

Business Insurance Trends

Overcome the current climate of uncertainty

Mitigating today's top business risks



Your future is limitless.SM

[MarshMMA.com](https://www.marshmma.com)

Striving for stability in the face of unpredictability

After four turbulent years, the near-term outlook for the global economy remains highly uncertain. This is due to both domestic factors in some of the world's largest markets as well as ongoing geopolitical conflicts escalating across the world.



While the global economy avoided an anticipated recession in 2023, the path ahead for small to mid-size businesses is more unpredictable and challenging to navigate than ever before.

Inflation and high interest rates linger amid continued supply-side pressures, creating uncertainty and threatening economic growth. Insurance premiums are increasing due to factors such as nuclear judgments and climate challenges, which are colliding to place additional financial strain and risk on businesses.

The top risks are not new, but many have grown—and will continue to grow—in complexity.

Economic volatility impacts them all, and businesses across industries will need to overcome the current environment of uncertainty by seeking ways to mitigate them.

Top risks for 2024 as identified by U.S. business owners



Source: 2024 Marsh McLennan Agency Business Insurance Trends Survey

Overview of methodology

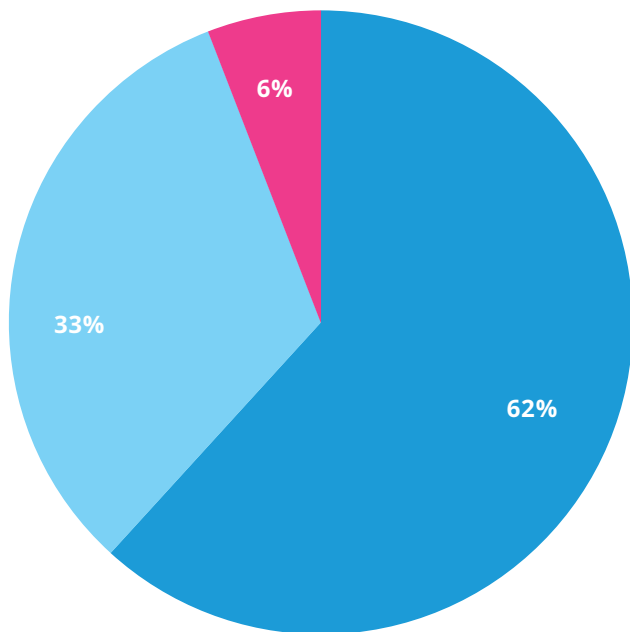
Our annual Business Insurance Trends report offers valuable insights into the evolving landscape of risk experienced by business leaders across the United States.

We've compiled the insights in this report based on our survey results collected from January 15 to February 6, 2024. We deployed this survey seeking knowledge on the concerns of our current clients and business leaders with a significant level of engagement in their company's risk management decisions and strategies. We asked participants to rate their top risk concerns and readiness to handle the most significant threats affecting their industry. A diverse spectrum of businesses is represented within the 507 completed surveys.

92%
of survey participants have high to medium engagement with risk management decisions and strategies within their organization.

Total annual revenue of survey respondents

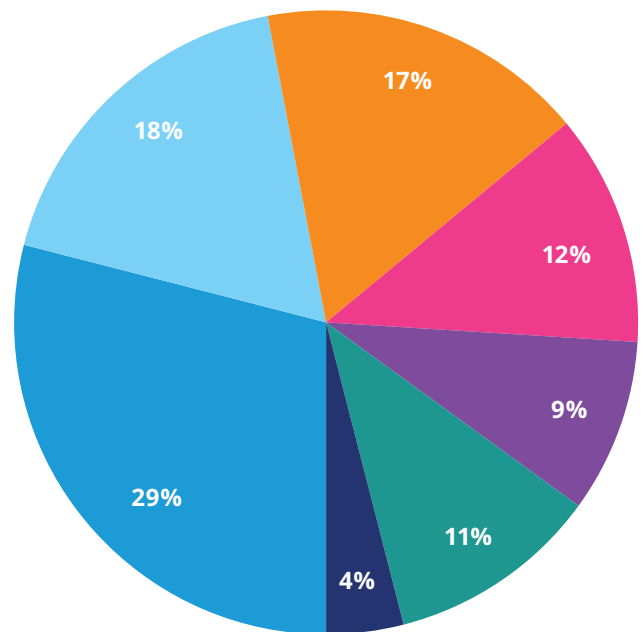
■ \$10M to \$49M ■ \$50M to \$1B ■ \$1B+



Source: 2024 Marsh McLennan Agency Business Insurance Trends Survey

Total # of employees of survey respondents

■ Less than 50 ■ 51-100 ■ 101-250 ■ 251-500 ■ 501-1,000 ■ 1,001-5,000 ■ 5,000+



Source: 2024 Marsh McLennan Agency Business Insurance Trends Survey

According to our Business Insurance Trends Survey, the top 5 risks for 2024 are:

01 Cyber and data risks

02 Regulatory risk

03 Workforce risk

04 Catastrophic weather risks and property limit capacity

05 Nuclear verdicts and social inflation

By understanding and addressing these five risks, your organization can become more resilient and ready for what's next.

