# RISK MANAGEMENT

Q4 2025 RMmagazine.com

Navigating the Intersection of Political Expression and Employment Law pg. 4

How to Overcome Cognitive Biases in Risk Management pg. 38

## YEAR IN RISK 2025

A publication of RIMS the risk management society


RIMS-CRMP®

RIMS-Certified Risk Management Professional

# Lead with Confidence

## Earn the RIMS-CRMP Certification

In today's unpredictable world, organizations need risk leaders who anticipate, adapt, and deliver strategic value. The RIMS-Certified Risk Management Professional (RIMS-CRMP) certification proves you're that leader.

Whether you're advancing in your career or deepening your impact, the RIMS-CRMP:

- Validates your expertise in identifying and managing risk.
- Demonstrates your strategic value to leadership and stakeholders.
- Enhances your credibility with a globally recognized credential.
- Opens doors to greater responsibility and higher earning potential.

Trusted by risk professionals worldwide, the RIMS-CRMP is the only ANAB-accredited risk management certification in the world. Start your RIMS-CRMP journey today.

ANAB
ANSI National Accreditation Board
ACCREDITED
ISO/IEC 17024
PERSONNEL CERTIFICATION BODY

Learn More: **RIMS.org/Certification**

75 YEARS RIMS
the risk management society®

Volume 72, Issue 5

# contents

28

Cover: Shutterstock / Molibdenis-Studio
This page: Getty / Anadolu, Dimitar Dilkoff

## FEATURES


28 / **Year in Risk 2025**

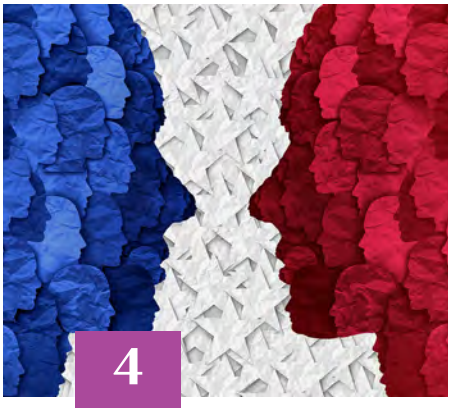
Our annual review of some the year's most notable risk events highlights the top challenges risk professionals had to address in 2025 and some that will shape the risk landscape in 2026.

38 / **How to Overcome Cognitive Biases in Risk Management**

By exploring the most pervasive biases shaping risk processes, risk professionals can better develop pragmatic techniques to counter their effects.

Volume 72, Issue 5

# contents



## WHAT'S INSIDE


4 **Navigating the Intersection of Social Media, Political Expression and Employment Law**
As people post political sentiments online and employers consider their response, what are the rights of employees and employers and the potential risks involved?

8 **Communicating Risk to the C-Suite**
In times of uncertainty, the ability to communicate risk with clarity, balance and strategic foresight is one of the most critical skills for risk leaders.

12 **Exploring Trade Credit Insurance in Response to Increasing Tariff Risk**
Surging tariff rates and new tariff announcements have highlighted the key role of trade credit insurance in safeguarding businesses engaged in international trade.

16 **Optimizing Your Enterprise Risk Management Strategy**
As ERM continues to evolve as a strategic advantage, these seven steps can help risk professionals enhance their organization's approach.

20 **Building Operational Resilience in Third-Party Risk Management**
Building operational resilience requires a comprehensive framework for strengthening your TPRM program.

24 **How Risk Professionals Can Navigate Potential Business Futures**
As more business leaders view resilience as essential to their organization, risk professionals must embed multiple perspectives into scenario planning.

42 **Findings**
The overlooked cybersecurity risk of misdirected email, mental health safety concerns in the workplace, and political risk loss trends.

44 **Hindsight**
The latest facts and figures on risk.


Shutterstock / Lightspring; DOERS


RISK MANAGEMENT

**Editor in Chief**
Morgan O'Rourke, *morourke@RIMS.org*

**Managing Editor**
Hilary Tuttle, *htuttle@RIMS.org*

**Editor**
Jennifer Post, *jpost@RIMS.org*

**Art & Production Manager**
Andrew Bass, Jr., *abass@RIMS.org*

**ADVERTISING**
**Account Executive**
Ted Donovan, *tdonovan@RIMS.org*
**T:** (212) 655-5917

A publication of RIMS, the risk management society

**Chief Executive Officer**
Gary LaBranche, *glabranche@RIMS.org*

*Risk Management Magazine* (ISSN 0035-5593) is digitally published 4 times per year, with a special issue in April, by the Risk and Insurance Management Society, Inc. Offices at 228 Park Ave S, PMB 23312, New York, NY 10003-1502; (212) 286-9364; Fax (212) 922-0716. Volume 72, Issue 4.



**AN AWARD-WINNING PUBLICATION**

AZBEE AWARDS WINNER
EXCEL AWARDS WINNER
FOLIO: EDDIES WINNER
GD:USA AWARDS WINNER

# Meet RICKY

RICKY is your go-to expert for all things RIMS! Whether you're curious about professional development opportunities, upcoming events, or membership benefits, RICKY has you covered.

**RICKY stands for:**
**R**isk
**I**ntelligence
**C**ontent &
**K**nowledge, all for
**Y**ou

Let RICKY be your guide to getting the most out of your RIMS experience.

**RIMS members get full access to RICKY.**

Start chatting with RICKY today: **RIMS.org/RICKY**

RIMS
the risk management society

Shutterstock / Lightspring

# Navigating the Intersection of Social Media, Political Expression and Employment Law

by Michelle Arbitrio, Karin Schaffer and Jacqueline Murphy

Social media has become the new public square as many people express their views on issues of political importance. Whether the subject is conflict in the Middle East, the ongoing war between Russia and Ukraine, U.S. politics or the assassination of political figures, employees increasingly take to platforms such as X (formerly Twitter), Facebook, Instagram and TikTok to share their views. These posts are often made in real time, are highly visible, and can go viral well beyond the author's intended audience. Keenly aware of public perception and the potential impact on their brands, employers are responding with swift and severe measures, including employees being terminated, suspended or placed on administrative leave based on their online speech.

In September 2025, the death of conservative activist Charlie Kirk and a wave of subsequent employment-related actions highlighted this precarious terrain. After Kirk was fatally shot, CNBC terminated a reporter following social media comments about Kirk's death. Other employees in various industries faced disciplinary measures for posts that either celebrated or condemned the event. These actions underscored the speed with which employers are now policing personal speech, as well as the broader social divide over how far employers should go to respond to the political commentary of employees outside the workplace.

## BLURRING THE LINE BETWEEN PERSONAL AND PROFESSIONAL

Employee conduct outside the workplace reflects on employers to varying degrees. For example, following the social media uproar around the "Coldplay affair," the number of online searches skyrocketed for Astronomer, the tech company where the individuals involved were employed, drawing widespread media attention and consumer backlash. The pervasiveness of social media has dramatically expanded the scope of what employers see and how

quickly they feel compelled or pressured to act. When an employee publicly posts commentary perceived as antisemitic, Islamophobic, racist, misogynistic or politically inflammatory, employers face immediate reputation risk. Media coverage about the account itself often identifies the employer by name, potentially leading to boycotts by advocacy groups or issues with suppliers or customers. Coworkers could also allege that the post creates a hostile workplace.

In response, employers increasingly err on the side of decisive termination rather than risk reputation damage or workplace discord. This is not confined to any one industry. Universities, law firms, hospitals, financial institutions and tech companies have all faced public scrutiny due to an employee's online activity. The message to employees is clear: The line between personal and professional spheres has blurred, and online speech can carry significant professional consequences.

