

Resetting risk management priorities

Global Technology Industry Risk Study 2023



Contents



Foreword

After more than a decade of strong growth, the technology industry is going through a reset, triggered mainly by shifting economic realities.

Global economies are slowing, and access to capital is pausing as investors assess the economic landscape. Supply chain issues are affecting hardware sales, and tech companies are announcing layoffs at levels not seen in 20 years.

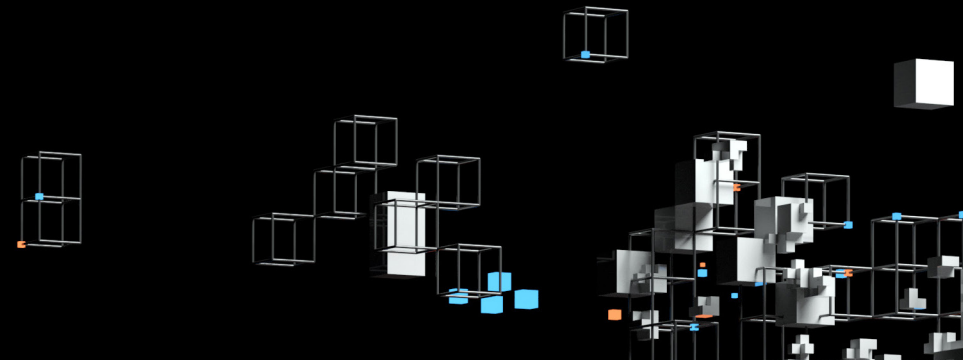
Our *Global Technology Industry Risk Study 2023* shows how economic uncertainty is affecting risk management at technology companies as they focus on resetting priorities to respond to existing and emerging risks.

To understand technology companies' responses to global economic uncertainty, we surveyed over 300 risk management leaders from 29 countries across six continents. We thank all of our respondents for taking the time to answer our questions.

We hope this year's study helps you better understand how your peers view the changing risks affecting the technology industry, and provides guidance on how to better manage those risks going forward. We will discuss the findings in this study at Marsh events throughout 2023 and we hope you are able to join us for a deeper dive into these important issues.



TOM QUIGLEY
US Technology Industry Practice Leader
tom.quigley@marsh.com

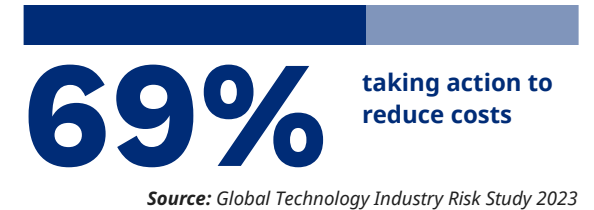


Economic slowdown challenging tech growth

The ever-increasing reliance on technology and connectivity has propelled tremendous growth in the tech industry. But as countries recovered from the COVID-19 pandemic, 2022 brought new challenges. Record rates of inflation, interest rate hikes, and the prospect of a global recession now threaten the tech industry's continued growth. Global information technology spending is forecast to have grown less than 1% in 2022, down from 10.2% the previous year.

With capital markets largely paused as they keep a close watch on economic indicators, many tech startups face the prospect of stalled growth. Even established firms are looking closely at expenses and signaling a slowdown. Many major tech companies recently reduced their workforces through headline-grabbing layoffs, while others adjusted their 2023 growth goals downward and indicated they will reduce or freeze hiring.

Valuations also declined significantly as the overall market became more volatile. Deal volumes went down by more than 20% in the third quarter of 2022; median deal sizes declined by close to 30%, with late-stage deals seeing the sharpest decline, almost 50%.



Economic environment leading to cost cutting measures, including layoffs

Demand for tech products shot up during the pandemic as lockdowns forced an increased dependence on technology for both businesses and individuals. But the reopening of societies and increased in-person interactions has softened demand. Further, supply chain disruptions have continued plaguing the industry, at times impacting production levels.

More than 80% of respondents to the *Global Technology Risk Study 2023* indicated that their company is taking action to counter the effects of global economic uncertainty. Cost reduction initiatives, such as administrative and operational cuts, were the most common actions, taken by almost 70% of respondents (see Figure 1). And close to half said their companies have implemented workforce reductions or slowed hiring. Both actions can have a significant impact on risk management and insurance budgets.

Note that the more than 300 survey respondents cited 27 different business models and combinations of those models (see Figure 12), indicating that although their products and services may differ, they face similar risks and challenges.

Despite the continued headwinds moving into 2023, there is still optimism for the new year. Spending is expected to rebound and grow by just over 5% this year. While still far from 2021's double-digit growth, the increase signals the potential start of recovery.

It is important to note that the increasing reliance on technology enables every other industry to grow and innovate. From the use of chips in automobiles to AI-enabled factories to new payment solutions for retailers to expanding sharing economy business models, nearly every company will continue to leverage technology and develop new solutions.

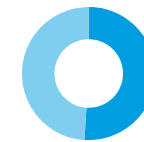
01| Most tech companies cutting costs

To what extent has the economic slowdown/uncertainty led your company to consider the following? Select all that apply.



69%

Direct cost reduction initiatives (administrative, operational)



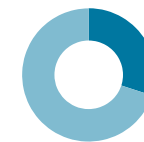
51%

Preservation of capital and rethinking our ability to retain risk



46%

Reduction in workforce or slowdown in hiring



30%

Reevaluation of sources of risk capital to fund losses



17%

None of these

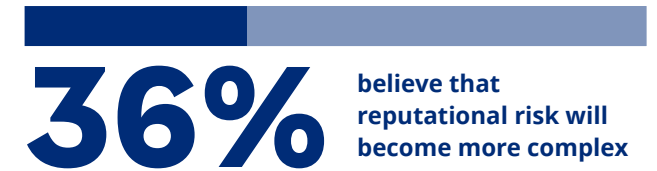
Source: *Global Technology Industry Risk Study 2023*

Reliability and security remain top worries, but reputational risk emerging as a major concern

Maintaining reliable and secure networks remains the biggest challenge for technology companies (see Figure 2). The top three risks in this year's report — data security and privacy, digital business interruption, and technology errors and omissions — have consistently ranked as top risks for all nine years of this report. IT resilience, which is closely linked to the top three risks, remained in the top 5, the same as last year.

But survey respondents have expressed a deepening worry about reputational risk. Ranked tenth in 2022, nearly half of respondents this year cited reputational risk as a major concern, pushing it up to the fourth spot. This could be a result of the growth of technology companies, many of which have become household names, which results in business practices or any mishaps being heavily publicized and scrutinized.

