beazley

Spotlight on Tech Transformation & Cyber Risk 2025

USA insights

Our research

This year's survey was undertaken between 06.01.25 and 17.01.25

In 2021 the survey was undertaken with respondents based in the UK and US. In 2022 and 2023 the sample base also included respondents based in Canada and Singapore, and in 2024 the sample base was expanded to include respondents in France, Germany and Spain.

beazley

We asked 3,500 business leaders about...

their biggest business risk concerns and how resilient they feel to the following risks...

- Cyber risk
- Technology disruption risk
- Technology obsolescence risk
- Intellectual property risk

We undertook this research in January 2025 with global business leaders (insurance buyers), from across these different industry sectors:

- Healthcare & Life Sciences
- Manufacturing, Retail, Wholesale and Food & Beverage
- Commercial Property, Real Estate and Construction
- Hospitality, Entertainment and Leisure (including Gaming)
- Financial Institutions and Professional Services
- Energy and Utilities (including Mining), Marine and Warehousing
- Public Sector and Education
- Tech, Media and Telecoms
- Transportation, Logistics, Cargo and Aviation

Perception

Cyber and tech risk concern is rising, but executives feel more prepared for these risks.

Reality

Many firms may be exposed and unprepared for fast-evolving digital threats.

Global businesses face a **'whack-a-mole'** of cyber and tech risks that demand vigilant, continuous risk management.

Businesses need help employing **defence in depth** strategies to boost their resilience.

31%

Selected cyber risks as their greatest threat this year, up from 22% in 2024. Despite this, 81% feel prepared* to deal with these risks, up from 73% in 2024.

74%

Agreed their business is planning to improve its cyber security with its third-party suppliers following high-profile systemic cyber incidents.

37%

Plan to invest in improved cyber security this year, up from 27% in 2024.

79%

Agreed that AI will have a positive impact on their business' economic prospects this year, while 71% agreed that AI will replace jobs in their company over the next 18 months.

21%

Ranked tech obsolescence risk as their top cyber & tech threat this year, compared with 27% in 2024.

21%

Ranked IP risk as their greatest threat this year – down from 29% 2024. At the same time, their sense of resilience to this risk has increased with just 17% feeling unprepared** compared to 28% in 2024.

beazley

* Very and moderately prepared answers combined.
** Not very well and not at all prepared answers combined.

What the data reveals

- Many firms still overestimate their resilience to cyber & tech risk.
- There are many organisations underprepared for a cyber or data breach incident.
- Firms are looking to improve their cyber security.
- Optimism around the business benefits of AI is growing.
- Perception around tech obsolescence and IP risk resilience is rising.

Report takeaways

For brokers

1. **Cyber resilience is more than insurance cover**
Businesses need layered cyber security and pre-emptive, responsive and adaptive support to help them pre, during and post a cyber incident, in addition to just buying cyber security insurance.

2. **First and third-party liability**
Today's tech interconnectivity creates supplier vulnerabilities resulting in both first and third-party liability, ranging from cyber risk and business interruption to D&O claims and loss of reputation.

3. **Political tensions increase cyber risk**
As geopolitical tensions rise and relationships shift, so too does cyber risk, as nation state threat actors create new vulnerabilities that cyber criminals can exploit.

For business leaders

1. **A growing concern for shareholders**
As cyber risk grows so too does the risk of disruption and reputational harm. Poor cyber security decisions now face greater scrutiny, exposing firms to legal, financial & operational consequences.

2. **All eyes on IP and data privacy**
National IP and data privacy regulations are fragmented and create risks for firms operating internationally who might inadvertently fall foul of new legislation. Yet concern over IP risk is dropping.