**Both employers and employees should proceed with caution, guided by clear policies, informed counsel, and an understanding that the line between personal speech and professional consequence has never been thinner.**

## LEGAL RIGHTS OF EMPLOYEES

At the foundation of U.S. employment law lies the doctrine of at-will employment, which allows employers to terminate employees at any time, for any lawful reason—or for no reason at all—so long as the termination is non-discriminatory and does not violate a contract, statute or public policy. However, this broad discretion is not unlimited. Courts and legislatures have carved out significant exceptions that become particularly relevant when termination is tied to employee speech.

Generally, private-sector employees do not enjoy First Amendment protection for political speech in the workplace. The Constitution restrains government actors, not private employers. Thus, while a public employer disciplining an employee for political speech can introduce constitutional concerns, a private employer's decision to terminate usually does not.

In *Pickering v. Board of Education*, the Supreme Court established a balancing test for assessing public employee speech rights. Courts weigh the employee's interest in speaking on matters of public concern against the employer's interest in maintaining discipline, workplace harmony and efficiency. Subsequent cases have refined this test, emphasizing the importance of context, time, place and the employee's role.

For example, in *Jones v. Board of Regents University System of Georgia*, the court emphasized that speech must be made primarily in the employee's role as a citizen, not in their official capacity as an employee, to qualify for protection. Even then, disruption to workplace discipline or operations can justify restrictions. In *Garcetti v. Ceballos*, the court held that a public employee must show: 1) speech as a citizen on a matter of public concern, 2) an adverse employment action, and 3) that speech was the motivating factor in the decision. Yet even when these elements are met, employers may prevail if they can reasonably predict disruption that outweighs the speech's value.

Federal regulations also reflect this balance, permitting federal employees to vote, express opinions and participate in nonpartisan civic activity, but restricting political activity that interferes with official duties or undermines agency neutrality.

## ADDITIONAL STATUTORY PROTECTIONS

Some states extend explicit statutory protections to employees for lawful off-duty political speech and activity. California labor code prohibits employers from controlling or directing employees' political activities and from retaliation against employees for political expression. New York law similarly protects employees' lawful off-duty conduct, including political activities, and Colorado provides comparable protections. Courts applying these laws often weigh whether an employee's expression undermines legitimate business interests.

Anti-discrimination and retaliation statutes further complicate matters. Federal and state law prohibit adverse actions motivated by an employee's race, religion, national origin or other protected status. A termination tied to a post about the Israel-Hamas conflict, for example, could lead to claims of religious or national origin discrimination if the discipline disproportionately affects one group.

Unionized employees may also look to "just cause" provisions in collective bargaining agreements, which limit employers' ability to terminate for off-duty conduct without a demonstrated workplace nexus. Moreover, under the National

Labor Relations Act, employees engaged in "concerted activity" for mutual aid and protection may be shielded from discipline. Social media posts about workplace conditions, pay equity or organizing efforts can also fall under this protection, even if published on personal accounts.

In sum, employees retain free speech rights, but those rights are not absolute. Public employees must navigate the complex balance between First Amendment protections and government employers' operational needs. Meanwhile, private employees rely more heavily on state statutes, anti-discrimination laws and contractual protections. Across both contexts, courts apply nuanced analyses, ensuring that speech restrictions are justified by legitimate interests and are not so broad as to unduly burden constitutional freedoms.

## LITIGATION RISKS AND COURT APPROACHES

When employees challenge disciplinary actions linked to political social media activity, they frequently assert wrongful termination in violation of public policy, discrimination, retaliation or breach of contract. Courts analyzing these disputes generally weigh the employee's right to lawful off-duty conduct against the employer's legitimate business interests. Outcomes often hinge on whether the speech created a tangible workplace disruption directly in conflict with the employer's operations.

For example, a nurse posting racially charged comments could undermine patient trust in a hospital and justify termination, while a teacher expressing general political views outside the classroom may present a different consideration. Even when employers ultimately prevail, litigation is costly and reputationally damaging. Publicized lawsuits can magnify the very controversies employers sought to quell by acting quickly.

## POTENTIAL LIABILITY FOR EMPLOYERS

Employers typically justify termination decisions on grounds such as protecting reputation and brand integrity, preventing hostile work environments, meeting client and customer expectations, and preserving workplace productivity. These rationales are practical and often legally defensible, provided employers apply policies consistently and avoid discriminatory enforcement.

Nonetheless, pitfalls remain. Selective enforcement can trigger discrimination claims under Title VII of the Civil Rights Act. Overreach into employee speech risks unfair labor practice charges under the NLRA. Monitoring private or restricted-access accounts may invite privacy challenges, while mischaracterizing employee speech in termination announcements can result in defamation claims. In states that recognize implied covenants of good faith, arbitrary or pretextual terminations may face additional hurdles. To mitigate these risks, employers should:

- Develop clear social media policies that define expectations, provide examples and articulate consequences.
- Ensure consistency in enforcement so that similarly situated employees are treated alike, minimizing the risk of discrimination claims.
- Balance discipline with business necessity, considering less severe measures such as warning or suspension before termination.
- Train managers and HR leaders on lawful enforcement practices to avoid missteps.
- Document decisions carefully to establish legitimate business reasons for adverse actions.
- Consult with legal counsel before acting, especially when speech implicates sensitive issues such as religion, race or political affiliation.

## FINDING A BALANCE

The intersection of social media, political expression and employment law reflects a profound societal shift as private conversations now unfold on public platforms accessible to millions. Acutely aware of reputational and legal risks, employers are responding with unprecedented vigilance, often terminating employees for speech they deem inconsistent with organizational values.

This issue presents a delicate balance. Employees understandably wish to engage in political discourse, while employers must safeguard their brands, workplace harmony and compliance obligations. The legal terrain is nuanced, varying by jurisdiction and context. Both employers and employees should proceed with caution, guided by clear policies, informed counsel, and an understanding that the line between personal speech and professional consequence has never been thinner. RM

**Michelle Arbitrio** is an office managing partner and equity partner at law firm Wood, Smith, Henning & Berman LLP. **Karin Schaffer** is a partner at Wood, Smith, Henning and Berman LLP, where she focuses on complex civil litigation and advises clients on labor and employment issues. **Jacqueline Murphy** is a partner at Wood, Smith, Henning & Berman LLP, where her practice is focused on employment practices and professional liability.

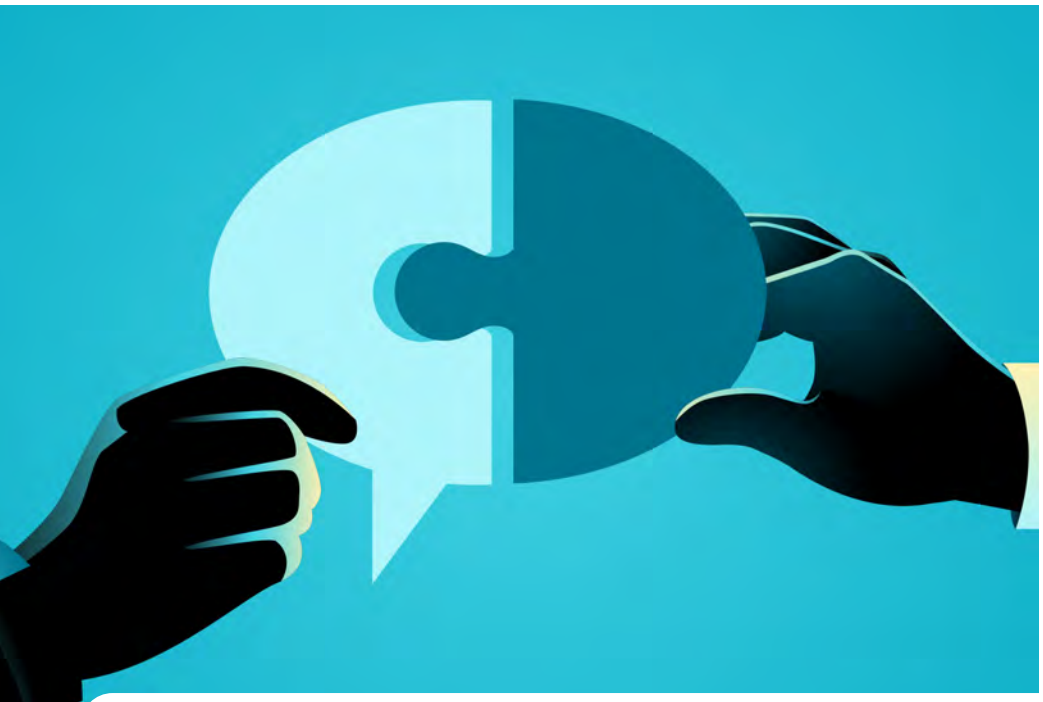
# WE WANT YOU

## To share your expertise and perspective

with your peers and help create a stronger and more vibrant risk professional community by contributing to *Risk Management*.