01

Cyber and data risks

Cyberattacks can occur at any time. However, there is some evidence that “successful” infiltrations tend to increase during and in the wake of economic downturns. When these occur, threat actors can take advantage of the distractions, causing additional strain on businesses. They can also take advantage of the increased reliance on third parties to cut costs, opening the door to third-party vulnerabilities.

75%

of business leaders are **extremely or very concerned** about cybersecurity and data privacy.

17%

of business leaders are **somewhat concerned** about cybersecurity and data privacy.



The urgency for cybersecurity risk management is amplified as attackers use more sophisticated methods.

This is especially true since vulnerabilities are increasing for businesses adopting various technologies such as artificial intelligence (AI), cloud computing, and Internet of Things devices. Furthermore, dependence on third-party technologies in all facets of an organization can stifle operations, lead to downstream business interruption, and reputational risks.

Security and data privacy stand as twin pillars of concern for modern enterprises when it comes to digital protection and compliance. Beyond information technology, these pillars must branch out to all segments of an organization.

Amid these risks, business leaders are looking for tools and resources to help them achieve their strategic goals in 2024, and most are looking to AI. AI applications for managing business risk, such as predictive analytics and compliance monitoring automation, have proven useful, helping companies understand workforce behavior, performance, and additional training needs. But technology presents emerging risks and potential liabilities, especially in the experimentation phase.



In our survey, 52% of leaders said tech advancements like AI, advanced imaging, data analytics, automation, and more will lead to new challenges for their business. A whopping 93% of them also said it would lead to new opportunities.

Like every dynamic in today's market, [getting the most out of AI](#) will require balancing innovation and risk management. Given the current novelty of AI technology, the regulatory framework around it is bound to evolve and companies employing these technologies will need to be extra vigilant to remain compliant.

Security

Integrating AI technologies into almost every industry introduces novel security concerns—and AI security frameworks are in their early stages. While it can significantly enhance an organization's ability to detect, respond to, and mitigate cyber threats more effectively, AI also presents new challenges. Some challenges include its ability to facilitate inadvertent malicious activities and the emergence of AI-driven attacks.

There have also been instances where AI systems have inadvertently released sensitive information from large language models that were used to train the AI but never intended to be public. Organizations should continue to be mindful of how they share data with third parties and especially whether it will be used in the training of AI models. These models could potentially be released or used in unintended fashion, violating contractual covenants or privacy laws.

As the potential risks continue to grow, third-party service providers in all segments of business should be monitored and contractual risk transfer should be implemented.

Not understanding how data may be used in unassuming manners could open organizations up to risks such as privacy, regulatory violations, reputational damage, and potentially intellectual property infringement.

Social engineering tactics such as phishing and business email compromise have also evolved to leverage AI to better deceive users and gain unauthorized access to systems. These AI-powered attacks can mimic the writing style and behavior of trusted individuals within an organization or automate the reconnaissance phase of business email compromise attacks. These pose significant financial risks for organizations. This is particularly the case for funds transfer fraud and social engineering fraud, which may present significant insurance reimbursement challenges.

Zero-day vulnerabilities: a crack in the dam

Zero-day vulnerabilities represent one of the most critical and challenging aspects of cybersecurity for many businesses. Much like a hidden crack in a dam wall, these vulnerabilities refer to weaknesses in software or hardware in the early stages of its development or deployment. Developers have not yet fixed these vulnerabilities but are just big enough for nefarious actors to slip through undetected.

While the opening might be small, it can jeopardize the integrity of an organization's sustainability due to its high reliance on third-party technology providers. Technology providers are that much more of a target given their central role in the delivery of solutions. If cracked, it could impact their portfolio of clients and vendors. This could lead to downstream outages, delays, and costly remediation efforts.

Undoubtedly, these vulnerabilities are attractive for the ransomware ecosystem of threat actors. Unfortunately, we will continue to see all industries reliant on critical technology infrastructure impacted significantly. Reviewing your third-party vendor risk management program is important to understand roles, responsibilities, and indemnities under contract should your supply chain be impacted. This will help ensure you have a compliant and quick response.

Organizations in highly regulated industries should be especially aware of the repercussions of the lack of compliant response as well as the impact on their data stakeholders. For better or worse, all organizations and industries are more connected than ever. Even if an organization does not house sensitive data, it can still be a target. Unauthorized access into a network can be quickly monetized by threat actors directly or by targeting your vendors and supply chain.