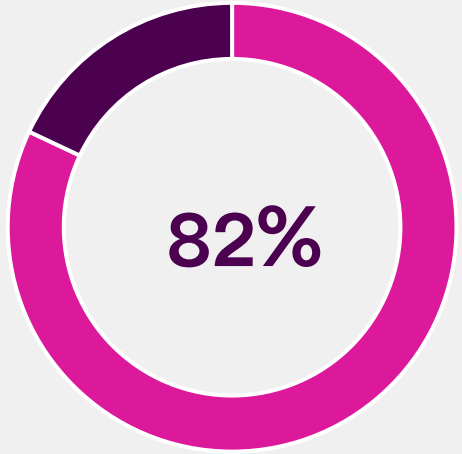
3. **Harnessing the power of AI**
With **43%** of US-based executives planning to invest in new technologies this year, and **71%** anticipating AI-induced job losses in the next 18 months, firms need to stay alert to best practice and evolving AI-related risks.

The Cyber Security Mirage

Global businesses face a ‘whack-a-mole’ of cyber and tech risks

Vulnerable connections

- Third party supplier cyber risk is escalating, as supply chains become interconnected and increasing vulnerability to cyber attacks.
- Cyber criminals target larger firms through smaller suppliers who may lack the resources to maintain robust cyber security.
- Outsourcing cyber security can create a false sense of security, and it doesn't eliminate the need for:
  - Active employee training
  - Business continuity planning
  - Maintaining internal best practices
  - Defence in depth cyber security



of US-based executives agreed that their business is planning to improve its cyber security with its third-party suppliers following recent high profile systemic cyber incidents.

The Cyber Security Mirage

Nation state actors are using cyber as a form of cyber warfare, and AI is making cyber criminals more effective

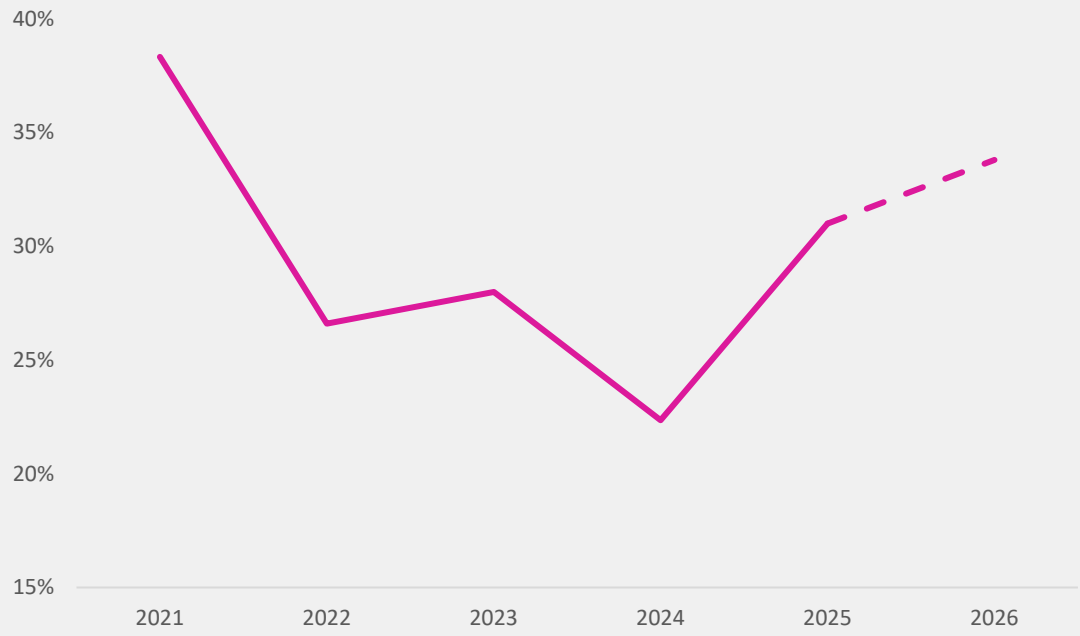
The intersection of politics and cyber security

- Cyber attacks are now tools of hybrid warfare, used to create disruption and apply political pressure.
- Hacktivists use cyber attacks to push agendas, often lingering in systems and posing a long-term threat.

Ransomware evolution

- The rise of Edge devices and IoT is giving cyber criminals new entry points into systems.
- AI is helping cyber criminals to automate attacks, enhance phishing and create more convincing deepfakes.

