights	49 %
Allegation of company infringement of third-party rights	11 %
Total	100 %

Q41. How do IP risks compare to other business risks?	EMEA 2026
IP risk is the number one or two business risk for my company	23 %
IP risk is a top 5 business risk for my company	32 %
IP risk is a top 10 business risk for my company	31 %
IP risk is not in the top 10 of business risks for my company	14 %
Total	100 %

Q42. Does your company’s existing insurance policy (e.g., property, general liability or crime) cover any of the following IP events?	EMEA 2026
A challenge to your company’s IP assets	41 %
Third-party infringement of your company’s IP assets	49 %
An allegation that your company is infringing third-party IP rights	39 %
Our existing policy does not cover IP events	34 %
Partial coverage of copyright, trademark/service mark, but no patent or trade secrets coverage	42 %
Total	205 %

Q43a. Does your company have a trade secret theft insurance policy as a complement to a cyber risk policy?	EMEA 2026
Yes	25 %
No	75 %
Total	100 %

Q43b. If no, what is your company’s level of interest in purchasing a trade secret theft insurance policy as a complement to a cyber risk policy?	EMEA 2026
Very interested	23%
Interested	27%
Somewhat interested	32%
Not interested	18%
Total	100%

Q44a. Does your company have an intellectual property liability policy?	EMEA 2026
Yes	41%
No	59%
Total	100%

Q44b. If not, what is your company’s level of interest in purchasing an intellectual property liability policy?	EMEA 2026
Very interested	34%
Interested	34%
Somewhat interested	28%
Not interested	4%
Total	100%

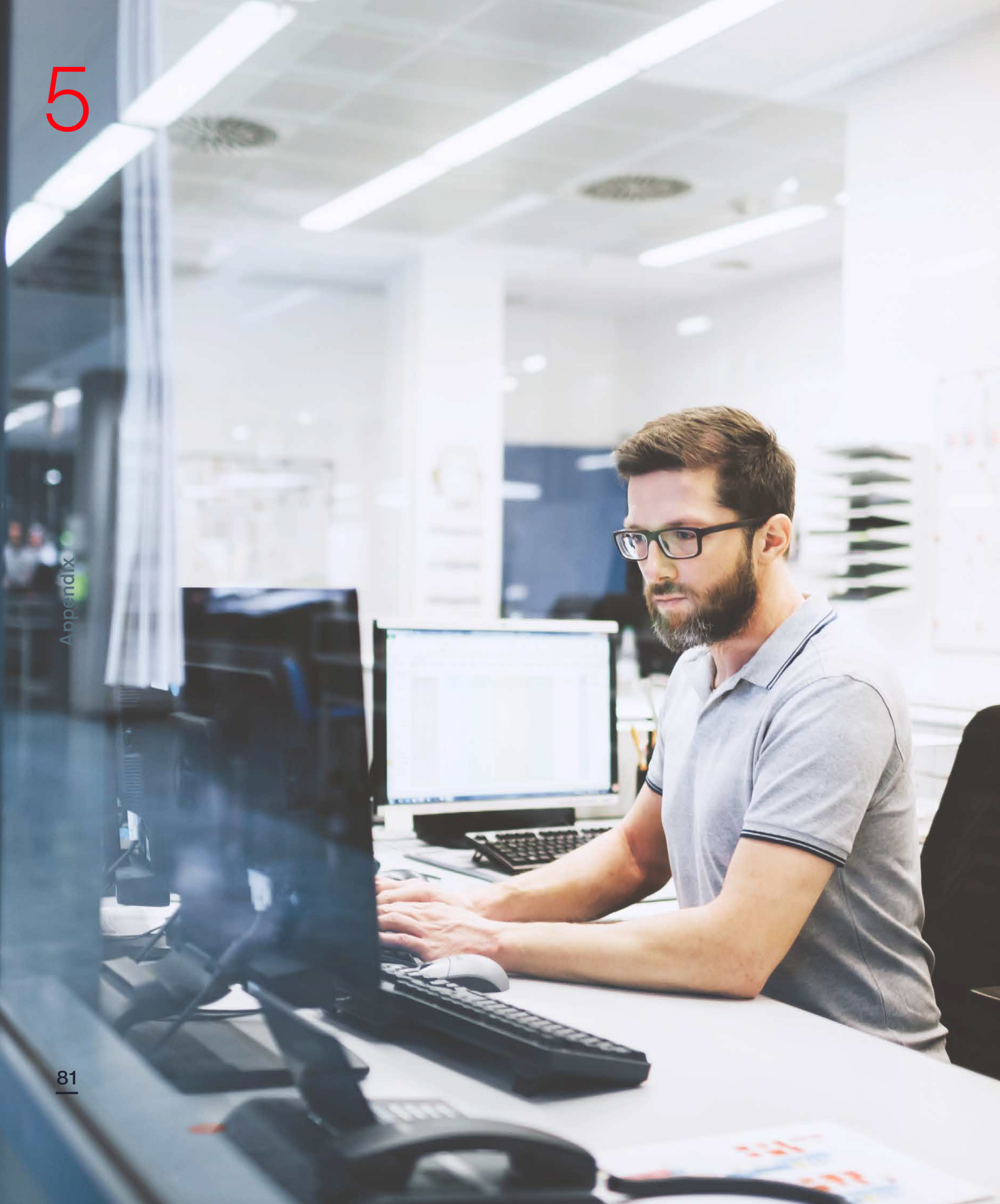
Q45. Can an external, cyber, intellectual property or AI-related incident become a Black Swan for your firm? Black Swan is an unpredictable or unforeseen event, typically one with extreme consequences (e.g. SolarWinds attack (2020); Log4Shell (2021) WannaCry (2017)?	EMEA 2026
Yes	45%
No	42%
Unsure	13%
Total	100%