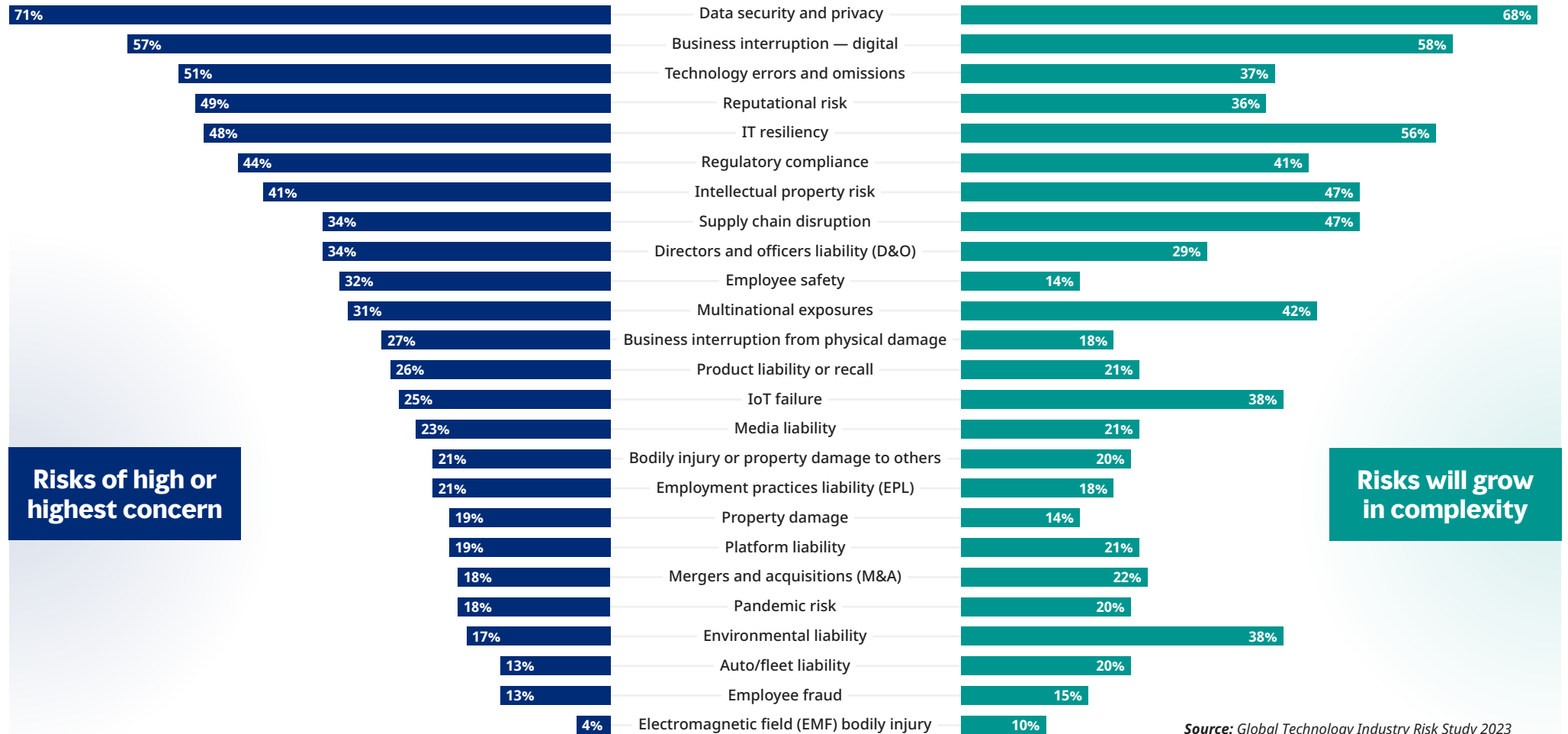
There is also increased recognition that a company's reputation is not threatened only by product or platform problems, such as a data security, a system outage, or a coding error. As they take their place among the largest and most well-known companies, other factors — including human rights issues within the supply chain, cultural issues at the workplace, data collection and use, workforce disputes, and executive compensation controversies — can negatively impact the reputation of tech companies. This reputational risk can lead to loss of customers as they seek products from other companies, drops in revenue, new or more stringent regulations, and an adjustment in growth trajectory.



Source: Global Technology Industry Risk Study 2023

02| Technology risks remain top concerns

How do you view the following risks to your business? How do you view the following risks changing in the next three to five years?



Risks of high or highest concern

Risks will grow in complexity

People risks may complicate existing challenges

46%

are reducing their workforce or slowing down hiring

Source: Global Technology Industry Risk Study 2023

Safeguarding business continuity through securing data, keeping systems online, and ensuring that computer code functions properly is top of mind for tech companies. But this would not be possible without the highly skilled tech employees — from cloud security specialists and security operations to programmers and web developers — who work to keep systems running efficiently and effectively.

The importance of a strong workforce is highlighted in our survey data. While technology is often thought of as automated, technical, and operating within a sterile environment, more than two-thirds of survey respondents said that workforce and employee risk factors contributed to each of the top five risks.

This comes at a time when close to half of respondents indicated that their organizations are either implementing layoffs or slowing down hiring in response to difficult economic conditions (see Figure 1).

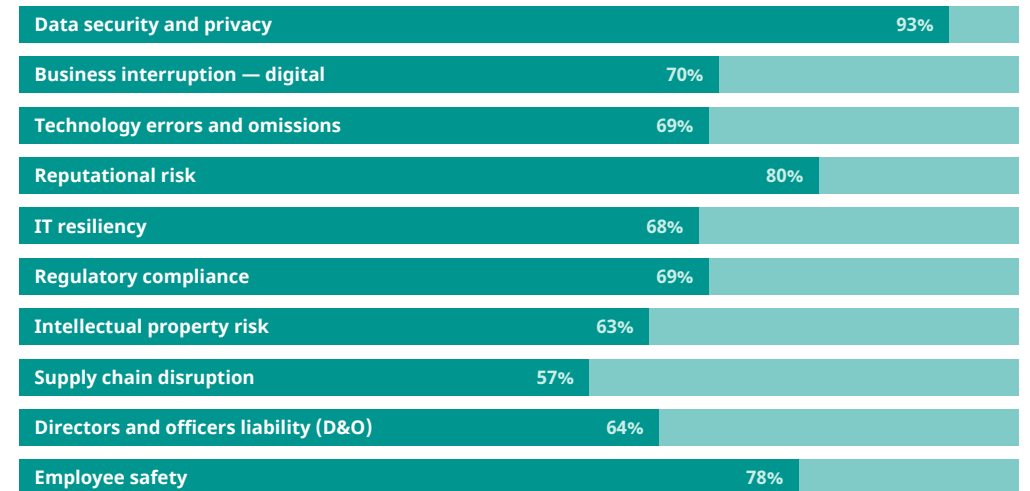
A tighter workforce and job security concerns can have a significant impact on operations and potentially exacerbate existing and emerging risks (see Figure 3). Aside from potentially slowing down production, delaying the release of new products or services, and slowing sales of current offerings, a stretched or distracted workforce can heighten cybersecurity risks. In the year ending April 2022 there were more than [714,000](#) job openings for cybersecurity roles or skills posted in the US. The global shortage is believed to be [3.4 million](#).

Human error, for example, is a [major contributor](#) to cyber breaches, and believed to be the root cause of the vast majority of cybersecurity breaches. Mercer's [People Risks 2022](#) report found that cybersecurity and data privacy is the top people risk for communications, media, and technology companies. Workers who are stretched with more responsibilities, including covering for colleagues who have been laid off or resigned, are more likely to make a mistake, increasing the overall risk.

This has contributed to burnout and in turn more resignations. In one survey of cybersecurity professionals, [66%](#) said they experienced more burnout through 2022.

03| Workforce challenges contribute to top risks

To what extent do workforce/employee risk factors contribute to the following risks?



Source: Global Technology Industry Risk Study 2023

Addressing the talent gap

Tech companies should mitigate their people risks by focusing on a three-pronged strategy of retention, attraction, and training. This process begins with determining what employees want and need. Or, more simply, understanding why they join a company and what encourages them to stay. This key data needs to be collected and updated regularly within a company for accountability purposes.



Talent retention

- Create effective compensation and total rewards packages. Consider offering spot bonuses based on tenure or skills, get creative with remote work, or offer a four-day workweek, in addition to delivering on total well-being.
- Understand what employees value and align this with a business purpose that highlights meaningful work. Burnout can be reduced with increased engagement, flexibility, and career opportunities, like on-demand training.
- Deliver and reimagine total well-being by reviewing healthcare affordability, mental health support, and wealth and retirement planning.