Concern around cyber risk over time



The percentage of US-based executives who ranked cyber risk - company failure to ensure data privacy or external criminal threat including ransomware or broader systemic threat generating severe business interruption – as their top cyber & technology risk over time. The 2026 figures is a prediction of the top risk concern in 12 months' time.

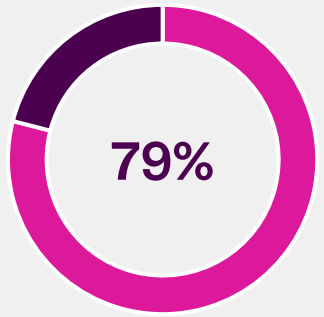
beazley

Tech Transformation – from code to cognition

AI is forcing businesses to balance its benefits with the need for strong safeguards against emerging risks

Risk and reward

- AI optimism is surging. Today, the risk of underinvesting in AI outweighs the risk of overinvesting.
- Human oversight is essential to mitigate risks such as copyright infringement, intellectual property violation, bias and defamation.

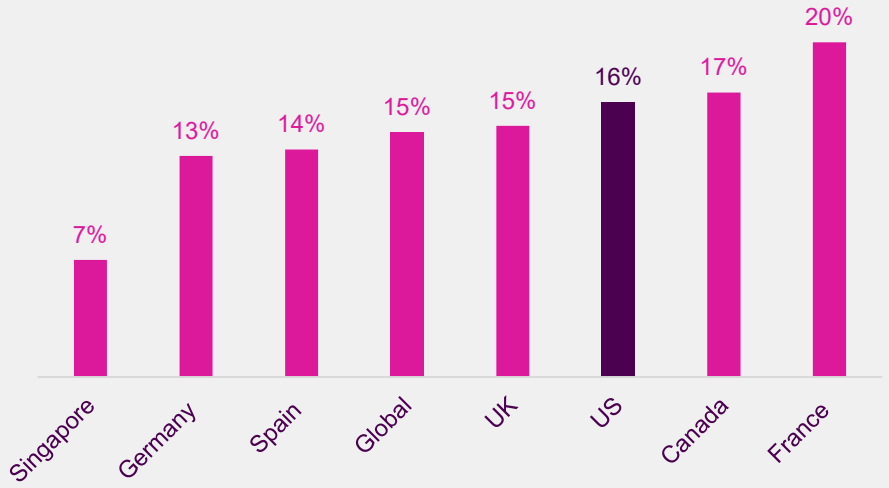


of US-based executives agreed that AI will have a positive impact on their business' economic prospects this year.

Outdated tech

- AI raises concerns about tech obsolescence, disruption and declining competitiveness.

Tech obsolescence preparation varies by region



The percentage of executives who feel unprepared ('not very well' and 'not at all' prepared answers combined) to anticipate and respond to tech obsolescence risk – the failure to keep pace with changing technology development and opportunities (e.g. Generative AI, IoT and automation); failure to update systems – as their top cyber & technology risk by region.

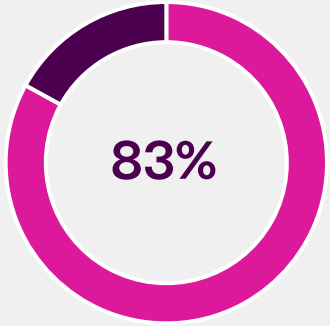
beazley

Secured or Exposed – IP & data privacy

Protecting data and ensuring the security of intellectual property has become increasingly important

Lurking risks

- Rules around AI and copyright are still unclear, and the risk of theft of existing IP is significant.