Visit **RMmagazine.com/contribute** for details on how you can get involved.


RISK MANAGEMENT



Shutterstock / rudall30; VisualBricks

# Communicating Risk to the C-Suite

by Caldwell Hart

Modern risks are rarely isolated and never static. Geopolitical tensions, economic shifts and environmental disruptions now intersect with increasingly complex supply chains, placing growing demands on organizational agility and resilience. For example, among the most headline-grabbing risks are tariffs, which have recently been imposed, lifted or altered with little warning, often disrupting procurement and operations. Risk managers know that focusing on a single issue like this, no matter how urgent, can lead to strategic blind spots. Risk managers must help the C-suite see beyond headlines, assess risk in a broader context and avoid over-indexing. In times of uncertainty, the ability to communicate risk with clarity, balance and strategic foresight becomes one of the most critical responsibilities of the modern risk leader.

## SEEING THE BIGGER PICTURE

With any risk, it is important to look at the bigger picture. Consider how the volatile nature of current U.S. trade policy has made tariffs an urgent concern. Shifts in import duties can quickly inflate costs, disrupt supplier relationships and force reactive adjustments to sourcing strategies. This presents a critical risk that demands detailed awareness and action, but there is danger in treating tariffs as a standalone risk rather than part of a wider ecosystem. A tariff change may drive companies to shift sourcing to alternate geographies. However, doing so may expose the company to new risks, such as reduced supplier quality, unfamiliar regulatory frameworks, logistics capacity and cybersecurity threats.

No risk exists in a vacuum, and messaging about risks should reflect that. It is essential to communicate with the C-suite in a way that highlights dependencies, not just singular disruptions. Senior executives have long relied on risk leaders for insight into external threats. However, increased expectations that companies respond immediately to global events can cause an organization to react before having all the information.

Executives are bombarded with information, and their natural instincts may be to act quickly. When tariffs dominate the news cycle, leadership may react by focusing solely on adjusting sourcing or renegotiating contracts. While urgency is understandable, single-risk responses may inadvertently introduce new vulnerabilities, increase costs and undermine long-term strategies.

This is why risk managers must communicate not just what the risks are but also provide the context by asking questions. For example: How likely is it that the risk will escalate? What is the timeframe? What is the opportunity cost of reacting immediately? What other initiatives could be delayed or deprioritized? What opportunity does reacting immediately present? And most importantly, what combinations

of factors are in play?

To support this kind of holistic, multidimensional thinking, risk professionals communicating with the board must focus on translating issues using clear, business-relevant language specific to the organization, and must take a balanced approach supported by facts.

## BREAKING DOWN SILOS

To communicate risk effectively, risk managers need visibility and engagement across the organization. Though tariffs originate from governmental trade policy, their effects impact many departments. Risk professionals should proactively collaborate across departments to build a comprehensive view of risk and resulting impacts on corporate goals. For example, consider:

- Partnering with engineering and operations teams to understand how sourcing changes could impact design and manufacturing timelines
- Engaging IT and cybersecurity teams to assess potential vulnerabilities introduced by new supplier integrations
- Gathering input from finance to model cost increases, margin compression or currency exposure
- Consulting compliance and legal teams to evaluate the regulatory implications of shifting suppliers or expanding operations into new regions

Breaking down silos and synthesizing input from different business areas can help create a more comprehensive and accurate risk assessment for senior leadership and other stakeholders that is grounded in facts and operational reality. This also demonstrates to leadership that the risk team is embedded in strategic decision-making, not reacting in isolation. With this balanced approach, the organization can develop a comprehensive plan to address near- and long-term considerations.

**Risk professionals communicating with the board must focus on translating issues using clear, business-relevant language specific to the organization, and must take a balanced approach supported by facts.**

## COMMUNICATING RISK WITH STRATEGIC CLARITY

Once a complete picture of risk is assembled, the next step is presenting it in a way that resonates with senior leadership. The objective is not to overwhelm the C-suite with detail, but to contextualize and prioritize risk so leaders can make swift, informed decisions. These key strategies can help:

**1. Anchor Risk to Business Objectives**

Always frame risks in terms of how they will affect growth, profitability, customer satisfaction and market reputation. For example: "If we react immediately to this tariff by shifting suppliers, we will increase short-term cost efficiency, but it could reduce our supplier diversity and increase exposure to labor compliance issues, undermining ESG commitments."

**2. Use Visual Tools to Show Interdependencies**

Risk heat maps, dashboards or spider charts can be powerful ways to display multiple risks and their interconnections. Instead of a long list of concerns, these visual tools show how different risks relate and where the most pressure points might form.

**3. Present Trade-Offs, Not Just Threats**

Every solution usually comes with a compromise. Strong C-suite communications should outline at least two scenarios, highlighting the preferred path and alternatives. For example: "Delaying a supplier shift may cost more in the short term but allows time for quality assurance and cybersecurity reviews. Accelerating the move could avoid potential tariff exposure but increases operational risk." This approach positions risk managers as strategic advisers, not just problem-flaggers.