Talent attraction

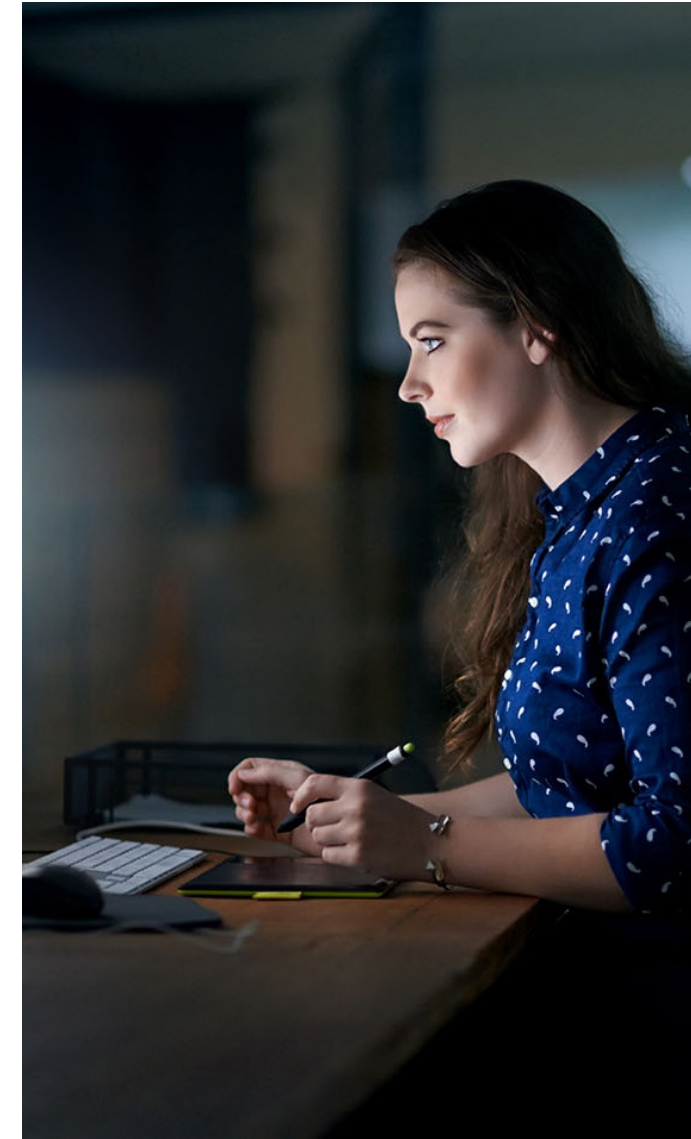
- Focus on the candidate experience and streamline the application process to make hiring decisions more quickly, or implement an employee referral program.
- Establish and deploy pay equity standards, including pay transparency.



Training

- [Ninety-eight percent](#) of HR professionals say their company has significant skills gaps. Map existing skills with future business needs to understand the talent landscape. Address potential gaps through training, especially for cybersecurity professionals and in-demand tech skills.
- Accelerate personalized career path mapping, on-demand and learning and development opportunities during work hours, as well as mentorship programs.

Tenure is the [largest human capital management driver](#) of a company's financial and operational performance. Investing in the workforce through talent retention, attraction, and training can help address a critical skills gap and create a robust workforce, which is an essential factor in sustained growth for technology companies.



Development of new offerings persevering despite difficult economic conditions

60%

of companies are marketing new uses for existing products or services

Source: Global Technology Industry Risk Study 2023

Despite potential staffing shortages and pressure to cut costs, technology companies are cognizant of the need to forge ahead with innovative product and service offerings to grow revenue. The vast majority of survey respondents (see Figure 4) said their companies are developing new products or developing new relationships to expand revenue.

But innovation can also bring new risks. Autonomous vehicles (read more on page 15), for example, may lead to injuries for both the vehicle occupant and others, as well as property damage. And the metaverse may lead to the potential for bodily injury when using AR headsets or haptics, while the absence regulatory clarity may exacerbate the risks it presents (read more on page 11).

Tech companies may also face evolving risks when introducing fresh uses for existing products and services, which 60% of survey respondents said they are doing. These may include embedding off-the-shelf integrated circuits into new products, adding new services to existing platforms, or expanding payment options into existing applications.

Although tech risk leaders have years of experience identifying, measuring, and mitigating the risks of their products in traditional technology business models, different uses can change the risk. This requires tech risk leaders to look beyond traditional technology risk benchmarks to fully understand the expanded risk profiles of their products or services. Increasingly, tech companies should revisit traditional business risk profiles to understand how they can be adjusted to fit their tech-enabled business models.

04| Products and services development ongoing despite economic challenges

How is your company expanding its products/service offerings? Select all that apply.

Developing new products and services

82%

Selling existing products or services to be used in new ways

60%

Partnering with other technology companies

54%

Mergers or acquisitions

48%

Partnering with non-technology companies

25%

We are not doing anything new or different

6%

Not sure

1%

RISK FOCUS: METAVERSE

Beyond play: As the metaverse evolves, beware of new risks



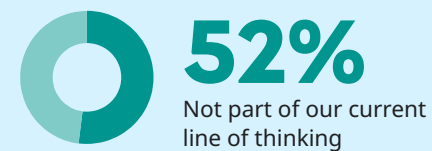
The “metaverse” refers to an emerging new reality where our life, work, and play are traversing physical and digital realms in a seamless, immersive way.

Today’s connected world has opened new opportunities for businesses and individuals. The emergence of immersive experiences, such as the metaverse, are taking connectivity to a new level. As technologies — including advances in connectivity speeds, 3D reconstruction, artificial intelligence, and augmented or virtual reality — advance, the metaverse is providing new ways to engage users, explore new places, and conduct business.

While more than half of our survey respondents said operations in the metaverse are not currently on their agenda (see Figure 5), the global metaverse is growing steadily, with revenue projected to [approach \\$800 billion](#) by 2024.

05| Metaverse adoption still low, but opportunities are being explored

Is your company operating in or exploring opportunities related to extended reality, from augmented reality to the metaverse?



Source: Global Technology Industry Risk Study 2023

ENGAGING THE METAVERSE

Several companies are exploring commercial opportunities in the metaverse in three main ways:

- 1. Establishing a commercial presence.** Many organizations are purchasing digital real estate and “setting up shop” on metaverse platforms where their customers and employees can convene virtually, whether to work, shop, or otherwise engage.
- 2. Launching fully digital products.** Digital assets such as non-fungible tokens (NFTs) are being sold and bought as end products in and of themselves. Sometimes, NFTs can also serve as passports to unlock physical world features, such as exclusive physical collector items or in-person membership benefits.
- 3. Creating digital twins of physical items.** Metaverse technologies can help create digital replicas of existing physical products and processes, ranging from apparel to buildings to supply chains. Digital twins can help proactively identify and mitigate potential issues with physical products and processes. Manufacturers, for example, can leverage digital twins to have a real-time view into their supply chains to identify potential problems with sourced components.

RISK FOCUS: METAVERSE

Largely unregulated space raises new risk questions

The opportunities in the metaverse are enormous, from allowing customers to virtually try on clothes to use in human or avatar form, to providing more immersive customer service experiences, to improving the reach and delivery of education, to leveraging AR technology to increase access to healthcare. And as AR/VR headsets and haptic wearables become more technologically developed and more affordable, adoption of the metaverse is likely to become more widespread.