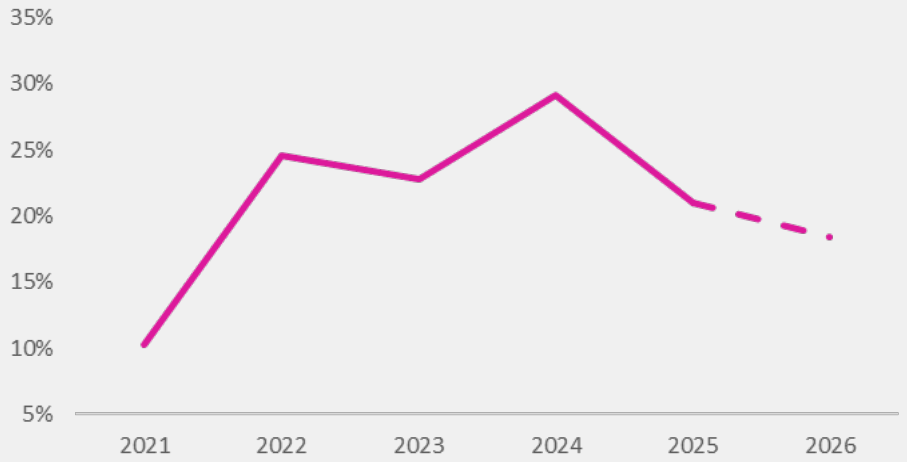
of US-based executives have a blind spot around IP risk, with concern dropping, but perception of preparedness is up from 70% in 2024.

Regulatory labyrinth

- New national regulations to counter risks around data privacy and IP, are creating additional complexity for international businesses.

- As geopolitical tensions endure, organisations are at risk of IP theft and data breaches from hostile governments.

Concern around IP risk falls



The percentage of US-based executives who ranked intellectual property risk – the failure to recognise and protect the value of intellectual property assets such as know-how, patents or intangible assets – as their top cyber & technology risk over time. The 2026 figures is a prediction of their top risk concern in 12 months' time.

beazley

Building resilience

The need for a multi-layered, defence in depth approach to cyber security has never been greater

Walls within walls

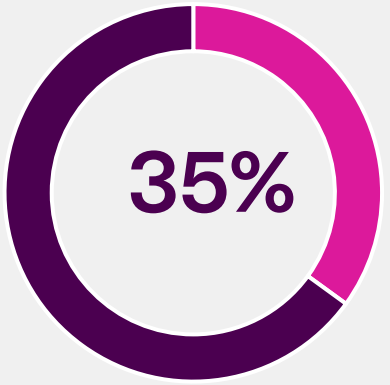
- Ensuring multiple layers of defence to restrict access to systems and data is critical.
- Organisations need a tailored, defence in depth strategy that reflects their unique supply chain and risk profile.

Third party threat

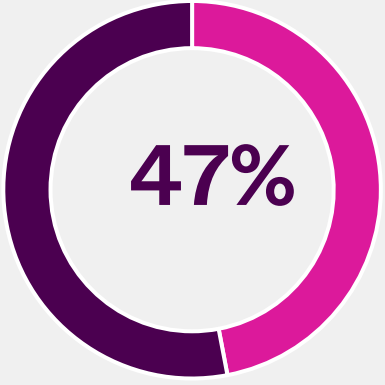
- Vendor contracts can cap liability, leaving firms to shoulder the legal fallout and the financial hit from third party attacks and disruptions.

Improving cyber hygiene

- Good cyber security includes a pre-emptive, responsive and adaptive approach to cyber risk mitigation.
- Investment in cyber security can help make an incident less likely as most cyber criminals are looking for the path of least resistance.