Data privacy

The interconnectedness between organizations, accelerated by increased technology reliability, application, and adoption in all industries, has resulted in an increased focus on sharing, collection, retention, and use of all forms of data.

Cornerstone regulations, such as the European Union's General Data Protection Regulation (GDPR), set a precedent for comprehensive data protection laws. As of Q1 2024, [at least 13 states in the U.S. have adopted similar measures](#), requiring businesses to ensure compliance across various departments, including legal, HR, and marketing. This trend will continue across the U.S., influencing more societal awareness of where and how data is stored and utilized.

Many multinational organizations have had a head start in complying with legislation such as GDPR. However, smaller and mid-sized organizations in the U.S. are steering their data privacy procedures and methodologies toward compliance. Additionally, privacy laws pertaining to collecting, using, and safeguarding sensitive biometric and genetic information will continue to impact organizations as technologies evolve.

Even dated laws such as the Video Privacy Protection Act and newer emerging regulations pertaining to transparency, consent, sharing, retention, and purpose of data in website tracking technologies have been brought into focus. These are commonly used by advertising and marketing departments to track user behavior and experience.

Failure to inform customers, employees, or business partners about data tracking activities and sharing of sensitive information with third parties can lead to major legal and reputational consequences.

With third-party involvement, data from a business's systems may be shared with external entities, potentially increasing the risk of unauthorized access or misuse. Each additional party introduces new vulnerabilities and potential breach points, making it more challenging to track threats and protect sensitive information.

Cyber risk solutions

How strong is your organization's cyber hygiene?

More organizations are realizing that cyber risk is not just an IT issue but also a legal and business imperative. Organizations must proactively address vulnerabilities in their IT systems and the use of technology in other departments. This is cyber hygiene—the practices and protocols a business implements to safeguard its digital assets to minimize the risk of security and privacy threats.

Businesses with strong cyber hygiene have implemented robust patch and vulnerability management programs, secured and encrypted backups, and employee training and awareness programs. Having strong cyber hygiene is not a guarantee that your business will never experience a breach, but it will make it more difficult for attackers to find and exploit vulnerabilities within your systems.



Top cybersecurity controls



Multifactor authentication for remote access and admin/privileged controls



Endpoint Detection and Response (EDR)



Secured, encrypted, and tested backups



Privileged Access Management (PAM)



Email filtering and web security



Patch management and vulnerability management



Cyber incident response planning and testing



Cybersecurity awareness training and phishing testing



Hardening techniques, including Remote Desktop Protocol (RDP) mitigation



Logging and monitoring/network protections



End-of-life systems replaced or protected



Vendor/digital supply chain risk management

Incorporating an incident response plan is key to limiting the impact of a security or privacy incident.

An **incident response plan** outlines clear roles and responsibilities, establishes communication protocols, and includes steps to contain and mitigate the attack for all stakeholders from different departments in your organization. Consideration of all third-party partners should be included in your response plans, whether the incident takes place within your organization or theirs. Each party should understand their responsibilities in case of a breach, how you'll share information, and coordinate response efforts.

Cyber insurance is also an important component of any effective response plan, providing financial protection and support during a cyber incident. Your response plan may also have a direct effect on your coverage. Strong cyber hygiene and action plans not only protect your business from cyber threats but play key roles in your ability to secure cyber insurance. You should expect insurance underwriters to ask detailed cybersecurity questions during the application process, as a lack of [key cybersecurity](#) and privacy controls may impact your terms and conditions.

TIP:

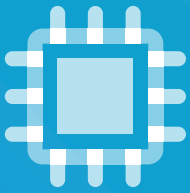
Your business's crime coverage can be a great supplement and companion to your cyber insurance because there may be instances where cyber-related losses reduce the effectiveness of your crime policy. It's important to know which one responds first in the event of a cyber incident, and how they interact with each other. Pay particular attention to coverage for social engineering attacks such as phishing, which may be covered under either policy.



Insurance policy language can make a difference.

Unlike traditional insurance policies, cyber insurance policies are constantly evolving to keep pace with the rapidly changing security and privacy threat landscape. The language used in your policy defines your current scope of coverage as well as exclusions and limitations. After assessment, you may find the need for coverage enhancements, such as:

- » **Affirmative wrongful collection:** Coverage for damages resulting from the wrongful collection of personal or confidential information (regardless of whether a security event contributed to such alleged wrongful collection or use)
- » **Contingent business interruption:** Protection against financial losses resulting from disruptions (security or system failure triggers) caused by your supply chain or business partners
- » **Invoice manipulation:** Coverage for losses resulting from fraudulent changes to invoices or payment instructions
- » **System failure:** Coverage for losses resulting from the failure of critical IT systems or infrastructure
- » **Betterment:** Coverage for expenses related to improving cybersecurity measures after a cyber incident



MMA's Cyber Resiliency Network

As part of our commitment to helping our clients navigate the complex world of cyber risk, we've established a [Cyber Resiliency Network](#) of third-party vendors who offer complimentary or discounted services in the event of a breach.