But organizations that have already established or are considering establishing a presence in the metaverse — as are more than a third of our survey respondents — need to think beyond the opportunities and consider the fast-evolving set of risks.

While some risks are familiar, such as those related to e-commerce and the potential of a cyber event, others are less straightforward. For example, while only one-fifth of our survey respondents listed bodily injury as a risk of high concern, today there is limited data showing the potential longer term health implications arising from prolonged use of VR headsets. There may also be physical injury risks if haptic wearables malfunction.

Additionally, the current lack of regulatory clarity leads to significant questions about liabilities. For example, how is property defined in a virtual environment? And with many transactions taking place using cryptocurrencies, insurance coverage for potential losses is still being put to the test.

Further, there are questions about the regulatory oversight of assets in immersive environments. For example, who is responsible and under which jurisdiction if a client's avatar is assaulted by a malicious third-party actor inside a company's virtual store that operates on a decentralized metaverse platform? Organizations need to stay on top of the latest regulations and be aware of the potential reputational and legal repercussions of operating in the metaverse.

3 actions to mitigate metaverse risks

As organizations explore augmented reality and immersive opportunities within the metaverse, they should consider taking the following actions:



Stay abreast of **regulatory developments** to determine potential responsibilities and learn from emerging cases that may **establish liability trends**. It is critical to closely follow regulatory classifications that may impact the use of the metaverse or digital currencies used to buy and sell items in the metaverse.



Be clear about the **geographical jurisdiction** that applies. Understand that users in different parts of the world may be protected by different types of laws. This is especially important when considering **data privacy laws**, which have historically depended significantly on geographical location.



Keep up with **emerging technologies** that can impact metaverse adoption. As **headsets, haptic wearables**, and other technologies become more affordable and user-friendly, the number of customers that can access metaverse platforms is expected to grow. But **metaverse-related risks** will also increase.

Exploration of the metaverse has only begun. The potential for growth is immense, as are the potential opportunities for organizations. As they explore these opportunities, businesses should not lose sight of potential risks, both existing and emerging.

RISK FOCUS: DIGITAL ASSETS

Proceed with caution: Digital assets bring both new and established risks



Cryptocurrency is a double-edged sword: Not relying on financial institutions or governments allows for faster and cheaper transactions (due to no transaction fees); however, there is also no government obligation to step in if there is fraudulent activity.

Digital assets continue to generate significant market interest, with [one in five Americans](#) having invested in, traded, or used cryptocurrencies, and [NFT ownership doubling over the past year](#). Cryptocurrency is seen as having many benefits over fiat money, such as increased transaction speed, security, privacy, transparency, and diversification. Retailers are responding to perceived customer interest; [one report](#) shows that 46% of merchants and 85% of big retailers in the US currently accept cryptocurrency payments.

Additionally, digital assets and their underlying blockchain technology may offer individuals and companies the potential to avoid using traditional banks, trade around the clock, and minimize the effects of inflation. However, they are not without risks.

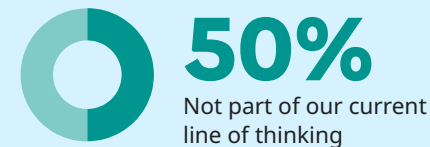
A volatile market requires adequate protection

Digital asset values are extremely volatile, making them high-risk investments. A market valued around \$3 trillion in November 2021 [dropped to under \\$900 billion](#) at the end of 2022. They are also prone to fraud; between January 1, 2021 and March 31, 2022, [over 46,000 people](#) reported losing over \$1 billion in crypto to scams — more than any other payment method. Although cryptocurrency blockchains are thought to be highly secure, crypto repositories, such as exchanges and wallets, have been hacked. The technology developers building or supporting these platforms may face reputational or public trust risks in the event of a security failure or hacking.

The recent collapse of the FTX cryptocurrency exchange and the broader [crypto selloff in May 2022](#) shed light on the importance of effective digital asset risk transfer solutions and insurance protections. Although digital assets share some risks with traditional products and services, the unique market structure and underlying blockchain technology cause risks to manifest in novel ways.

06| Digital asset and cryptocurrency adoption still low, but opportunities are being explored

Is your company operating in or exploring opportunities related to digital assets and/or NFTs?



Source: Global Technology Industry Risk Study 2023

The need to address the risks and benefits of digital assets at a federal level is becoming increasingly clear. In the US, for example, President Biden issued [an executive order](#) directing federal agencies and financial regulators to develop frameworks that, among other priorities, protect consumers, businesses, and investors. The administration also calls for research into a United States Central Bank Digital Currency (CBDC) — a digital form of the US dollar.

For those organizations that either have already adopted digital asset practices or are exploring opportunities — as 50% of our survey respondents are (see Figure 6) — these factors and a fluctuating digital asset market have increased their focus on insurance solutions. However, organizations should start with evaluating their strategic objectives and risk profile, and have that inform their insurance strategy.

Level setting

To create the initial risk assessment framework, it's important to understand the extent of the organization's involvement in the digital asset space, namely whether these will be used internally or externally and if they will be managed in-house or through a third party partnership.

From here, organizations can take a scenario-based approach to assess their security, controls, compliance, and operational resilience to determine effective risk transfer and mitigation techniques. Consider also where there are interrelated risks and risks that may have multiple potential insurance policy responses.

Although the risks ranked highest on this year's survey are concerning, organizations operating in this space should especially consider their counterparty risks, a significant risk since most companies are not building their own digital asset infrastructure.

Organizations will also need to think about their regulatory risks and consider how potential regulations may affect them and change their objectives.

Regulatory clarity is likely to be helpful from a corporate governance perspective; however, as regulations and categorizations of digital assets evolve, more complex challenges may arise. Currently, courts and regulators struggle with how to define digital assets, as currencies, commodities, securities, or something else entirely. How these assets are classified ultimately determines which laws and bodies have purview over their regulation. As situations evolve,

organizations using digital assets in house will need to review whether they are able to handle any added regulatory responsibilities, or if they need to partner with a third party to continue business in this space.

Securing adequate insurance coverage

Strategic direction is key to securing effective insurance coverage. Organizations should consider how their risks change as they move further along their strategic plan, which allows them to overlay a risk framework and map it back to insurance. In building the plan, organizations should seek advisors to consult on technology best practices and digital asset regulations. Performing this due diligence will not only help organizations better understand their current and potential exposures, but may also put them in a more favorable position with underwriters.

Both directors and officers liability (D&O) and errors and omissions (E&O) insurance policies — which most organizations already purchase — typically provide protection for digital asset exposures and typically do not require additional affirmative coverage. Even so, it is advisable for organizations to be proactive by informing insurers before entering this space and being prepared to answer their questions. If an insurer discovers an organization's digital asset exposure only when a claim is being made, it can damage the organization's relationship with the insurer, potentially leading to exclusions on future policies.

Unlike D&O and E&O policies, crime policies typically do require affirmative coverage for digital assets, as they normally are intended to cover all of the insured organization's money and tangible property. Since they will involve modified definitions and specific valuation language, it is critical to involve advisors so that digital assets can be appropriately valued if they're stolen or become inaccessible.

Although digital assets have many risks, both established and emerging, thorough risk analysis and proactively discussing strategic plans with underwriters can help organizations operating in this space secure the necessary insurance protections.