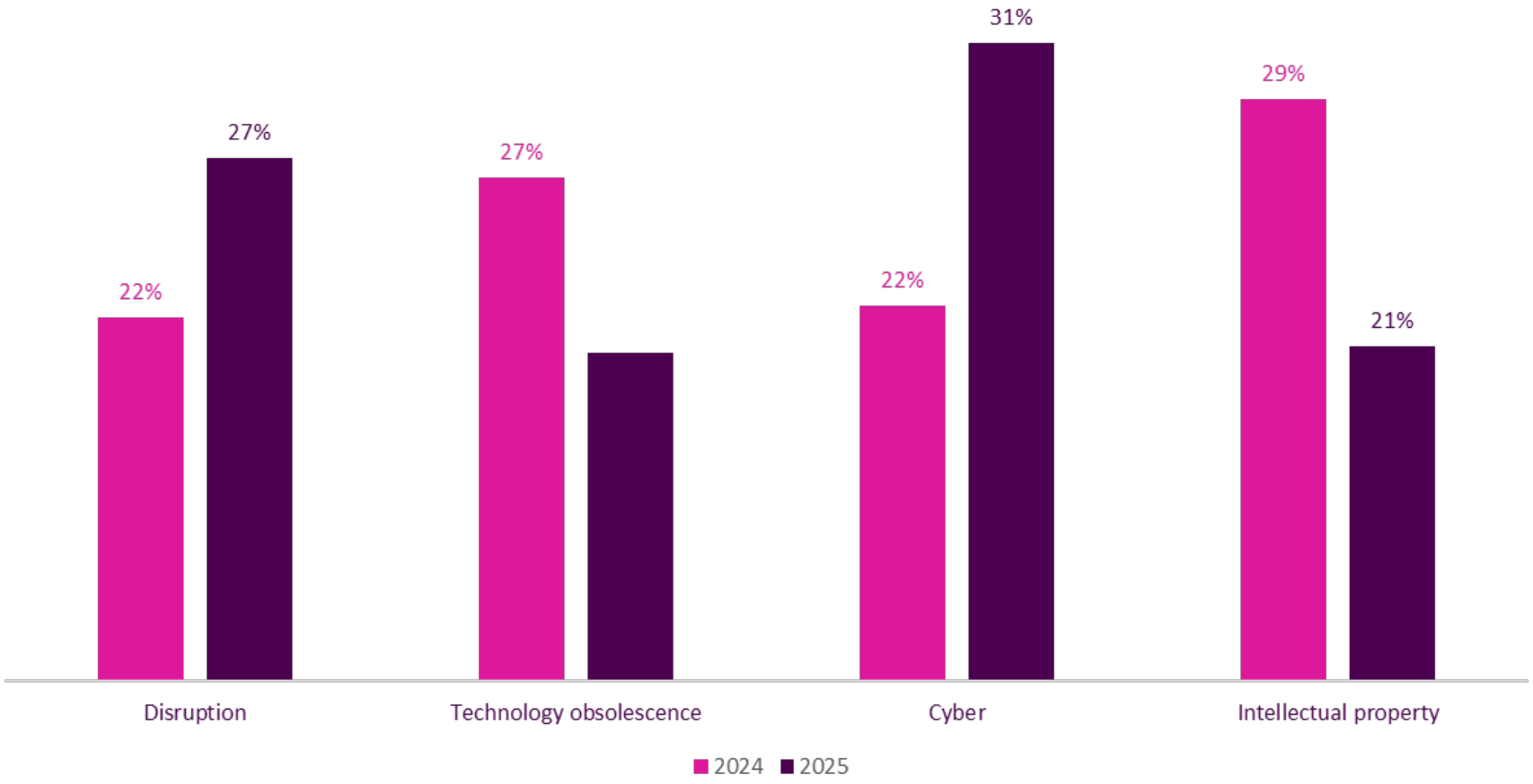
of US-based executives plan to explore insurance options this year, including risk and crisis management.



of US-based executives say their trust in the value of insurance has increased.