These vendors specialize in privacy law, information security, and employee awareness training. Regardless of which policies are placed with us, all clients have access to these valuable resources. They can help mitigate the impact of cyber incidents and enhance an organization's cyber resilience.

02

Regulatory risk

The nature and magnitude of regulatory risk can vary significantly across industries and regions, depending on the pace of regulatory change, the level of enforcement, and the complexity of regulatory frameworks within sectors. However, key themes of improving the employee experience, data privacy, and business accountability are pervasive across the 2024 compliance landscape.

61%

of business leaders are **extremely or very concerned** about regulatory challenges in the coming year.

24%

of business leaders are **somewhat concerned** about regulatory challenges in the coming year.



There are four regulatory examples gaining momentum this year:

1

Worker classification

The distinction between employee and independent contractor carries significant implications for taxation, benefits, and the legal obligations organizations have to their workers. In recent years, regulatory scrutiny around this issue has heightened as governments crack down on misclassification. Effective March 11, 2024, the [Employee or Independent Contractor Classification Under the Fair Labor Standards Act](#) makes it harder to classify workers as independent contractors under federal law. Businesses in California are already required to adhere to stricter tests to determine employment status, and other states are likely to follow soon. Failure of businesses to properly assess each worker's classification and follow appropriate employment laws can result in costly fines and legal disputes.

2

Biometric Information Privacy Act (BIPA) laws

BIPA laws have emerged as a focal point of privacy regulation, particularly at the state level. They govern the collection, storage, and use of biometric data such as fingerprints and facial recognition. [Illinois was one of the first states](#) to issue such an act, requiring informed consent, protection obligations, and retention guidelines. The act also prohibits the profit from biometric data. Businesses operating in jurisdictions with BIPA laws must require consent for data collection and establish clear protocols for data retention, protection, and disposal.