RISK FOCUS: ADVANCED AUTOMOTIVE

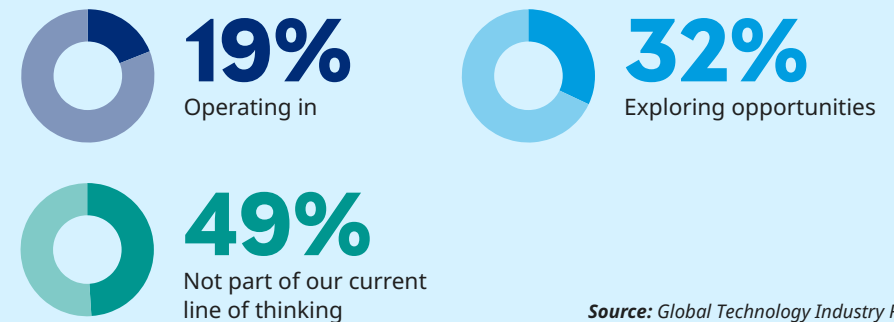
Autonomous mobility risks gathering momentum

Growth in the production and use of autonomous vehicles (AVs) and electric vehicles (EVs) is creating new and exciting partnerships between Silicon Valley and Detroit, but is also giving rise to several significant risks for technology companies in the mobility sector. While some of these risks are likely to intensify in the coming years, the mobility industry broadly is undergoing a structural shift, which will require companies to think differently about their risk and exposures.

The EV and AV markets are expected to continue growing at a steady pace, especially as urban populations swell and consumers' interest in mobility-as-a-service expands. Just over half our survey respondents are either already operating in this space or exploring opportunities (see Figure 7). The United Nations Department of Economic and Social Affairs forecast that [68%](#) of the planet's population will live in urban areas by 2050, up from 55% in 2018. That population shift will accelerate sustainable development, including mobility initiatives, according to the UN.

07| Autonomous and next-generation mobility adoption still low, but opportunities are being explored

Is your company operating in or exploring opportunities related to autonomous or next-generation mobility?



Source: Global Technology Industry Risk Study 2023

13%

Portion of all light-duty vehicle sales in 2022 accounted for by EVs; expected to increase to 34% of total global vehicles by 2030.

Source: [International Energy Agency](#)

4.3 million

Number of new EVs delivered in the first half of 2022; a 60%+ increase over the first half of 2021.

Source: [EV Volumes](#)

\$1.8 trillion+

Revenue the global AV market will generate by 2030, up from \$94 billion in 2021.

Source: [Precedence Research](#)

WHO WILL BUILD THE CAR OF THE FUTURE?

Technology has spearheaded an evolution in nearly every part of the automobile. From lane departure warnings and electric engines to automatic braking sensors and entertainment and navigation consoles, the automobile of 2023 is hardly recognizable when compared to its 1923 predecessor.

But the design and assembly process for creating cars has remained similar to that of a Model T. A single company designs and assembles the final product today — just like Henry Ford did.

As technology companies both collaborate and compete with traditional automotive companies, that model is beginning to shift to something closer to the way technology products are manufactured. Some companies will continue to design and assemble themselves, but newer automotive companies will likely bifurcate the process.

We will likely start to see one company research and design the product before partnering with a contract manufacturer to create the final product. That outsourced assembler will likely build cars for a number of different brands — similar to the way existing contract manufacturers work within the global tech supply chain. Still, there will likely remain companies that retain design and assembly in house and others may take a more blended approach.

RISK FOCUS: ADVANCED AUTOMOTIVE

6 existing and emerging risks in mobility

Autonomous and electric vehicles have a complex array of components and technologies, from advanced driver assistance systems to a variety of sensors that gather and relay information to the driver or take control of certain vehicle operations. As a result, the mobility sector faces a growing set of risks, including:

1

Data security and privacy

Data is essential to the development and operation of AVs and EVs, as is managing the risks to data security and privacy. But the possession of data has made companies in all industries vulnerable to cyberattacks as cyber criminals seek to steal data or extort payments for encrypting or threatening to disclose data.

Systems resiliency and cybersecurity are important considerations for technology companies as well as regulators, especially for vehicles with higher levels of autonomy. One risk scenario on the minds of manufacturers, consumers, and regulators is an AV getting hacked and remotely controlled, causing the vehicle to injure people or cause property damage.

2

Supply chain

As a global industry, mobility has complex supply chains spanning most of the developed world. A semiconductor shortage that began during the coronavirus pandemic has stabilized, but the lack of chips is still causing backlogs in vehicle inventory. The next bottleneck in the supply chain may be related to having sufficient batteries to keep EV and charging station facilities running. As demand for EVs continues to rise, the battery manufacturing supply chain must keep pace. Societies must also continue to build out the infrastructure needed to recharge vehicles on longer trips, especially since an inadequate charging infrastructure may dampen enthusiasm for EV.

As EV production increases, consolidation among suppliers is a strong possibility for certain key components. Few manufacturers are prepared for such consolidation and its impact on supply chain risks. An example of this risk is Taiwan, which makes a majority of the world's advanced microchips for many industries, not just automotive. With few options for alternate suppliers, vehicle manufacturers sourcing chips in Taiwan have a [heightened risk](#) of disruption. Looking to the future, companies that select a contract manufacturer business model may also face contingent business interruption risks.

3 Regulatory compliance

Numerous regulations have an impact on the mobility industry, and keeping up with changing regulations in different jurisdictions is challenging. For example, the General Data Protection Regulation (GDPR) in the European Union has inspired similar regulation in the United States.

Supply chain regulations are pushing for manufacturers and suppliers to provide greater transparency and allow for monitoring of where materials originate. This kind of regulation is a particular challenge for manufacturers of EV batteries, which require metals and rare earth minerals. Most of the world's supplies of these materials are mined in developing countries.

4 Product liability


Most incumbent original equipment manufacturers do not purchase product liability insurance and, instead, tend to seek to mitigate their own exposure to product liability through contractual risk transfer to their suppliers. Makers of advanced driver assistance systems and other AV technologies are therefore likely to see their product liability exposure increase.

5 Environmental liability

Mobility companies in the EV space frequently advertise the environmental benefits of battery-electric and plug-in hybrid electric vehicles. Consumers, investors, and regulatory authorities are paying more attention to companies' public statements and are insisting on disclosure of environmental, social, and governance (ESG) programs.

6 Reputational risk

Underlying the set of risks in the mobility sector is reputational risk. This can be triggered by various actions, from a cyber incident to failure to comply with regulations, to accidents that cause bodily injuries or deaths. A failure or defect in a component produced by a supplier can pose a significant reputational risk to the original equipment manufacturer that used the component.