Q46. For a Black Swan, even if you cannot predict the event type, firms are able to prepare for the impact of the event. Is preparation for a Black Swan event, including those related to AI, cyber or IP risks part of your enterprise risk management approach?	EMEA 2026
Yes	48%
No	49%
Unsure	3%
Total	100%

Part 5. Role & Organisational Characteristics

D1. What level best describes your current position?	EMEA 2026
Senior executive	7%
Vice president	8%
Director	12%
Manager	17%
Supervisor	16%
Associate/staff	19%
Technician	12%
Contractor/consultant	6%
Other	3%
Total	100%

D2. What is the worldwide employee headcount of your company?	EMEA 2026
Less than 500	12%
500 to 1,000	23%
1,001 to 5,000	19%
5,001 to 25,000	17%
25,001 to 75,000	24%
More than 75,000	5%
Total	100%



D3. What best describes your company's industry focus?	EMEA 2026
Communications	
Consumer products	5%
Defense	2%
Education	3%
Energy & utilities	7%
Entertainment & media	4%
Financial services	14%
Healthcare	9%
Hospitality	2%
Industrial	8%
Manufacturing	12%
Pharmaceuticals	6%
Public sector	12%
Retail	3%
Services	
Technology & software	8%
Transportation	5%
Other	
Total	100%

AI experts estimate a varied potential range of AI frequency and severity losses. Geoffrey Hinton, the widely considered “Godfather of AI,” sees two main future possibilities for the relationship between humans and AIs: either AIs take over and humanity goes extinct, or AI amplifies human potential and greatly improves healthcare, education, scientific discovery, productivity, and the economy; it democratizes knowledge, helps address climate change, and enhances standards of living. In Hinton’s dichotomy, avoiding the catastrophe of the former, and realising the benefits of the latter depends heavily on governance, ethical design, and avoiding misuse.²⁷ If Anyone Builds It, Everyone Dies is the title of a September 2025, book by Eliezer Yudkowsky and Nate Soares. The ‘it’ in question is superintelligence/Artificial General Intelligence (“AGI”) built on some form of the current AI paradigm, and the authors very much mean this literally.²⁸ However, the probability of doom (i.e., the probability of catastrophic, human-extinction-level outcomes caused by advanced AGI) referred to by AI computer scientists as p(doom), is not preordained. There are multiple public-private collaboration initiatives that can, and would, if implemented, lower the p(doom) and facilitate AI growth.²⁹ In fact, some AI experts believe that we can lower the p(doom) to effectively zero.³⁰ From an insurance perspective, we need to leverage the best available quantifiable, objective, fact-based information, which means analyse the measurable range of possible outcomes for each AI scenario.