beazley

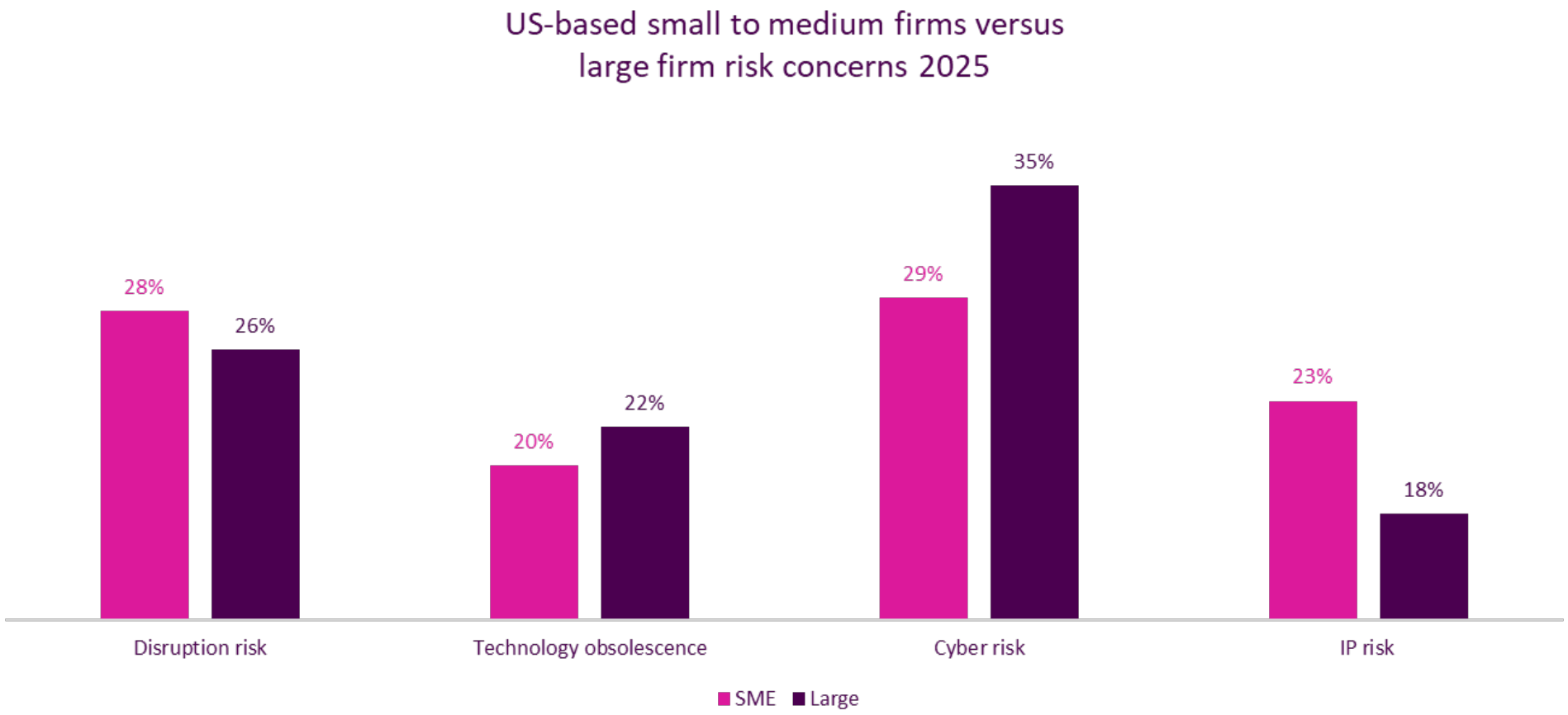
Cyber & Technology USA risk ranking



Percentage of US-based executives that ranked these cyber & tech risks as their top concern in 2024 and 2025.