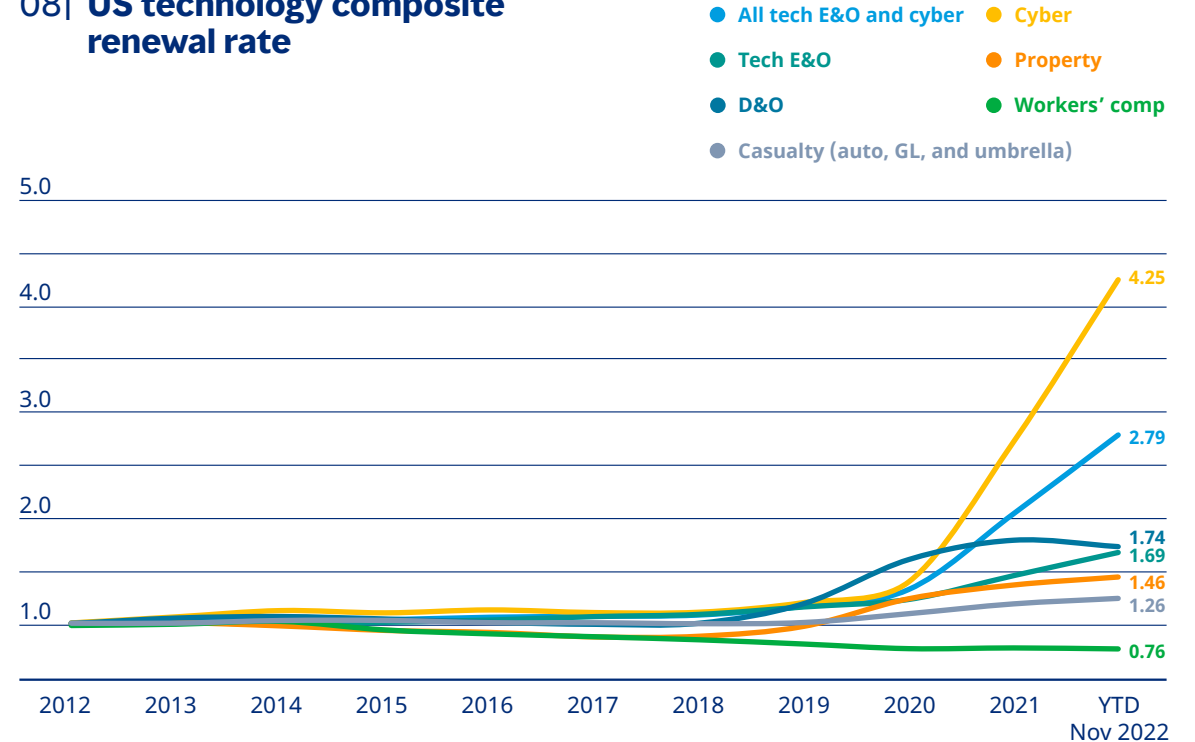
Autonomous and electric vehicles use highly sophisticated engineering and require specialized infrastructure to support their operations. As a result, they introduce complex and dynamic risks, not only on the road but also in manufacturing and maintenance. AV and EV technology is introducing a new and more complex era for risk management for manufacturers, technology suppliers, operators, drivers, and mobility regulators.

Tech companies face large increases for key insurance lines

Technology companies should prepare for potential challenges for some of their key insurance lines going forward. Marsh tracked the cost of seven key coverages since 2011 for tech companies. We found that only workers' compensation premiums are lower in 2022 than they were in 2012 (see Figure 8).

Cyber premiums have more than quadrupled for tech companies since 2012 — with especially large jumps since 2019. And although D&O rates are starting to plateau, property rates have shown a rise in the last two years.

08| US technology composite renewal rate



Tech companies rethinking and remarketing insurance programs

Persistent premium increases over the last decade, which have recently [started to slow](#), have driven many technology firms to take more aggressive actions to preserve capital and protect their operations. In fact, close to 40% of survey respondents said they have switched or are considering switching primary insurers this year in response to price increases (see Figure 9).

Note that 25% of respondents to our 2022 survey and 24% of respondents to our 2021 survey said they were switching primary insurers, even though the market was also difficult when data was being collected in 2020 and 2021, with double-digit average increases.

As they have in past years, respondents have shown eagerness to seek new insurers throughout the program layers.

These shifts may indicate a continued move by tech companies toward retaining key risks rather than transferring them. And if tech companies no longer rely as heavily on insurance to manage their most critical risks, maintaining key primary insurer relationships may become less important. And while insurance purchases remain critical for many tech companies, some may be relying on them to transfer less critical risks or simply to meet regulatory or lending requirements, further reducing the perceived importance of a long-term relationship with their primary insurer and making switching carriers in search of better rates more attractive.

We are still seeing tech companies express interest in taking more control of their risks through alternative risk solutions (34%), captives (22%), and moving toward pure catastrophic coverage (18%).

09| More than a third of companies switching primary insurers

What actions has your company taken or considered in order to deal with the ongoing premium increases and reduced capacity in the market? Select all that apply.



Standard actions

Aggressive program marketing

45%

Introducing new insurers throughout program layers

45%

Switching primary insurers

38%

Increasing retentions

54%

Reducing limits

38%

Narrowing terms, conditions, or definition of services

21%

Reallocating insurance budget from more expensive lines of coverage

13%

Exploring integrated, structured, or other alternative risk programs

34%

Leveraging or exploring captives

22%

Moving toward pure catastrophic coverage only

14%



Retaining more risk



Taking more control

Optimizing risk management

The global economic slowdown has affected organizations across regions and industries, leading to difficult decisions. The majority of survey respondents reported a need to adapt their risk management decisions to respond to economic conditions, with only 35% saying that the company's risk management decisions were not affected.

Those that had to shift the ways they manage risks are doing so in different ways. Some tech companies are changing their risk strategies or cutting back on investments in risk management, whether it means reducing human resources, risk mitigation projects, or investments in digital risk platforms.

Despite the challenging economic landscape, some companies continue to prioritize risk management. In fact, 20% of survey respondents said their companies are actually increasing their investment in risk management (see Figure 10). Considering the current economic uncertainty, this suggests that these firms view their risk management departments as key strategic partners for growing revenue and protecting the organization.

10| Difficult economic conditions affecting risk management departments

In what ways has the economic slowdown and tightened access to capital affected risk management decisions at your company already? Select all that apply.



Risk strategy changes

Electing to retain more risks to lower premium costs

38%

Seeking financial certainty by transferring more risk

21%



Cutting risk management costs

Hiring freeze/reduction in staff directly or indirectly supporting risk management

38%

Lower investments in risk mitigation efforts or projects

14%

Postpone/cancel investments in digital risk platforms

12%



Embracing risk management as a cost control tool

Increased investment in risk management

20%

Source: Global Technology Industry Risk Study 2023

Enabling growth

There is a shift in the way tech companies view risk management as an enabler of growth. Close to half of respondents said risk management and insurance support public trust and a positive reputation (see Figure 11). This is a significant shift from 2022, when 33% pointed to the role risk management plays in enabling public trust and positive reputation.

This change also comes at a time when reputational risks for tech companies have increased significantly. As more companies recognize the potential repercussions of reputational damages, it is important for risk management teams to focus on identifying and quantifying potential reputational challenges and work to find ways to manage and mitigate these risks.

11| Changing perception of risk management

Increasingly our tech clients view risk management and insurance as an enabler of growth. How does risk management and insurance enable growth within your organization? Select all that apply.

Smooths contract negotiations by limiting liabilities



Supports management in aggressive decision-making or making big bets



Supports public trust and a positive reputation



De-risks multiple participants throughout our company's ecosystem



Protects operating or R&D budgets



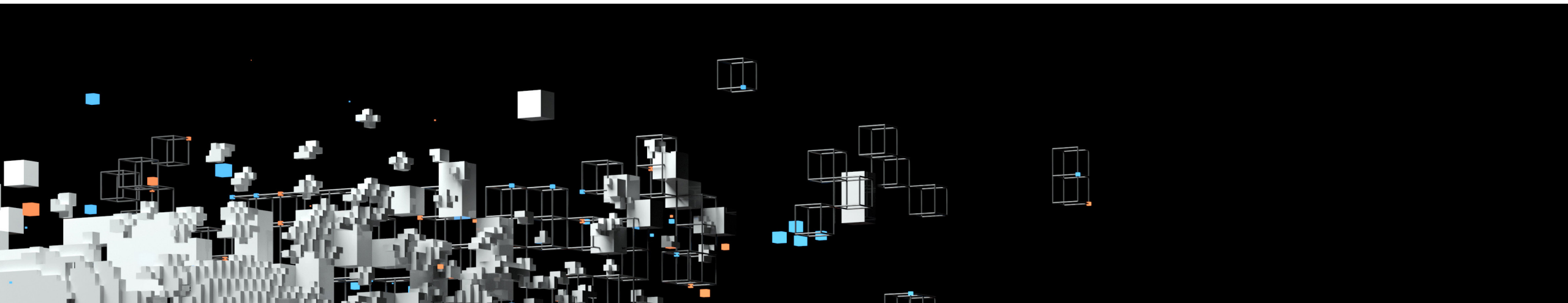
Enables new business models



Identifies off-strategy risks which could derail growth



Provides new sources of B2B or B2C revenue





Conclusion and next steps

Addressing the growing risks for tech companies while controlling costs during an economic slowdown will require risk departments to be grounded in basic risk management tactics while also embracing alternative solutions. Following are 10 recommendations for successful technology risk management in 2023.