Specifically, we can apply various risk analyzers³¹ to map the frequency and severity of AI-related events across sectors by line of insurance (e.g. Cyber, Property, Casualty and Directors’ & Officers’). Through these lenses, organisations can implement a range of best practices, including maintaining an AI model inventory, quantifying exposures through scenario modelling, conducting end-to-end AI system audits, performing third-party vendor due diligence, implementing unacceptable bias detection and validation testing, defining contractual indemnities, and appointing dedicated governance leads for AI deployment. These practices help translate risk into measurable risk mitigation action. For potential aggregated, correlated, systemic risks, insureds may need to consider alternative risk transfer, such as a captive or catastrophe bonds. In fact, insurance-linked securities are being explored for hyperscale data center risk and the world’s first data center reinsurance treaty has been placed.³² Better access to AI insurance markets translates to lower premiums, which frees up capital for research & development and scaling.

²⁷ Hinton’s collaborators, Ilya Sutskever and Yoshua Bengio, share similar views although their estimates of the p(doom) vary.

²⁸ If any company or group, anywhere on the planet, builds an artificial superintelligence using anything remotely like current techniques, based on anything remotely like the present understanding of AI, then everyone, everywhere on Earth, will die. See Eliezer Yudkowsky, X, <https://x.com/esyudkowsky>.

²⁹ Policy Alert: New U.S. Executive Order on Artificial Intelligence – Aon Tips for Better Risk Capital Decisions.

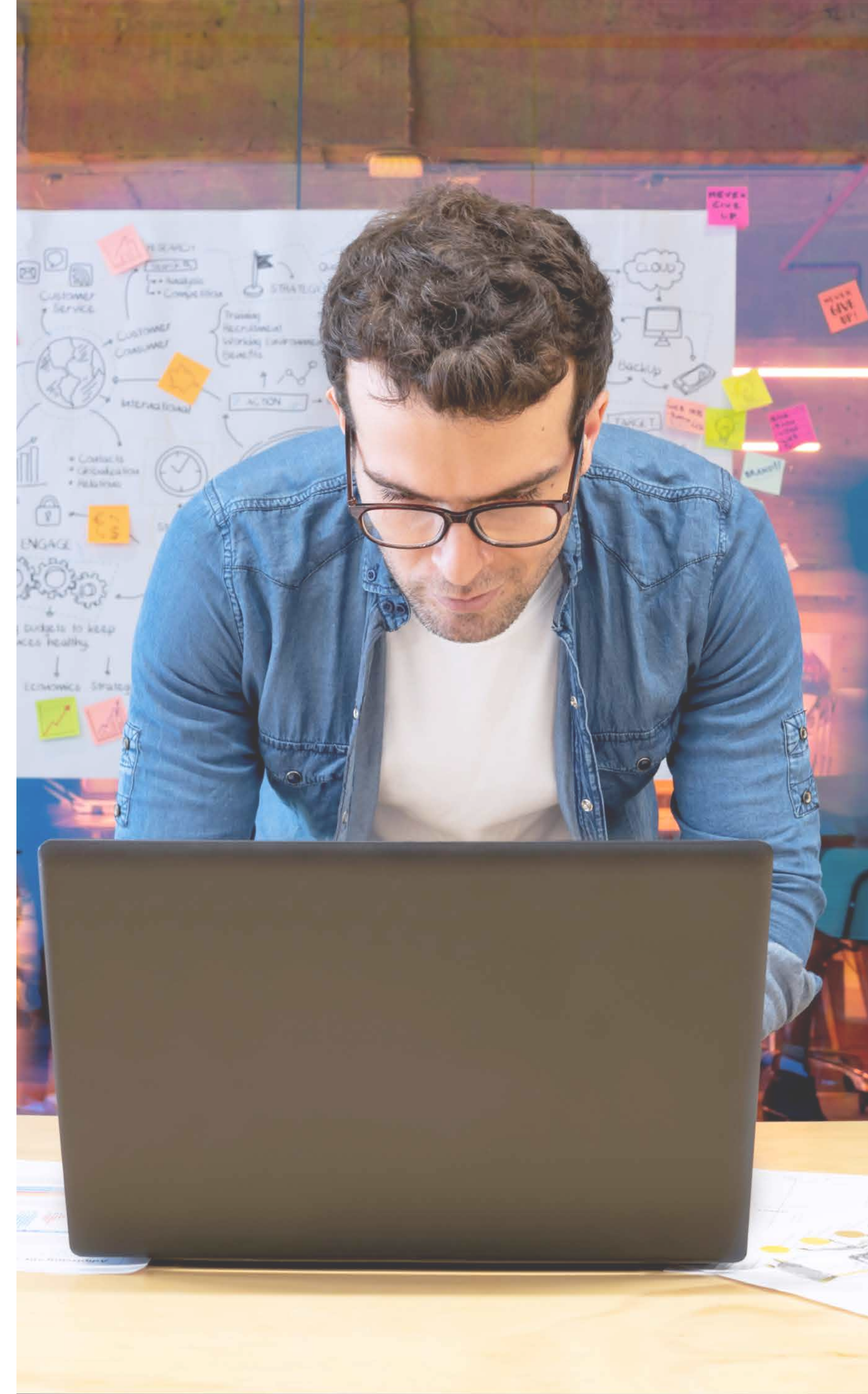
³⁰ Yann LeCun, a prominent AI researcher and Chief AI Scientist at Meta, believes the probability of an AI-caused existential catastrophe is effectively zero. His skepticism about existential AI risk contrasts sharply with the views of others in the field, including fellow Turing Award winner Geoffrey Hinton. See Christopher Mims, This AI Pioneer Thinks AI Is Dumber Than a Cat, Wall St. J. (June 20, 2024) (updated Oct. 11, 2024), <https://www.wsj.com/tech/ai/yann-lecun-ai-meta-aa59e2f5>. Jensen Huang, NVIDIA founder, CEO and President, shares similar views.