**4. Balance Immediate Action with Long-Term Strategy**

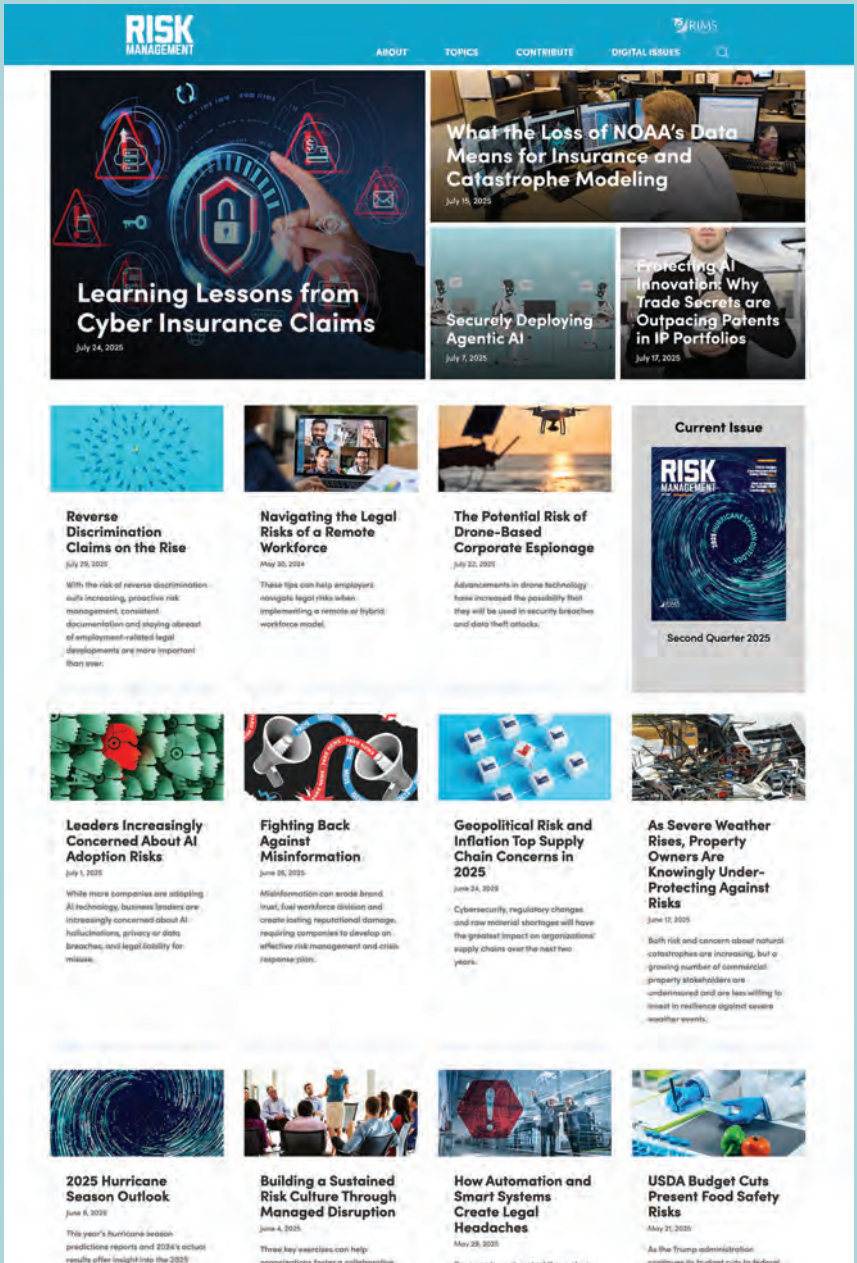
An organization's leaders are often looking for answers now. Risk managers must be able to defend both immediate responses and their alignment with long-term goals. Consider this example: "Our short-term mitigation for tariff increases is to absorb some of the cost, but we recommend a phased supplier transition plan over 12 months to ensure resilience and regulatory compliance in new regions." Providing a "now-and-next" plan builds credibility and keeps leadership grounded.

## THE EVOLVING ROLE OF THE RISK MANAGER

Tariffs may be the headline risk of the moment, but tomorrow, it could be sanctions, climate events, supply chain labor laws, AI compliance or all of these simultaneously. Risk managers must guide senior leaders through today's dynamic landscape of interconnected, ever-changing threats with measured, clear communication rooted in strategic insight. By synthesizing cross-functional inputs and framing supply chain risks within the organization's broader goals, risk leaders can become indispensable partners to the C-suite—not only in time of crisis, but as a constant presence.

**Caldwell Hart** is the principal of procurement and supply chain management at Avetta.

# Whatever the topic, we have you covered




From fundamental resources to news you can use, *Risk Management* has a wealth of content to help risk managers stay at the top of their game. Check out the *Risk Management* website to browse resources such as:

- **Topics Index** to help you find articles on key subjects like Cybersecurity, ESG, Disaster Preparedness, ERM, Emerging Risks and Diversity, Equity & Inclusion
- **Online Exclusive Articles**
- **Current Issue,** including our Digital Edition
- **Archive of Past Articles and Back Issues**

Visit **www.RMmagazine.com** to learn more.

RISK MANAGEMENT


Shutterstock / Lightspring

# Exploring Trade Credit Insurance in Response to Increasing Tariff Risk

by Russ Banham

As the Trump administration continues to impose a wide range of tariffs on U.S. imports, U.S.-based companies are facing significant financial uncertainty. Many are paying more to source goods and materials and are experiencing lower profit margins and reduced cash flow, resulting in payment delays or defaults and causing potential accounts receivable problems for global trade partners. Some businesses could face financial distress and, in severe cases, may even be at risk of bankruptcy.

Surging tariff rates and the turbulence of new tariffs being announced or revised at frequent, irregular intervals has magnified the critical role of trade credit insurance in safeguarding businesses engaged in international trade. This coverage absorbs losses due to non-payment of commercial debts, however, relatively few companies have purchased this form of protection.

"Given the current tariff situation, trade credit insurance absolutely should be on a risk manager's radar," said Jerry Paulson, senior vice president in HUB International's complex risk practice. "If a company has to pay 15% to 20% more for raw materials [because of a tariff], the financial impact can be severe. Trade credit insurance helps solve this dilemma by covering the risk of unpaid invoices caused by a customer's insolvency, mitigating the risk of buyer defaults while freeing up capital and improving cash flow."

Approximately 15% of global trade is covered by trade credit insurance, according to the International Credit Insurance and Surety Association. Although a March 2025 survey by insurance broker WTW suggested increasing customer demand, most companies engaged in global trade choose not to buy the coverage, either due to perceptions of high cost or restrictive coverage terms, condi-

tions and exclusions. However, brokers note the current geopolitical climate and growing uncertainty over U.S. tariffs and trade disputes may prompt businesses to rethink the value of this insurance line.

"Most global trade is done on open account terms, where goods are shipped and delivered before payment is due," said Ian Watts, credit risk specialty growth leader at WTW. "Companies cannot manage that risk [of non-payment] without trade credit insurance."

Aside from reducing the risk of non-payment, trade credit coverage increases the confidence of importers to do business with companies they may otherwise have spurned or neglected in the past. As the exporter's sales volume increases, cash is freed up to invest into their business for innovation and growth.

"One cannot dismiss the importance of the insurance as a risk mitigant, regardless of the size of the company and whether you are a manufacturer or a wholesaler," said Marc Wagman, managing director of credit and political risk at Gallagher. "Typically, receivables—the lifeblood of a company fueling cash flow—are the largest uninsured asset on the balance sheet. Having the insurance greases the wheels of global trade."

## HARD TIMES AND HARD LESSONS

It is difficult to estimate the number of insurance carriers offering trade credit policies globally, with some reports suggesting around two dozen insurers and government entities, while others peg the total significantly higher. Regardless of the number of providers, it is clear the aggregate size of the market is substantial. The trade credit market is on target to reach $13.3 billion this year, up from $12.2 billion in 2024, demonstrating a compound annual growth rate of 8.9%, according to the Business Research Company.

> **"This is a very mercurial administration. A lot of it is posturing with our trading partners. [President Trump] takes astonishingly unreasonable first positions to get trading partners' attention."**

For years, the trade credit insurance market was relatively stable. When the COVID-19 pandemic began to emerge at the end of 2019, the market suddenly hardened. Many governments mandated lockdowns and closed borders, disrupting global supply chains and trade flows. The volume of trade credit claims shot up significantly. Insurer Euler Hermes (now Allianz Trade) reported huge increases in claims throughout April, May and June 2020. In response, some insurers withdrew their capacity and others decreased their credit limits and became more cautious in their underwriting.

"I was a commercial underwriter at trade credit insurer Coface when COVID hit," said Sam Rodda, now a client manager of trade credit insurance and political risk at insurance broker Lockton Australia. "The primary markets hardened and increased rates 20% to 30% and the excess [market rates] doubled. Some coverages were cut back 20%."

Governments intervened to alleviate the negative market consequences. Wanting to support businesses and ensure trade credit insurance coverage and credit limits were maintained during the coronavirus pandemic, the United Kingdom established a temporary £10 billion ($13.4 billion) trade credit reinsurance scheme. The government acted as a reinsurer to private trade credit insurers, sharing the risk of losses. "If the trade credit market pulled back their appetite, it could strain supply chains further, creating a much bigger impact," said Sarah Murrow, president and CEO of Allianz Trade Americas.

Comparable programs were also implemented in other countries, such as France and Germany, but not in the United States. "As was demonstrated during COVID, trade credit insurance is vital to keeping liquidity in supply chains," she said. "It is the glue that keeps world trade going."