3

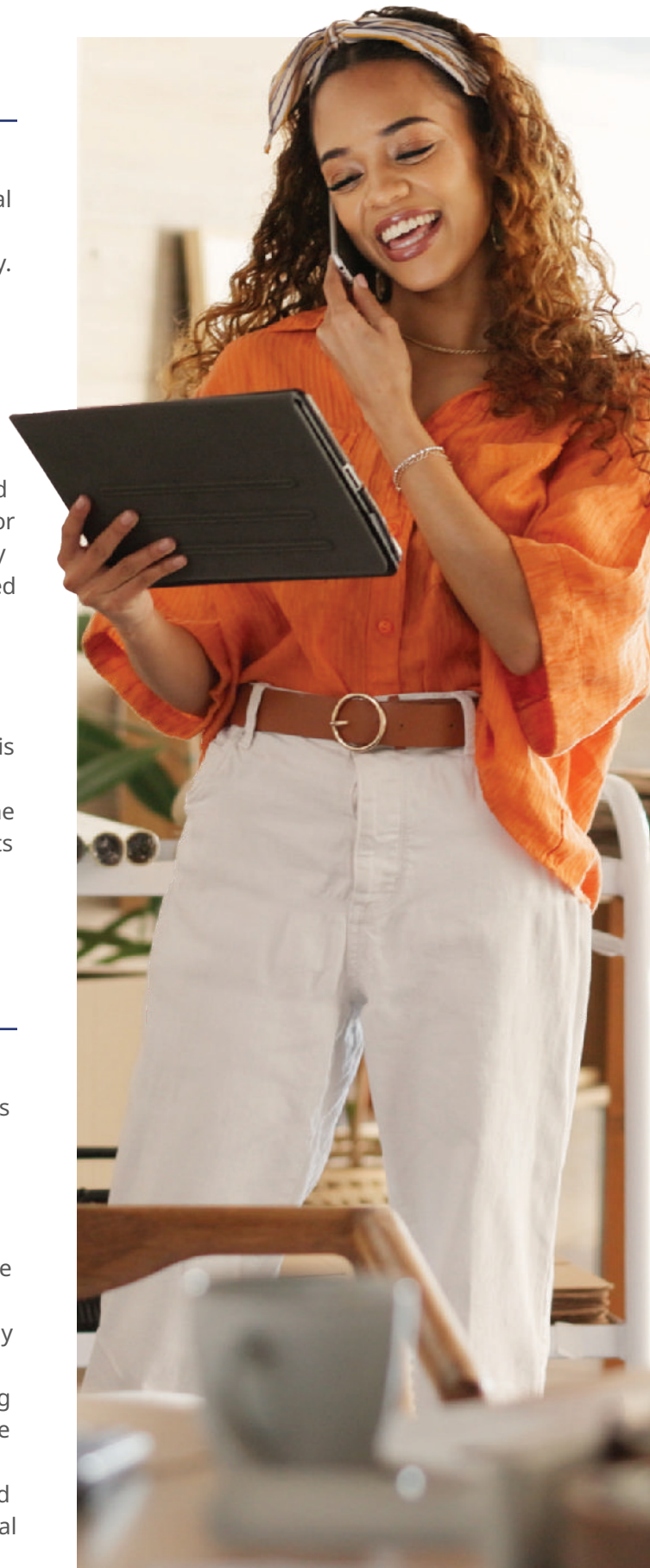
Climate disclosure

Regulatory frameworks aimed at enhancing environmental transparency and accountability are gaining traction as efforts to address climate change grow in social popularity. The Security and Exchange Commission chair has directed its [Division of Corporation Finance to increase its focus on climate-related disclosure](#) in public company filings. Large SEC-registered firms are grappling with new regulations forcing disclosure of information related to “material” emissions and climate risks. While legal challenges have delayed some of the forward momentum, the SEC adopted the final ruling for climate-related disclosure requirements for Scope 1 and 2 emissions, but eliminated the vendor supply chain Scope 3 emission obligations. Regardless of the reduced extent of this ruling, these new requirements can present implications across various lines of coverage. Directors and officers need to be especially mindful that they will be held to these higher transparency obligations from their investors. For this reason, entity investigation coverage that is often declined by organizations, should be considered going forward. Additionally, all organizations should understand the nuances and understand the time and financial commitments that will be required to comply with the final ruling.

4

Workers’ compensation presumptions

There has been a notable shift in some jurisdictions towards establishing presumptions that certain injuries or illnesses are work-related, thereby placing the burden of proof on employers to rebut these presumptions. California again leads the way in these classifications. Cancer presumptions for active firefighting members have been in effect for some time now, but newer presumptions related to COVID-19 passed as emergency legislation, were in effect until January 1, 2024. While the intention is to safeguard employees, these laws also underscore the importance of implementing robust workplace safety measures and protocols to mitigate the risk of occupational illnesses and injuries. Failure to address these concerns adequately could result in increased financial liabilities, higher insurance premiums, and potential legal ramifications.



Regulatory risk solutions


Assessment is the first step for any organization regarding regulatory risk at state, local, and federal levels.


Understanding what regulations apply to your business and the potential impact of non-compliance helps you prioritize your focus and resources. The resources for dedicated regulatory risk managers within companies are not always feasible. In heavily regulated industries, such as financial services, health care, pharmaceuticals, and energy, it's an important role to fill.


Otherwise, engaging with external consultants or legal advisors with expertise in compliance can help you navigate any complexities. Consider [regulatory risk assessment and consulting services](#) for insurance issues that apply to multinational companies and their global programs.


Once you understand your exposure and requirements, build a regulatory risk management plan that includes:




 **Regular compliance audits** to assess compliance with relevant regulations and internal policies. Your audits should be comprehensive and cover all aspects of regulatory requirements applicable to your organization.

 **Processes for staying informed** of regulatory changes and updates within your industry and all regions where your organization operates. Establish processes for assessing the impact of any changes that occur in your business.

 **A culture of compliance** that provides training to employees on regulatory obligations and compliance procedures promotes ethical conduct throughout the organization. Keep open communication channels for employees to report potential compliance concerns without fear of retribution.

 **Third-party relationship management** for vendors, suppliers, and other partners to ensure they adhere to regulatory standards and requirements. You don't want to pay for their negligence. It is important to note that contract language and obtaining certificates of insurance are ways of transferring risk to third-party vendors.

 **Documentation requirements** for all compliance efforts, including audit reports, policies, procedures, and employee training.

03

Workforce risk

For many organizations, there is nothing more important to its success than its people. People have always driven innovation, production, and revenue. In return, they expect safe working environments and fair compensation. Still, the workforce has experienced a major shake-up over the last several years with new ways of working, changing expectations from workers, and expanding regulations, creating an unpredictable talent market.

57%

of surveyed business leaders are **extremely or very concerned** about their workforce safety, well-being and expansion.

27%

of surveyed business leaders are **somewhat concerned** about their workforce safety, well-being and expansion.

As for the talent market, only 34% of business leaders believe their organization is well-prepared to effectively manage gaps.