beazley

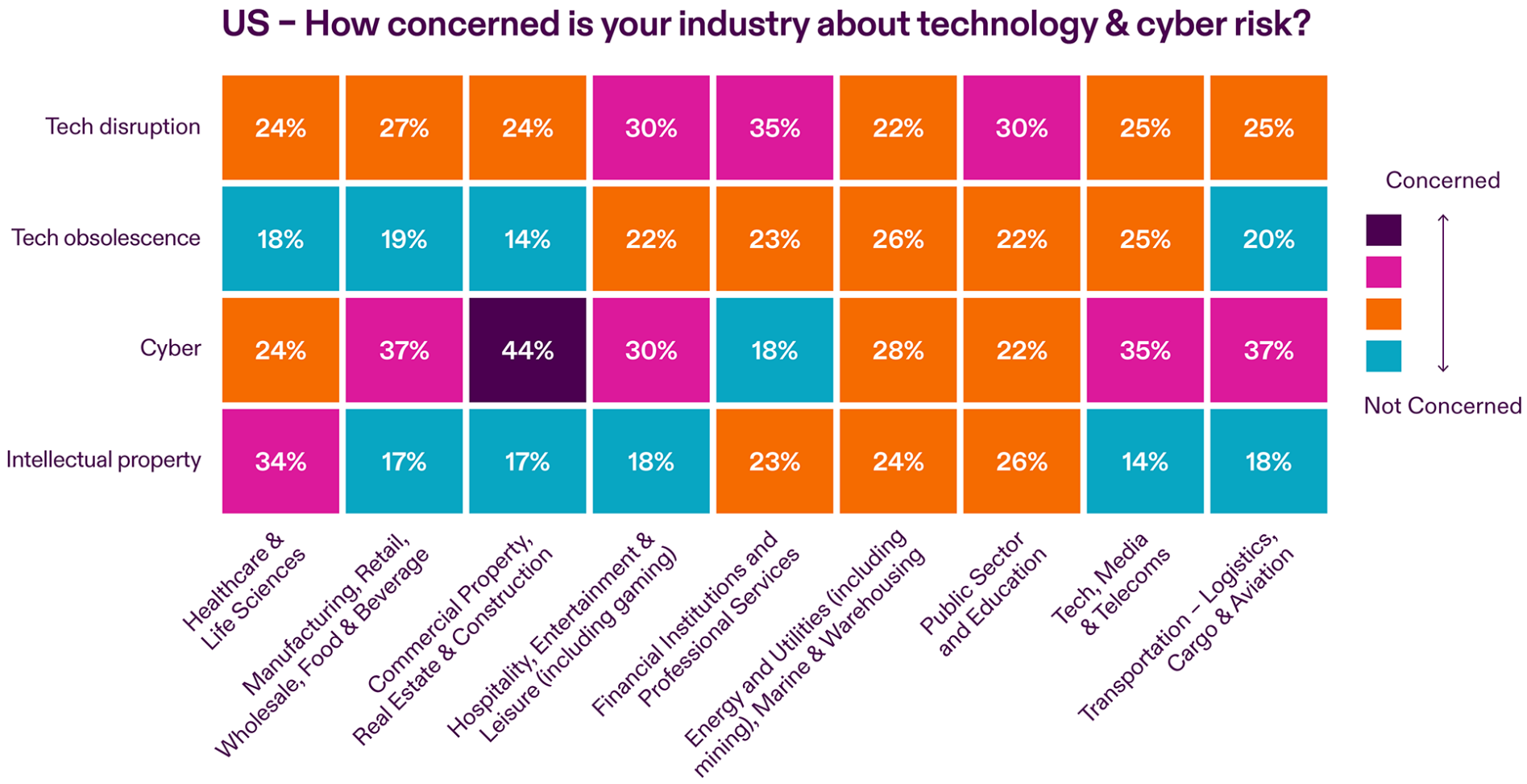
Cyber & Technology Risk Concerns



beazley

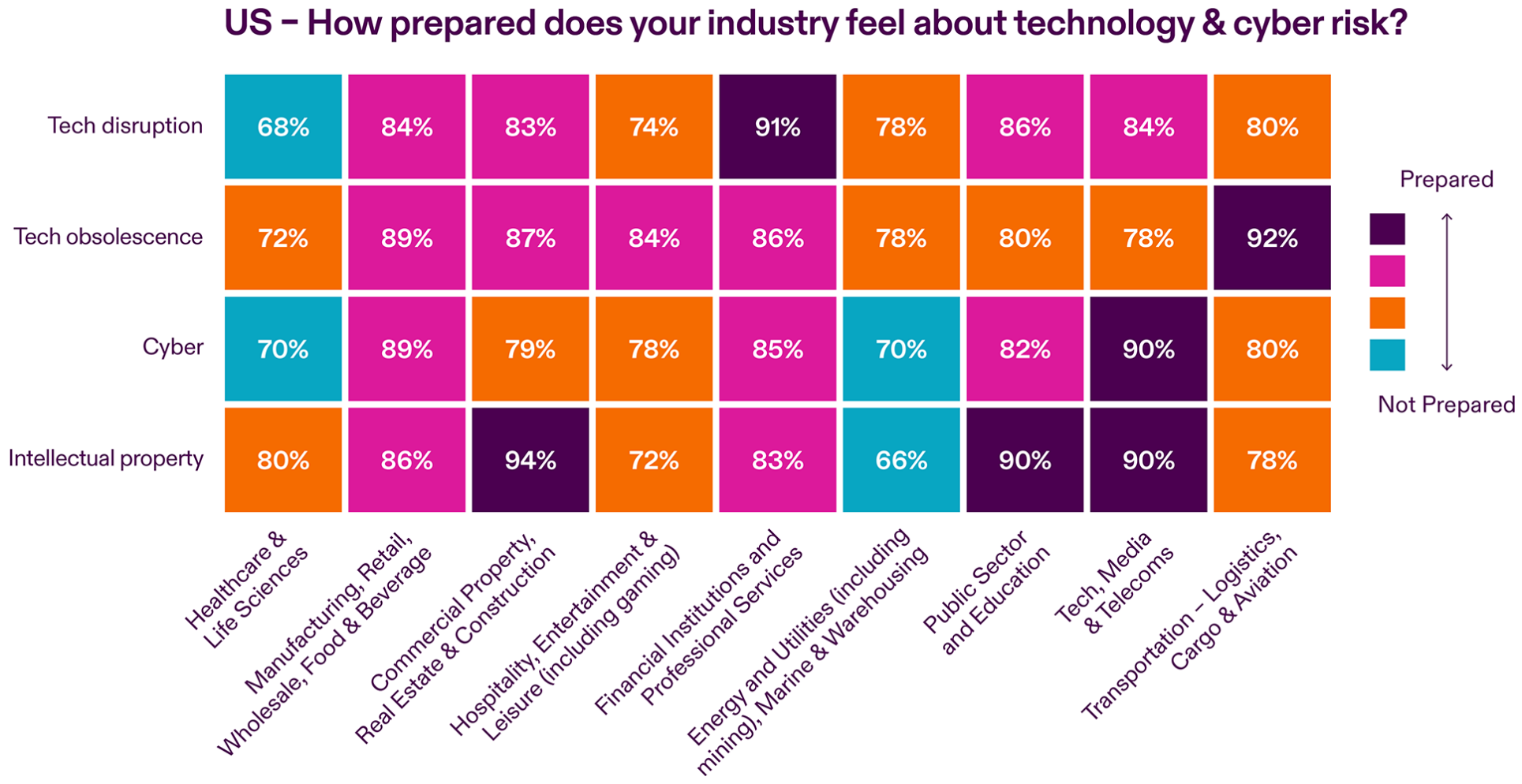
Percentage of US-based executives from SME firms (US$250k-99.99m annual revenue) and large firms (US$100m+ annual revenue) who ranked these cyber & tech risks as their top risk concerns.

USA Industry Risk Heatmap



The percentage of US-based executives ranking these cyber & tech risks as their top risk concern in our 2025/26 Risk & Resilience survey.

USA Industry Resilience Heatmap



beazley

The percentage of US-based executives who feel 'prepared' (very and moderately prepared responses combined) for these cyber & tech risks in our 2025/6 Risk & Resilience survey.

beazley

Beazley plc (BEZ.L) is the parent company of specialist insurance businesses with operations in Europe, United States, Canada, Latin America and Asia. Beazley manages seven Lloyd's syndicates and, in 2023, underwrote gross premiums worldwide of $5,601.4m. All Lloyd's syndicates are rated A by A.M. Best.

Beazley's underwriters in the United States focus on writing a range of specialist insurance products. In the admitted market, coverage is provided by Beazley Insurance Company, Inc., an A.M. Best A rated carrier licensed in all 50 states. In the surplus lines market, coverage is provided by Beazley Excess and Surplus Insurance, Inc. and the Beazley syndicates at Lloyd's. Beazley's European insurance company, Beazley Insurance dac, is regulated by the Central Bank of Ireland and is A rated by A.M. Best and A+ by Fitch.

Beazley is a market leader in many of its chosen lines, which include professional indemnity, cyber, property, marine, reinsurance, accident and life, and political risks and contingency business.

For more information, please go to: beazley.com