## THREATENING THE STATUS QUO

The latest blow to global trade equilibrium is President Donald Trump's tariff strategy, characterized by his inclination to issue unpredictable waves of high tariffs and seemingly arbitrary deadlines, retreat from these decisions, and then impose even higher tariffs. Although the trade credit insurance market is stable for now, the president's vacillating tariff pronouncements could change the status quo. The Trump administration seeks trade reciprocity, where foreign companies face comparable tariffs when their goods enter U.S. markets that U.S. companies confront when their goods enter foreign markets.

For example, in February, President Trump issued a 10% percent tariff on Chinese imports, increased it to 20% a few weeks later, and then raised it to 145% in April. The next month, he reduced

the effective tariff rate to 30%. Then in October, he threatened an additional 100% tariff on Chinese goods that would go into effect on November 1. The president has made similar on-again, off-again tariff declarations to nearly all U.S. trading partners, including a 10% tariff increase imposed on Canadian exports in October after a dispute over an anti-tariff political ad from the government of Ontario.

"This is a very mercurial administration," Wagman said. "A lot of it is posturing with our trading partners. [President Trump] takes astonishingly unreasonable first positions to get trading partners' attention."

Assuming high tariffs remain in place for the foreseeable future, an unfavorable impact on trade credit insurance is likely. In a July survey by KPMG, 57% of U.S. companies reported declining gross margins as a direct result of having to pay more for foreign goods. Nearly half the respondents said it is taking them from seven months to a year to implement supply chain changes that are needed to offset high tariffs. "Businesses are navigating a trade environment that is no longer defined by short-term volatility but by sustained disruption," Joe Lackner, industrial manufacturing advisory partner at KPMG US, said in a press release.

Several economists also predict that tariffs will increase pressure on companies experiencing financial strains, leading to higher rates of insolvencies down the line. U.S. bankruptcies through March 2025 were at their highest level since 2010, according to data compiled by S&P Global Market Intelligence. Experts are monitoring the evolving insolvency picture closely.

"In certain sectors, we are coming to a point where [customer] vulnerability is increasing, causing insurers to start to reduce cover," Watts said. "Anything in the external economic environment creating additional risk for companies—tariffs, high interest rates, geopolitical tensions—will be plugged into the algorithms and risk assessments. For longer-term risks, there is a possibility that capacity may be reduced and prices will rise."

> **"This is a great opportunity for risk managers to present the value of trade credit insurance to their CFO or treasurer while there is still plenty of insurance market capacity, strong carrier appetite and aggressive pricing."**

## A STABLE MARKET FOR NOW

Despite ongoing tariff uncertainty, the trade credit insurance market remains stable, which is good news for companies buying and selling goods around the world. Insurance brokers and carriers report that prices remain competitive. Capacity is at a near-high point, with multiple carriers offering coverage in addition to the three largest providers. Allianz Trade, Coface SA, and Altradius together hold approximately 70% of global risk capacity. "Globally and in the United States, we have a prolonged soft market for trade credit insurance," Murrow said.

She attributed the present market to the low claims environment that followed the hardened conditions during the COVID-19 pandemic, a period of sharply reduced capacity, tighter underwriting and higher pricing. Credit insurers have since been able to build up their reserves and be more competitive in their risk appetite, she explained.

Even for exporters in countries confronting high U.S. tariffs, the soft market has persisted. For example, President Trump imposed a 35% tariff on goods from Canada starting August 1. Yet, according to Michelle Davy, president of insurance broker CrediAssur and past board chair of the Receivables Association of Canada, "it remains pretty competitive out there, with trade credit insurers still fighting for deals and few insurers exiting the market."

So far, this has been the case in the United States as well, according to U.S.-based insurance brokers. "Pricing is holding firm, unlike talks of double-digit year-over-year declines in terms of what property/casualty underwriters are quoting—that is not happening in our market," Wagman said. "To write risk on both a portfolio and single situation basis, the capacity is definitely there."

However, the lingering impact on suppliers in countries facing steep tariff increases could quickly alter market capital and appetite as companies may seek to replace those suppliers with suppliers in countries facing lower or no U.S. levies. Such a replacement strategy would result in lost income affecting the original supplier's financial condition, particularly if the U.S. buyer contributed a substantial part of the company's revenue and profits. The pressure on the supplier's bottom line could result in payment defaults, generating trade credit losses for insurers. Extrapolated across innumerable global suppliers, the soft market conditions may harden.

"The trade credit market should expect to see more losses overall than normal," said Julie Potter, senior vice president and

Shutterstock / Graphic and Photo Stocker

head of insurance and small business partnerships at trade credit insurance provider Export Development Canada (EDC). "For us, our loss ratio is increasing." High U.S. tariffs on Canadian exporters have also compelled some insureds to pause their decision to purchase coverage while they monitor the situation. "The way I look at it, we will likely have more losses," she said. "When something changes in the system, that is to be expected."

However, Potter is optimistic that the impact would be short-lived. "In general, as we have seen before, companies are usually able to get through the valleys," she said. "They are quite agile. We had the financial crisis and the pandemic and got through them, and we will get through this, as long as [trade credit insurance] markets do not lose their risk appetite."

For the time being, buyers of trade credit insurance still have the upper hand, and should be able to negotiate comparable if not better trade credit terms and prices than at their last policy renewal. "Despite the doom and gloom, it is a good time to buy credit insurance," Murrow said. "Even though tariffs are at their highest levels since 1940, trade deals are still being made."

She pointed out that many companies are rerouting their supply chains to suppliers in countries with lower tariffs. "The [trade credit insurance] markets are very much in a wait and see moment to see what shakes out. It continues to be a work in progress," she said.

As a result, this may be an advantageous time for risk professionals to explore coverage options. "This is a great opportunity for risk managers to present the value of trade credit insurance to their CFO or treasurer to absorb accounts receivable risks while there is still plenty of insurance market capacity, strong carrier appetite and aggressive pricing," Paulson said. "For those who do not already have a seat at the executive table, this is the invitation." R

**Russ Banham** is a veteran business journalist and author based in Los Angeles.


Shutterstock / JourneyStudio7

# Optimizing Your Enterprise Risk Management Strategy

by John Rogula

In recent years, businesses have had to navigate a string of large-scale disruptions, underscoring that resilience is essential. As a result, enterprise risk management is evolving from a compliance exercise into a strategic advantage. As a structured, systematic approach to assessing and managing a broad range of strategic, operational, financial and compliance risks across an organization, ERM helps businesses stay ahead of volatility.

With rapidly advancing technologies, shifting regulatory environments and increasing interconnection among global markets, a proactive, risk-informed culture is critical. These seven considerations can help risk professionals enhance their organization's ERM approach:

## CULTIVATE A RISK-INFORMED MINDSET ACROSS THE ORGANIZATION

At its core, ERM aims to build resilience and align risk with strategic growth. That begins with mindset, which involves understanding an organization's risk profile and aligning risk tolerance with strategic objectives.

A risk-informed mindset must start at the top and cascade through the entire organization. Corporate boards should engage in risk-based discussions to ensure organizational security and work with management teams to integrate ERM into organizational strategy. In turn, management should foster a risk-aware culture, educating employees about the importance of risk management and encouraging proactive risk identification.

## UNDERSTAND THE ORGANIZATION'S RISK PROFILE

Effective ERM starts with the risk management team having a deep understanding of the organization's internal and external risk profile, supported by risk assessments that gather insights from a wide set of stakeholders. Often supported by audit committees, risk managers must conduct ongoing assessments that incorporate input from across the organization. This threat detection process empowers the team to analyze and implement risk mitigation strategies that enable the organization to thrive.

It is essential that the risk management team work closely with the organization's board to ensure they are aware of the most consequential risks facing the organization, such as market trends, regulatory changes and supply chain disruptions. Understanding the operational threats and overall risk landscape will help ensure the board is making well-informed decisions that enhance resilience.