Conduct continuous risk assessments

As noted in Figure 4, the vast majority of respondents say their companies are growing in innovative ways in 2023. New products and new partnerships create new risks. As tech companies make big bets and move quickly to grow, risk management departments must constantly assess how these moves impact risk profiles.

Engage in marketing diligence

Pay attention to real-time market insights, not just annual or even quarterly reports, to better understand what is happening in the insurance market. As your company develops new products and solutions, be ready to understand the costs and budgets for mitigating the risks.

Truly entertain alternative structures

For several years, some technology companies have been considering alternative risk transfer solutions, reviewing captives and thinking about integrated or structured programs. Only about one-third of respondents to this year's study reported that they are trying to go beyond traditional risk transfer programs. 2023 should be the year that technology companies get more serious about developing the foundation that allows alternative risk solutions to become a viable option.

Market your program strategically

While there have been improvements in the cyber market, especially for good risks, some clients are still facing challenges obtaining a quote. Marsh data show that cyber underwriters provided a quote for 84% of requests made in 2020; this dropped to 64% in 2022. Yet, only 45% of respondents said their companies are aggressively marketing their insurance programs. To remain competitive in a dynamic and quickly changing market, tech companies should review their coverage needs and market their program strategically as they seek to secure the broadest coverage that aligns with their risk transfer budget.

Quantify risks beyond benchmarking

Benchmarking reports can be helpful, but are by their nature backward looking. Tech companies should conduct scenario analysis and look to other industries to truly understand the magnitude of their changing risks.

Understand your entire risk ecosystem

The global digital supply chain requires technology companies to understand all the interdependent risks across their ecosystem. A thorough review does not stop with analyzing your own risks, but requires mapping those of your vendors, partners, suppliers, customers, and platforms.

Focus on enabling growth

From streamlining contract negotiations to enabling new business models, risk management departments can help drive revenue. Seek to find risk management solutions to enable growth and try to identify and address problems that can derail growth.

Identify and address your people risks

People risk is tech risk. The systems and checks and balances that keep tech companies operational still rely on people to keep them running. Pay close attention to staffing levels, morale, and fatigue and adjust your risk models to account for the people element.

Drive operational efficiency

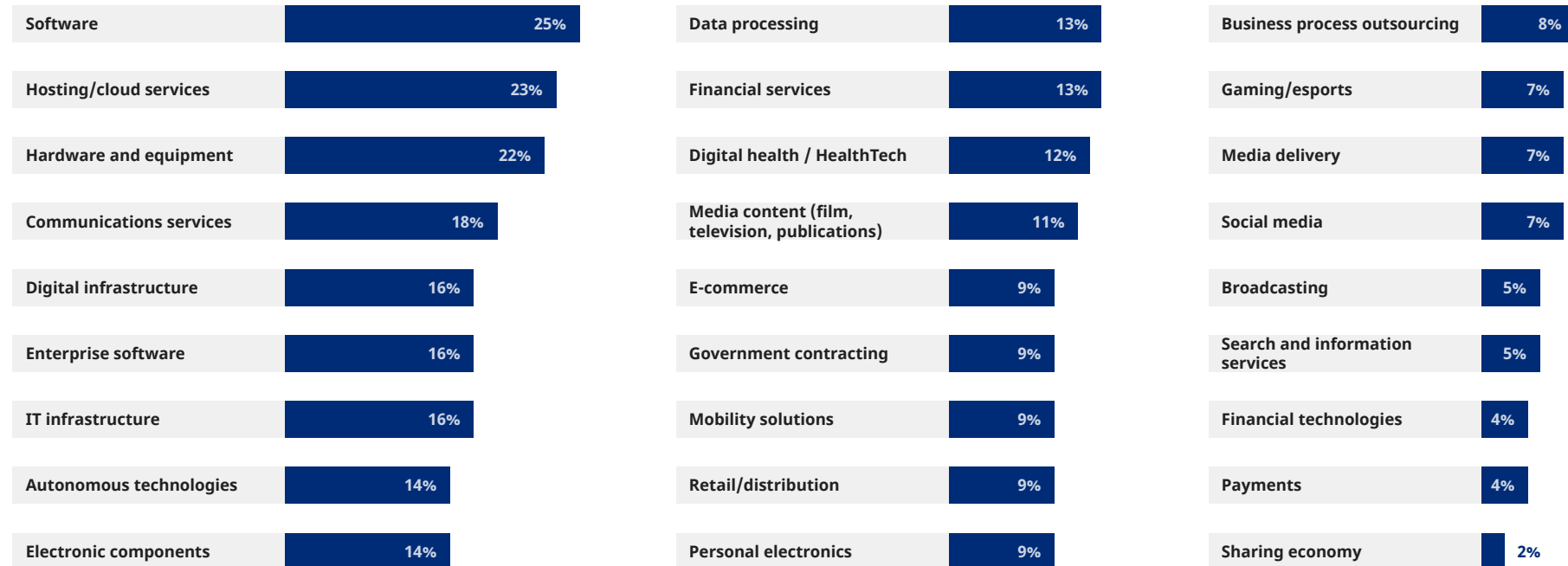
Embrace digital solutions, analytics, and modeling to help ease the burden on your [overworked?] risk management department. Inefficient processes and procedures can be an obstacle to innovating new risk management solutions.

Be nimble

The tech industry is constantly evolving. Be ready to move with it. Staying relevant in risk management means challenging the status quo every day.