Workplace safety

At the forefront of these risks are the expanding regulatory and compliance requirements around workforce safety meant to help industries adapt to changing work environments, technologies, and hazards. Along with COVID-19 pandemic responses such as new personal protective equipment requirements, the [Occupational Safety and Health Administration \(OSHA\)](#) has demonstrated an increased focus on ergonomics, fall prevention and protection, heat-related hazards, and [recordkeeping and reporting requirements](#) in recent years. Along with expanding rules, OSHA is hiring more inspectors and planning to conduct more inspections year-over-year. This is being reinforced by the current administration, which is [seeking to increase OSHA funding by an additional \\$23 million](#) when the upcoming fiscal year begins October 1, to reach these goals.



Absence, disability, and leave (ADL)

[Absence, disability, and leave \(ADL\) benefit regulations](#) have also been a challenge for small and mid-sized businesses, with 42% indicating difficulty staying updated and compliant with state and local leave laws. Whether for sickness, injury, family responsibilities, or personal time, employees need to take time off from work. These absences can impact both the employee and the employer when not managed correctly. It becomes even more complex for employers with employees in multiple states, as paid family and medical leave laws can vary from state to state.



Employee Health & Benefits Trends

Understanding today's multigenerational workforce is essential to providing effective benefits and appropriate employee support. Our [2024 Employee Health & Benefits Trends: The Evolving Workforce report](#) outlines three key themes shaping employee benefits throughout the year: benefits and talent, whole-person health, and health care costs. Boomers, Gen X, millennials, and Gen Z have unique generational values, work attitudes, health care issues, and economic challenges. It is important for today's corporate leaders to create an environment that is tailored to the holistic perspective where all employees can thrive. No matter the age or differences, each generation serves as an important piece of the workforce.

Workforce risk solutions

Workforce risk is a challenge many organizations will need to overcome.

When companies fail to establish processes and procedures around workforce management, support, and safety, they are likely to experience increased incidents and dissatisfaction among their teams. As a result, productivity may decrease, turnover rates rise, and company reputation suffers, making it harder to hire skilled workers in the future. Companies can remain trapped in a loop of workforce vulnerability and potential disruption to both the organization and employees. Fortunately, there is a path forward.

Best practices for addressing workforce risk include:

Talent recruitment strategies

- » Conduct compensation benchmarking for both salary and benefits.
- » Regularly review and adjust benefits plans to remain competitive.
- » Optimize your recruiting process by identifying effective talent sources and channels, and ensuring job descriptions accurately reflect skills requirements.
- » Demonstrate management's commitment to safety through regular training, communication, and rules reinforcement.

Data utilization and analysis

- » Collect and analyze workforce safety metrics such as injury rates, lost time incidents, and OSHA recordable incidents to measure the effectiveness of safety initiatives and identify areas for improvement.
- » Keep a record of safety metrics to demonstrate the organization's commitment to safety compliance.
- » Be transparent with employees about safety performance to build a culture of accountability, trust, and engagement.

Employee support and engagement

- » Prioritize employee onboarding to foster engagement and safety through clear communication of safety protocols and expectations.
- » Demonstrate genuine care for employees by prioritizing well-being and mental health, and cultivating a culture of compassion and support.
- » Establish and communicate employee career paths to foster growth and retention.
- » Develop a [strong workers' compensation and return to work program](#) that continues to engage employees and connect them to the team when out due to a work injury. Workers' compensation program features should include agreements with local doctors and clinics, and a teammate dedicated to acting as a liaison for each injured worker.





Workers' Health 360[®]

Our [Workers' Health 360[®]](#) empowers business owners concerned about workforce risk by leveraging their organization's data to drive comprehensive insights and actionable strategies.

This digital platform seamlessly integrates data from various sources such as workers' compensation, pharmacy utilization, medical plan data, and short- and long-term disability, to provide a complete view of your employee population. Through guidance from our data analysts and clinicians, you can gain meaningful insights to reduce risk exposures, enhance productivity, and improve employee health and well-being.

04

Catastrophic weather risks and property limit capacity

Our [2024 Commercial Property Insurance Trends report](#) demonstrates that a nuanced recovery for the property insurance market is underway. However, rising exposure from secondary perils, the increasing number of climate events resulting in \$1 billion losses or more, and urbanization in riskier areas will continue to define a "new normal."

56%

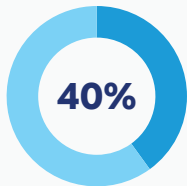
of business leaders are **extremely or very concerned** about catastrophic risks.

25%

of business leaders are **somewhat concerned** about catastrophic risks.

In January, [Swiss Re Institute](#) analyzed 2023 natural catastrophes, noting that global economic losses were \$280 billion.

Of these, \$108 billion (40%) were covered by insurance, above the previous 10-year average of \$89 billion. Swiss Re also stated that claims costs have risen by approximately 30% since 2020, signaling that organizations need to double down to reduce their overall loss potential.