Risk managers should also familiarize the board with the risk management strategies already in place. This awareness ensures that board actions and decisions support ongoing risk mitigation efforts and create opportunities to strengthen the risk management team.

## ALIGN RISK TOLERANCE AND APPETITE

Once the board and risk management team understand the risk profile, it is important to

solidify the organization's risk tolerance and risk appetite. Before formulating an updated response plan, it is essential for the board and risk professionals to reach a consensus on the level of risk they are comfortable taking on to maintain desired performance levels.

It is equally important for other internal stakeholders to comprehend the agreed-upon risk tolerance and appetite. Although the board does not need to be involved in every decision, it is vital that the risk management team and other leaders are aware of the board's stance, enabling them to make informed strategic decisions that align with the established risk tolerance level.

These discussions should be approached as opportunities for organizational enhancement and alignment. Given that risk is defined as future uncertainty with both positive and negative potential outcomes, companies must manage both the upside and downside of risks. By reframing risks as opportunities for positive change rather than merely consequences to avoid, organizations can remain prepared to capitalize on organizational changes.

## PLAN FOR BLACK SWAN RISKS

Traditional risk analysis typically relies on two criteria: the impact of a risk and the likelihood of its occurrence. During risk assessment, equal weight is often given to both factors, but this approach can be short-sighted and may ultimately hinder progress toward the organization's strategic objectives.

Assigning equal importance to impact and likelihood tends to minimize black swan events—rare occurrences with extreme consequences. Recent global crises have demonstrated that the improbable is possible, and black swans cannot be ignored. The COVID-19 pandemic and the 2024 CrowdStrike outage are examples of foreseeable yet unlikely events that significantly disrupted business operations. While many organizations had identified these events as possible risks, they under-prioritized preparation or mitigation due to the low likelihood assessment. That approach left organizations unprepared for these black swan events, which profoundly affected both internal and external stakeholders.

To effectively address potential black swan risks, risk managers must shift from probability-based thinking to impact-based planning, preparing for extreme outcomes even if their likelihood seems low. Resilient organizations develop contingency strategies that encompass the full risk environment—not just the most likely events.

**At its core, ERM aims to build resilience and align risk with strategic growth. That begins with mindset, which involves understanding an organization's risk profile and aligning risk tolerance with strategic objectives.**

## ADOPT A COLLABORATIVE APPROACH TO ASSESSMENT

Risk managers must understand the importance of conducting risk assessments for identifying, analyzing and prioritizing risks to avoid strategic missteps, missed opportunities and worst-case loss scenarios. However, traditional risk assessment methods often come with challenges in ensuring timely representation of all stakeholders and gathering meaningful, actionable data. Most risk assessments rely on manual methods like interviews and surveys to gather insights from various stakeholders and external sources. This process can be cumbersome and prone to errors, focusing mainly on threats while neglecting opportunities.

Collaborative methodologies and tools can address these challenges, enhance the risk assessment process, and enable organizations to proactively mitigate risks and uncover growth opportunities. As risks become more interconnected, managing them in isolation is impractical. Traditional ERM methods often use impact and likelihood criteria, which provide a limited view and overlook risk tolerance and strategic goals. An improved collaborative approach offers a holistic perspective by leveraging historical data, industry benchmarks, continuous monitoring and communication. This approach involves stakeholders across the organization, which can enhance early detection of emerging risks and effective prioritization, boosting resilience and fostering a stronger risk culture.

## LEVERAGE COLLABORATION TOOLS

Relying on traditional ERM methods to conduct a collaborative risk assessment that involves multiple stakeholders and up-to-date insights can be difficult, costly and time-consuming. Leveraging collaboration tools can help enhance an organization's approach to ERM.

Technology-based collaboration tools allow for quicker, more efficient risk assessments with higher-quality outputs and facil-


Shutterstock / Nichcha

itate remote collaboration, allowing broader stakeholder inclusion and enriching risk identification with diverse perspectives. These tools can also capture risk information anonymously, encouraging diverse input and providing a voice to all stakeholders. Real-time collaboration automates repetitive tasks, which can enable teams to focus on outcomes and foster deeper discussions and better alignment on key risks.

## DEVELOP AN ENHANCED ERM APPROACH

Enhanced risk assessments necessitate collaborative methodology and technology-enabled tools. Effectively leveraging collaborative tools can significantly enhance both the risk assessment process and the quality of the data it produces, enabling organizations to continuously plan for what is on the horizon.

Enhanced ERM can be broken into three phases:

**1. Data collection:** In this phase, the focus shifts from merely identifying risks to informing strategy. This involves questioning how the organization measures success and identifying significant roadblocks. Technology-enhanced assessments can leverage a risk universe tools that list multiple sector-relevant risks to broaden perspectives and gather richer data.

**2. Risk analysis and prioritization:** Collaboration software can help engage individuals, prioritize risks and build consensus quickly, reducing the traditional data collection period. The analysis and prioritization phase takes risk tolerance, management preparedness and risk velocity into consideration, emphasizing high-impact events and necessary responses.

**3. Outcome and reporting:** Technology-driven collaboration tools can help assess risk scenarios, foster stakeholder consensus and quantify impacts. These tools automate reporting, providing timely and insightful analysis that shapes response plans and guides strategic decisions.

Enterprise risk management is not about avoiding failure—it is about enabling agility, insight and growth. By fostering a risk-aware culture and leveraging collaborative, tech-enabled tools, organizations can not only weather uncertainty but transform it into a strategic advantage. R