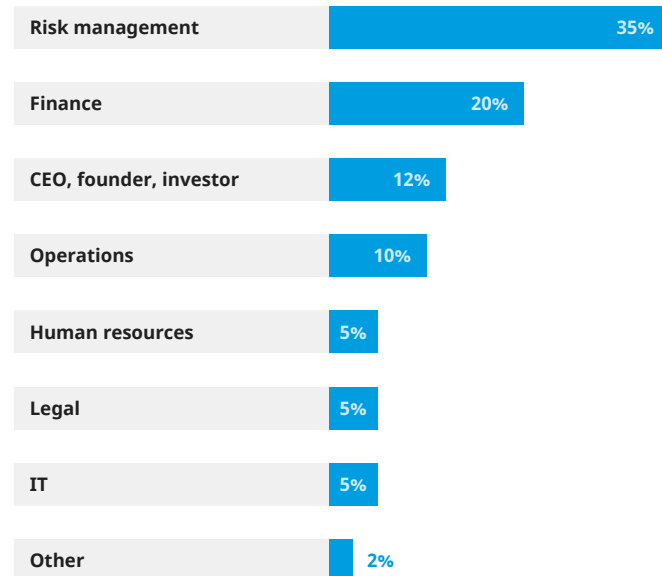
Survey demographics

12| Business models of respondents show a varied landscape

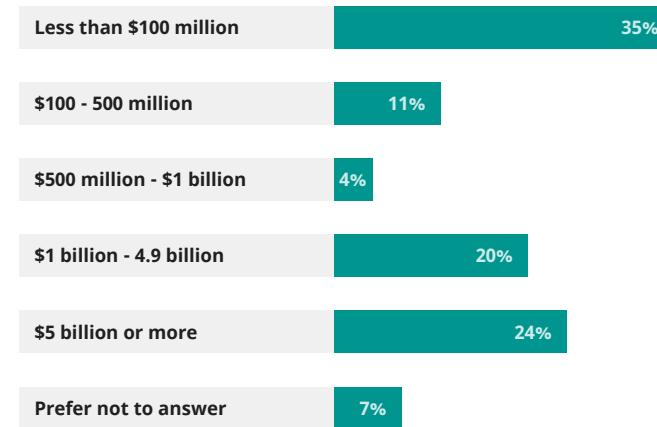


Survey demographics

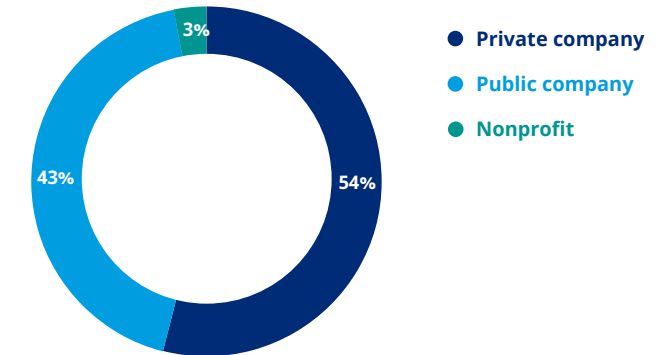
13| Position/business area



14| Annual revenue (in USD)

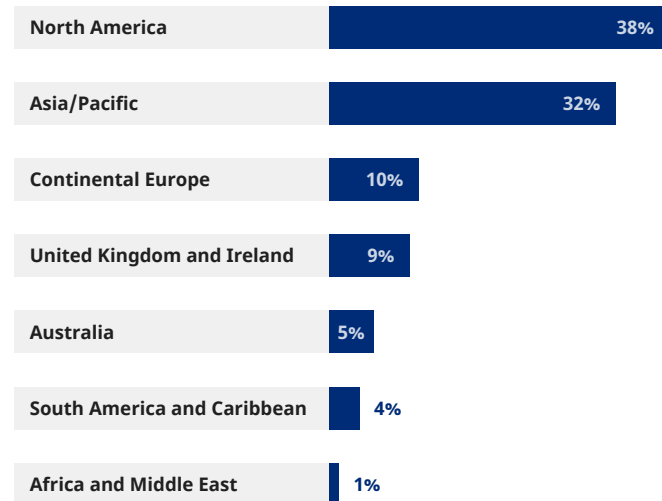


15| Company type



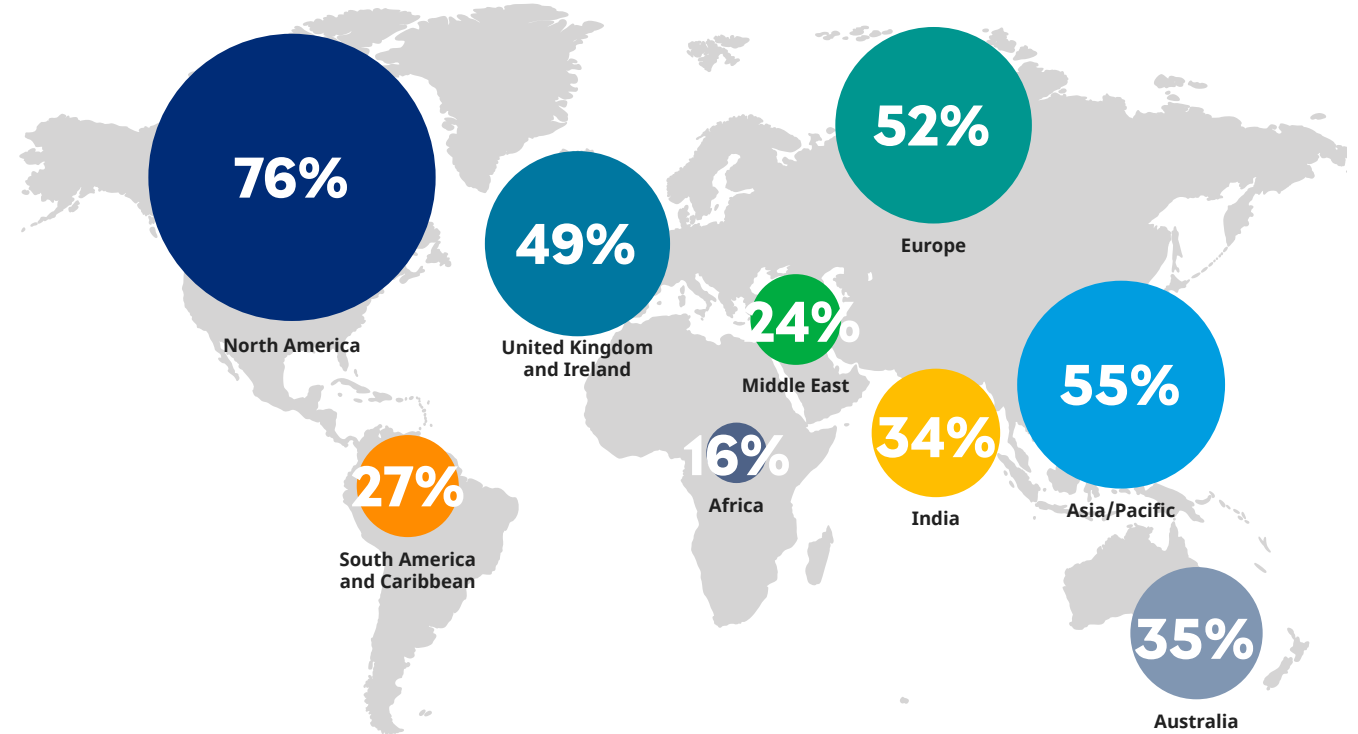
Survey demographics

16| Company headquarters



17| Risk exposure by geography

In which geographies does your company have significant risk exposures? Select all that apply.



Marsh's Global Technology Industry Practice

Marsh's Global Technology Industry Practice delivers decades of experience to its diverse and innovative clients from specialized hubs around the world — including our San Francisco Technology Center of Excellence. Our colleagues have a thorough understanding of emerging technology trends by sitting at the heart of technology innovation. Beyond general technology knowledge, Marsh has also developed specialists who focus on specific sectors of technology risk including:



Sharing economy
and mobility



FinTech



Digital
infrastructure



E-commerce



Advanced
automotive



High tech and
semiconductors



Communications



Software and
IT services



Digital assets



Consumer
electronics



Social media/
gaming



Digital health

Marsh's technology industry expertise



Local, specialized tech
expertise in **100+**
global offices.



Committed to the
85% of clients that
are high-growth,
middle-market
companies.



Placing **\$4B** in
premium annually.



4,000+ tech
clients, globally.



Served by a global
network of **600+**
dedicated tech
risk management
professionals.



About Marsh

Marsh is the world's leading insurance broker and risk advisor. With around 45,000 colleagues operating in 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue nearly \$20 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. For more information, visit marsh.com, follow us on [LinkedIn](#) and [Twitter](#) or subscribe to [BRINK](#).

Marsh is a business of Marsh McLennan.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.

1166 Avenue of the Americas, New York 10036

Copyright © 2023, Marsh LLC. All rights reserved. MA23-16258 988982046