40% of global economic losses caused by natural catastrophes in 2023 were covered by insurance



~30% increase in natural catastrophes claims costs has occurred since 2020



Let us help you manage your risk.

There's no one-size-fits-all solution when it comes to managing risk—every risk comes with its own unique challenges. We have a track record for strong performance in any market conditions through our broad market access and consultative approach. Whether you may be facing a hurricane, wildfire threat, or other catastrophic events, we offer a guide for [emergency resources](#) to help you stay in the know and navigate the unknown.

Catastrophic weather risk solutions

There is no silver bullet to addressing the long-term effects of natural catastrophes, but state and federal commitments are a key element to this growing dilemma.

Discouraging urban growth in catastrophe prone areas, enforcing building codes, and building flood protection barriers are just a few examples of how community actions can move us to a place of critical adaptation. Organizations can also:



Understand natural catastrophe risks. Work with your broker to perform thorough risk and hazard assessments.

Use catastrophe modeling. Sophisticated probabilistic modeling will help your organization understand how the likelihood of losses in certain size and frequency scenarios might impact loss costs.

Close the gap on any property data quality issues. The quality of your statement of values influences insurance pricing. It's important to address all ambiguity related to property valuations for buildings and equipment. There are a number of property valuation solutions that can help tighten up any misunderstandings related to your exposures.

Prioritize and act on loss control recommendations from insurance carriers. Improving your risk profile over time by tackling any risk management recommendations from your carrier will improve access to limit capacity.

Address uninsured and underinsured perils. Flood and earthquake are example perils that are often under appreciated. It's important to shore up coverage gaps for any risks in your property portfolio.

Leverage analytics. Our proprietary analytics capabilities can help you:

- » Validate the best approach to align your risk management and risk financing strategies with capital management objectives.
- » Make informed decisions surrounding risk retention and risk transfer.
- » Select the best limit and deductible options.
- » Measure overall risk tolerance in dealing with unexpected losses.

Employ robust due diligence procedures. When engaging in merger and acquisition activities, be sure to scrutinize all aspects of the additional risk exposures you could be assuming in the transaction. These are often hidden from view.

Explore alternative risk transfer options. Inform senior leaders within your organization that uncertainties in the property marketplace could negatively affect your property coverage terms and pricing. Cargo stock throughput coverage for businesses with first-party products moving through the global storage and distribution chain, for instance, can be a jumping-off point for digging deeper into broader risks. This option can lead to an analysis of supply chain risk and associated contingent business interruption exposures. Work closely with your broker to explore other alternative risk transfer opportunities, such as:

- » Captives
- » Parametric insurance
- » Structured programs

05

Nuclear verdicts and social inflation

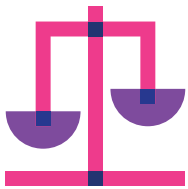
Civil litigation cases, particularly those involving corporate defendants, continue to gain attention and build concern as the frequency and severity of nuclear verdicts climb.

40%

of surveyed business leaders are **extremely or very concerned** about nuclear verdicts and social inflation.

38%

of business leaders are **somewhat concerned** about nuclear verdicts and social inflation.



From 2010 to 2019, the average award for [general liability verdicts](#) increased by [224%](#).

The cost of corporate nuclear verdicts nearly quadrupled after that, [from \\$4.9 billion in 2020 to over \\$18.3 billion in 2022](#).

Some sources are also coining a new label, [“thermonuclear,”](#) for verdicts exceeding [\\$100 million](#).

The risk for [nuclear verdicts extends across industries](#) but is exceptionally high in commercial auto, product liability, directors/officers, malpractice insurance, and professional liability cases.

This trend shows no sign of slowing down, with attorneys becoming increasingly adept at securing these massive awards through [strategic litigation tactics](#) and sympathetic juries. The threat of punitive damages adds an extra layer of uncertainty and financial burden if juries see a defendant’s actions as particularly reckless or malicious.

Third-party litigators are seeing the potential gain in providing financial support to plaintiffs and are driving award demands. In exchange for this funding, the litigators typically receive a portion of the settlement or judgment. When these verdicts go nuclear, the litigator’s portion can be quite significant and well worth their upfront investment.

The increased availability of funding for litigation is leading to more cases being pursued against corporations, and even plaintiff attorneys who are expanding their scope in identifying potential targets.

Social inflation risk solutions

Risk transfer mechanisms such as insurance are your business's safety net against harmful financial losses.

The ripple effects of nuclear verdicts extend beyond individual cases, impacting insurance premiums, C-suite and shareholder confidence, and ultimately, the bottom line of businesses across industries.