**John Rogula** is the managing director of risk advisory at Baker Tilly.

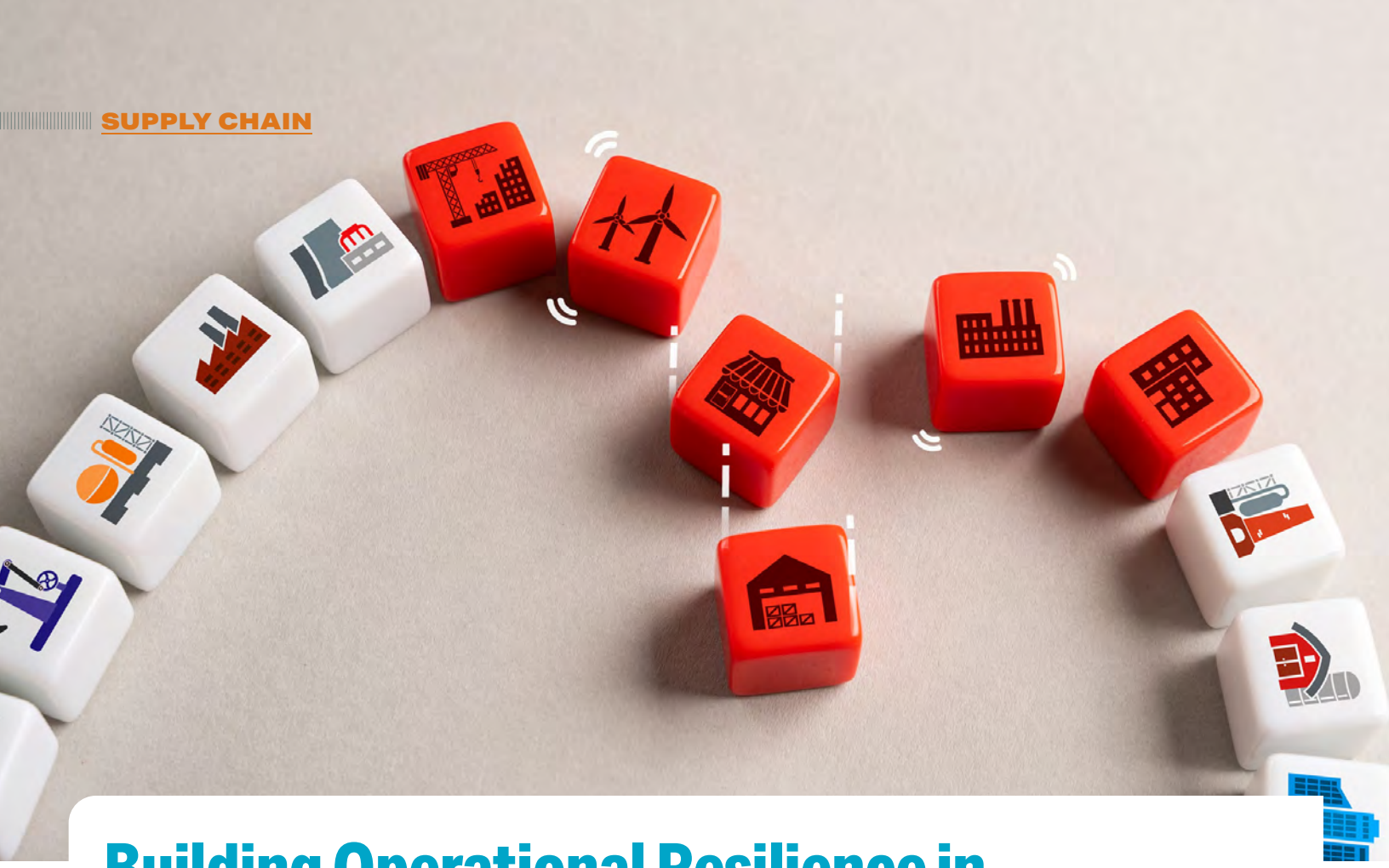
# GLOBAL THREATS

Since 1954, *Risk Management* has provided readers with the latest in risk management news, insight and analysis.

Whether it is dynamic issues of cybersecurity, the emerging risk landscape, reputation risk, insurance, disaster preparedness, or anything in between, **we are the authority** on information you need to meet the challenges of today's evolving business landscape.

Visit **RMmagazine.com** for our article archive.


RISK MANAGEMENT



Shutterstock / Andrii Yalanskyi

# Building Operational Resilience in Third-Party Risk Management

by Ryan Patrick

Third-party risk management (TPRM) has reached a critical inflection point. Traditional approaches focused on compliance assessments and security questionnaires are proving insufficient for today's interconnected business environment. From ransomware attacks to supply chain failures and cloud outages, high-profile disruptions have exposed a fundamental gap: Organizations are measuring vendor security, but not vendor resilience.

When a single vendor goes down, the ripple effects can be catastrophic for every business that relies on them. This is forcing organizations to rethink their approach to TPRM and expand their focus from reactive risk assessments and compliance checkboxes to proactive resilience and business continuity. It is not enough to ask if a vendor is secure—the better question is if an organization can withstand the operational impact if that vendor is taken offline tomorrow.

Most TPRM programs excel at evaluating whether vendors protect data but struggle to assess whether they can maintain operations under pressure. A vendor might have pristine SOC 2 reports and ISO certifications yet lack the recovery capabilities to withstand a major disruption. This gap becomes critical when you consider that modern businesses often depend on dozens of third-party services for core operations.

The Change Healthcare breach illustrated this perfectly. As a payment intermediary handling billions in medical claims, the company's operational failure affected its business as well as teh businesses of thousands of healthcare providers that could not process payments, verify insurance or fill prescriptions. The compliance frameworks that validated Change Healthcare's security

posture had not captured its role as a critical dependency for an entire industry.

## A FRAMEWORK FOR RESILIENT TPRM

Building operational resilience requires a systematic approach that goes beyond traditional risk assessments. The following is a comprehensive framework for strengthening your TPRM program:

**1. Map Critical Dependencies and Business Impact**

Start with a thorough dependency-mapping exercise that identifies which vendors you use and how critical they are to your operations. Creating a dependency matrix can help simplify this process. Categorize vendors by asking:

- What business processes would halt if this vendor went offline?
- How difficult would it be to replace this vendor or implement workarounds?
- How would a vendor outage affect your customers, partners or stakeholders?

Business impact scores can be based on revenue loss, operational disruption and regulatory exposure. This helps prioritize where to focus your resilience efforts. An organization should also trace and document how a vendor failure would impact various areas of the business. Often, the most critical dependencies are not obvious until you map the connections.

**2. Expand Risk Assessments Beyond Security Controls**

When evaluating third parties, go beyond cybersecurity policies. Ask about their disaster recovery plans, recovery time objectives and recovery point objectives. Additionally, ask them to demonstrate backup systems, data replication strategies, incident response procedures, escalation protocols, and business continuity testing frequency and results.

If a vendor is unwilling or unable to provide this information, that is a red flag. Operational transparency is now as important as technical security and vendors should be willing and able to demonstrate their monitoring capabilities, communication protocols during incidents and historical performance during disruptions.

**3. Strengthen Internal Contingency Planning**

Organizations cannot control whether a vendor experiences problems, but they can control their response. The most resilient organizations prepare for vendor failures with the same rigor they apply to other business continuity scenarios. Each critical vendor needs a vendor-specific contingency plan, including pre-identified alternative providers with which you have established relationships, manual workarounds for key automated processes and clear decision criteria for when to activate backup plans.

The goal is to build operational buffers before they are needed, which means maintaining relationships with secondary vendors, keeping backup systems ready for activation and training staff on emergency procedures. Organizations should also account for the hidden costs of vendor disruptions including overtime, expedited services, revenue loss and customer retention efforts. The key is not leaving it up to contingencies that take weeks to implement or leave an organization scrambling for emergency funds in the middle of a crisis.

**4. Implement Dynamic Risk Monitoring**

Annual risk assessments might be inadequate in today's fast-moving threat landscape. Modern TPRM requires continuous monitoring that spots problems before they become crises. The best monitoring systems help organizations understand patterns, predict issues and continuously refine vendor risk assessments based on real-world performance.

Consider deploying comprehensive monitoring that tracks both security and operational health indicators, including automated alerts for vendor security incidents and performance degradation, financial stability monitoring through credit ratings and newsfeeds, and social media and industry intelligence for early warning signs.

If an organization is just getting started with a TPRM framework, it should focus on calibrating alert systems to minimize noise while maximizing signal. Too many false alarms and a team becomes numb to warnings; too few and a team is caught off guard when genuine threats emerge. The sooner an organization knows a vendor is compromised, the faster it can activate contingency plans.

**5. Foster Collaborative Vendor Relationships**

The strongest vendor relationships are built on shared responsibility for resilience rather than one-sided auditing. Treat critical vendors as strategic partners invested in mutual success and establish transparent communication protocols that define the method and timeframe for incident notification, what information they will provide during disruptions and clear escalation paths for critical issues.

An effective way to strengthen a vendor relationship is to invite them to engage in joint resilience planning through regu-

lar business continuity exercises, shared threat intelligence and co-developed incident response procedures. When vendors understand how their failures impact the business they work with, they are more likely to invest in preventing those failures. Organizations can also design service-level agreements that reward resilience, preferred vendor status for operational excellence and financial penalties for avoidable disruptions.

**6. Build Organizational Resilience Capabilities**

Internal capabilities determine whether contingency plans succeed or fail under pressure. The most prepared organizations invest in people, processes and governance structures that can execute effectively during vendor crises.

Team members from the IT, legal, business continuity and communications departments should be part of an active cross-functional response team. The key here is having the right people on the team. They need to work together regularly and understand each other's capabilities before a crisis hits. Realistic exercises that go beyond theoretical tabletop discussions can include scenario-based drills that simulate actual vendor failures, technical exercises that test backup system activation and communication drills for managing stakeholder expectations.