³¹ <https://www.aon.com/en/capabilities/risk-analytics/overview/cyber-risk-analyzer>

³² <https://www.reinsurancene.ws/aon-designed-placed-worlds-first-data-centre-reinsurance-treaty-says-ceo-case/>

Done well, this creates the optimal trust-innovation balance point, accelerating AI growth responsibly. Insurance does more than transfer risk; it optimisation, imposes performance standards, and validates operational discipline. If an AI safety implementation is effective at reducing AI risk, then insurers will broaden insurance coverage robustness and adjust premium rates accordingly. This creates a virtuous cycle: good governance leads to better insurability, which in turn supports innovation and insureds' protection. Since artificial intelligence opportunities and perils are dynamic and fluid, insurance underwriting safeguards require constant refining and incentivises behavioural changes. We can scale incremental guardrails to the maturity and criticality of AI applications. For example, higher-risk AI like healthcare, defence and autonomous robotics, such as drones & vehicles should face stricter oversight than low-risk AI like marketing automation. By deploying an iterative risk calibration, insurance underwriters, regulators and organisations can pilot test

AI risk frameworks, observe impacts, and then adjust AI governance in phases. Indicators show when equilibrium is near. Feedback loops (user trust metrics, incident reporting, adoption rates) signal whether risk management is encouraging or choking growth. For example, a rise in AI adoption rates alongside stable risk incidents suggests governance is well-balanced. Conversely, flat AI adoption with rising compliance costs signals over-scrutiny. Technology will remain a defining megatrend for the foreseeable future (along with interconnected megatrends weather, trade and workforce). Organisations that understand their AI perils and risk domains, leverage insurance intelligently, and embed AI into enterprise risk and capital decisions will be better positioned not only to avoid downside, but to capture AI's upside with confidence.



The 2026 Intangible Assets Financial Statement Impact Comparison Report is the sixth intangible assets/cyber risk transfer research paper that examines the comparative values, probable maximum loss and allocation of resources to protect certain tangible assets compared with intangible assets. We thank the following Aon colleagues and industry leaders who assisted Larry Ponemon, Ph.D., founder and chairman, Ponemon Institute, and Susan Jayson, executive director and co-founder, Ponemon Institute, and contributed to these efforts:

Joe Peiser

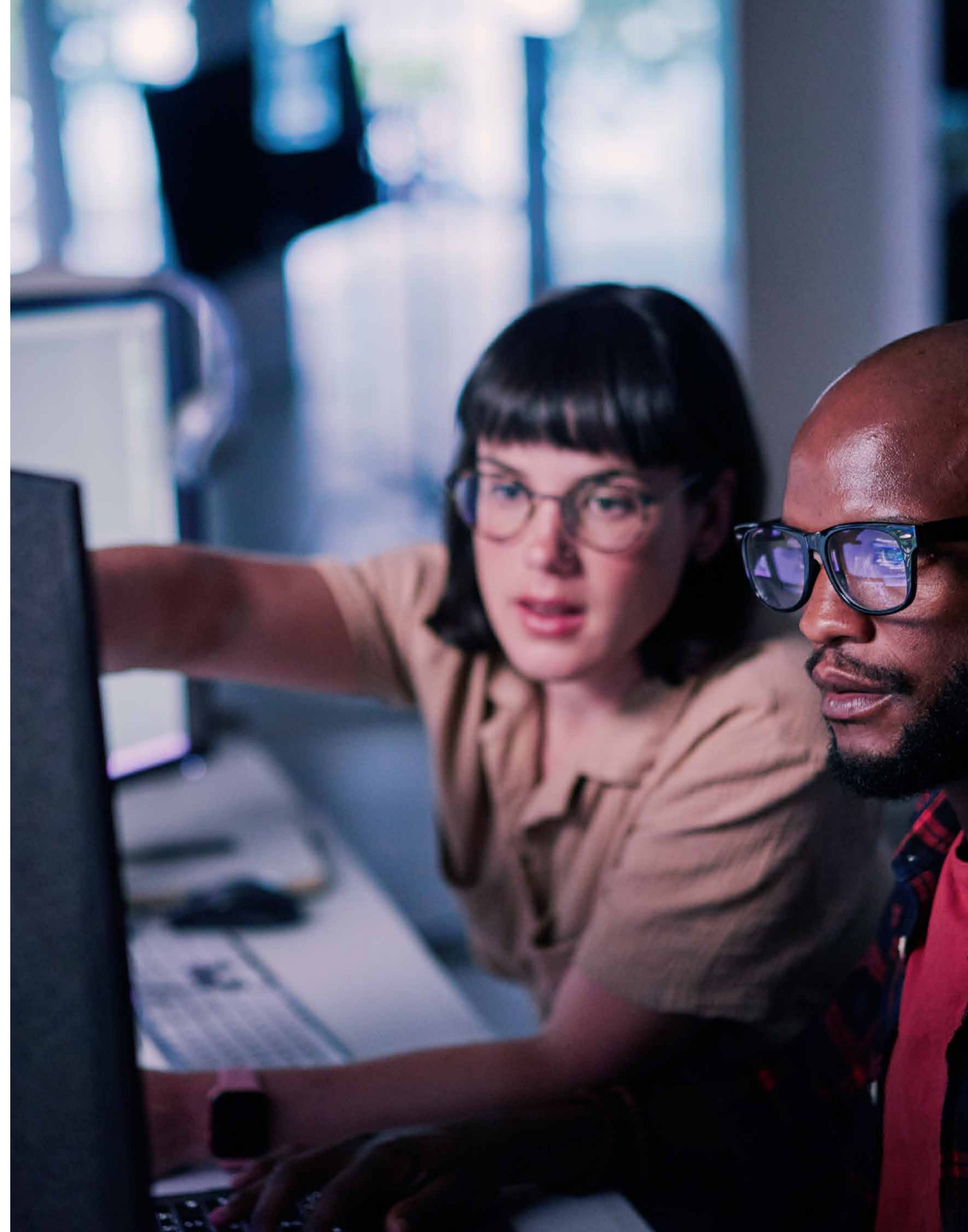
CEO, Risk Capital
Aon

Kevin Kalinich, Esq.

Intangible Assets Global Collaboration Leader
Aon

Jesus Gonzalez

Intangible Assets Global Collaboration Co-Leader
Aon



“

In the immortal words of the fictional HAL 9000 AI supercomputer from 2001: A Space Odyssey: “It can only be attributable to human error.”

“Learn from yesterday, live for today, hope for tomorrow. The important thing is not to stop questioning.”

Albert Einstein



Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organisations.

As a member of the **Council of American Survey Research Organisations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.



About

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Through actionable analytic insight, globally integrated Risk Capital and Human Capital expertise, and locally relevant solutions, our colleagues provide clients in over 120 countries and sovereignties with the clarity and confidence to make better risk and people decisions that help protect and grow their businesses.

Follow Aon on [LinkedIn](#), [X](#), [Facebook](#) and [Instagram](#). Stay up-to-date by visiting Aon's [newsroom](#) and sign up for news alerts [here](#).

©2026 Aon plc. All rights reserved.

Aon has commissioned this report from the Ponemon Institute. Aon has not verified, and cannot accept responsibility for, the accuracy or completeness of any such data, or any conclusions that have been drawn from such data. Aon does not warrant, represent or guarantee the accuracy, adequacy, completeness or fitness for any purpose of the report or any part of it and can accept no liability for any loss incurred

in any way whatsoever by any person who may use or rely on it. This report does not constitute advice, and no person should act on such information without appropriate professional advice after a thorough examination of the particular situation.