To address the inflation in settlement costs, underwriters are reviewing contracts more thoroughly to see that businesses have risk mitigation measures in place. Industries such as manufacturing, trucking, and construction that work closely with third parties or subcontractors also want to review these agreements to ensure enough protection exists between parties.

Robust risk management practices are key to securing the right coverage for your business. This includes processes that allow you to get ahead of potentially harmful claims and legal battles, and relationships with risk mitigation experts who can maximize their effects. The knowledge and expertise of your broker, your insurer, and your legal counsel can provide you with customized and appropriate risk mitigation and transfer approaches.

We've put together some general best practices to get you thinking about the topic.

Regular process reviews

Regularly reviewing your incident and litigation exposure can help prevent claims. The right broker will offer fleet solutions, behavioral driving programs, and safety and risk control services to supplement your own diligence.

Communication and collaboration with insurers

Open communication with insurers and brokers about potential claims allows for collaboration on strategies for resolution and the ability to optimize your insurance coverage to limit potential losses.

Early intervention tactics

Mediation and settlement negotiations can help resolve claims quickly and prevent them from escalating into costly legal battles.

Robust compliance programs

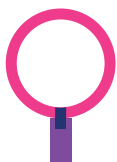
This includes staying updated and compliant on legal developments in your industry and maintaining best practices to minimize legal exposure.

Thorough record-keeping

Maintain documentation of business activities, transactions, and communications, which can serve as valuable evidence in the event of litigation and help defend against claims.

Vigilant monitoring and response

Constantly look for signs of potential litigation threats. Watch for any increased regulatory scrutiny or competitor actions, as these can be hints at what's to come.



For businesses interested in exploring innovative insurance solutions, one existing option is **punitive damages wraparound policies (puni-wraps)**. These policies, which pair a domestic policy with a wraparound policy offered by an offshore affiliate, can be tailored to cover punitive damages awards in jurisdictions where such awards are not typically covered by insurance.

The elephant in the room: global instability

While insurance and risk trends are often influenced by market fluctuations, technological advancements, regulatory changes, and the pervasive effects of geopolitical uncertainties are increasingly becoming the elephant in the room.

56%

of business leaders are **extremely or very concerned** about global instability.

49%

of business leaders are **extremely or very concerned** about the potential of domestic terrorism, civil unrest, and political violence.



Global factors such as climate change, high-stakes regional conflicts, and the spread of misinformation are introducing layers of complexity into the risk management landscape for all businesses and creating profound impacts affecting industries and economies worldwide.

Misinformation and disinformation is perceived as [the most concerning global risk](#) anticipated over the next two years. This is mainly due to the billions of people across several economies who are expected to head to the polls during this time [for the largest global election year in history](#). Ongoing conflicts and geopolitical tensions, such as those between Israel and Gaza, as well as Russia and Ukraine, are injecting more uncertainty into global markets.

With this global instability comes the potential and likelihood of continued supply chain disruptions, market volatility, regulatory changes, and political risk. Instability of global economic conditions, such as recessions and inflation, can also affect consumer spending patterns and investment decisions.

The role of insurance in mitigating risks and safeguarding businesses against global uncertainties has never been more critical. Traditional risk models may not adequately capture the multifaceted risks posed by today's climate. Instead, insurers are adapting their strategies, products, and services to better support businesses against unforeseen disruptions to help them strive towards resilience.

The ever-changing geopolitical environment is rife with uncertainties that have the potential to significantly impact your strategic plans and operational activities. Are you adequately prepared for the monumental global election year that lies ahead? Our [Political Risk Report guide](#) can help.

The future is not dire, but it is unclear.

The trajectory of each of these business risks will depend greatly on global conditions such as the:



Economy



Environment



Technology



Geopolitical relations

Businesses can expect this uncertainty and high-risk environment to continue in the short term, and those looking to grow and thrive will need to ensure they have the right partners and resources for the journey.

We are here to help.



Why face the current climate of uncertainty alone?

[Get in touch](#) with a Marsh McLennan Agency specialist for guidance, risk assessments, and resiliency-focused solutions that will help your business thrive.

This document is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. Marsh & McLennan Agency LLC shall have no obligation to update this publication 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 consultants and are not to be relied upon as actuarial, accounting, tax or legal advice, for which you should consult your own professional advisors. Any modeling analytics or projections are subject to inherent uncertainty and the analysis could be materially affected if any underlying assumptions, conditions, information or factors are inaccurate or incomplete or should change. d/b/a in California as Marsh & McLennan Insurance Agency LLC; CA Insurance Lic: 0H18131. Copyright © 2024 Marsh & McLennan Agency LLC. All rights reserved. MarshMMA.com

01-1273462864-0424

Business Insurance
Employee Health & Benefits
Private Client Services
Retirement & Wealth



A business of Marsh McLennan