Every organization needs clear governance structures that define decision-making authority during crises. This includes who can authorize expensive backup systems, approve emergency contracts and speak for the organization during outages. Without clear governance, vendor crises often become organizational crises.

The organizations that adapt to current TPRM needs will be the ones that thrive in an increasingly interconnected and disruption-prone business environment. Those that cling to compliance-only approaches risk being caught unprepared when the next major vendor incident occurs. R

**Ryan Patrick** is the vice president of market research and adoption at HITRUST.



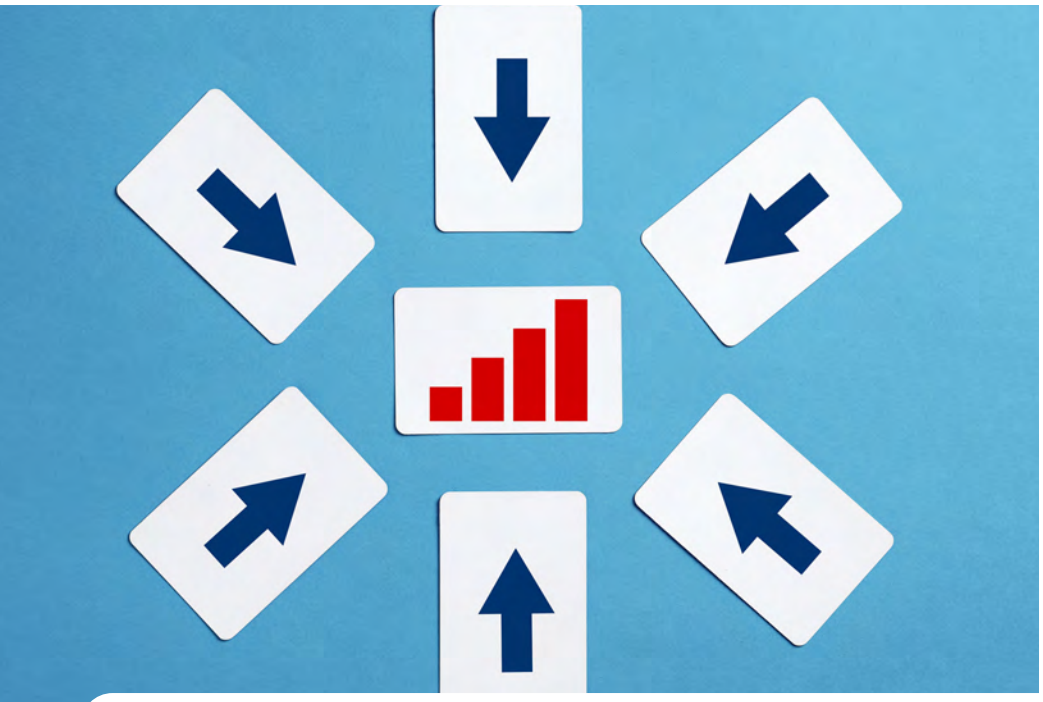

# Helping Risk Professionals Succeed in a Digital World



Access current and past issues of *Risk Management* for award-winning content about ERM, cyberrisk, natural catastrophes, emerging risks and insurance.

Experience the best of *Risk Management* on your mobile devices today.

Available at **rmmagazine.com**.

Shutterstock / Çağkan Sayin

# How Risk Professionals Can Navigate Potential Business Futures

by Ric Opal

As a result of rising geopolitical tensions, accelerating technology adoption and changing macroeconomic conditions, executive leaders view the current business landscape as less predictable than ever before.

According to BDO's *2025 Techtonic States Report*, 61% of global business leaders now view resilience as their organization's most important characteristic, a fundamental shift that reflects the new reality of operating in an increasingly volatile world. Once the backbone of risk management, traditional single-scenario planning is no longer sufficient in an environment of accelerating change.

When surveyed on their predictions for the future business landscape, 73% of executives said their organizations must prepare for multiple potential futures simultaneously, suggesting that this complex risk environment will persist indefinitely. Rather than viewing current conditions as a temporary disruption, organizations must adapt to a landscape where risk drives strategic decision-making and operational planning.

## THE FOUR WORLDS FRAMEWORK

BDO surveyed 1,050 C-suite leaders across 10 global markets, ultimately identifying four distinct potential business scenarios that could become reality by 2028. Each scenario, which forms the foundation of their "Four Worlds Framework," demands a fundamentally different risk management approach.

**World Fragmented** refers to a business environment with deeply segmented markets due to policy volatility, shifting geopolitical alliances and supply chain disruption. Current data suggests we are already operating in fragmented conditions, with 52% of leaders expecting this environment to persist. Of all the potential futures in the framework, this scenario has caught businesses most flat-footed, primarily due to inadequate early warning systems and over-reliance on previously stable supply chains.

**World Divided** is best described as geopolitical bifurcation that creates competing economic models between East and West. This scenario, which 33% of business leaders anticipate will become reality by 2028, is characterized by divergent regulatory standards, technology fragmentation and fundamentally different approaches to compliance across regions. In this world, organizations would face the challenge of operating across incompatible economic systems with conflicting requirements and compliance metrics.

**World Accelerated** is marked by rapid technological advancement and aligned global networks. While only 8% of leaders expect this scenario to occur, it would

require organizations to expertly manage artificial intelligence governance challenges, accelerated workforce adaptation needs and heightened cybersecurity vulnerabilities as technology transforms entire industries. With only 42% of leaders reporting that they currently have AI-ready data infrastructure, meeting these requirements would prove particularly challenging.

**World Sustained** represents measured, human-led technology adoption with gradual change. While the most moderate, it is the least likely anticipated business future, cited by 7% of leaders. While this environment is seemingly less disruptive, it carries the hidden risk of external shock vulnerability, as organizations optimized for gradual change may lack the agility to respond to sudden market disruptions.

## BUILDING MULTI-SCENARIO RESILIENCE

Businesses do not need to focus on identifying the "right" scenario—the imperative issue is building the capacity to succeed in any future. Specific risks and compliance challenges will vary depending on each organization's industry, geography, operating model and risk tolerance. Even if these scenarios evolve into hybrid versions or as entirely different business models unfold across regions and sectors, some preparations and investments can be universally applicable. To build resilience, organizations should focus on the following:

1. **Early warning systems** enable organizations to track leading indicators across all potential futures rather than waiting for one scenario to fully materialize. These systems should integrate social media monitoring, policy analysis and market intelligence to provide decision-makers with sufficient warning to implement contingency plans. This includes monitoring regional technology divergence, investment surges and regulatory stability.
2. **Digital agility** forms the foundation for success in business resilience planning, with employee-driven technology adoption creating more resilient and adaptable systems. Rather than restricting employee technology use, successful organizations encourage and monitor it, ensuring their workforce can adapt quickly when facing policy shifts, regulatory changes or rapid transformation.
3. **Supply chain diversification and flexibility** represent perhaps the most imminent preparatory measure across all scenarios. Whether confronting market segmentation, economic bifurcation or gradual change, diversified sourcing provides essential protection in each future business scenario. Organizations should move beyond isolated, transactional supplier relationships to create integrated networks that incorporate third-party vendors into crisis simulations. It is also imperative to develop contingency plans that activate automatically when specific triggers occur.
4. **Enhancing cybersecurity** remains critical as cyberattacks increase globally. With 76% of leaders expecting increased cybersecurity risk from market fragmentation and 68% citing technology advances as a reason for intensifying cyberrisk threats, comprehensive security must address multiple threat vectors simultaneously. Essential elements include immutable backup systems, consistent data recovery drills, and integrated cyber simulations involving all relevant stakeholders.
5. **Financial flexibility** refers to maintaining resources for both protection and opportunity. Organizations need to understand their value chain dependencies and keep reserves available for quick pivots when conditions change. This approach requires building intentional "slack" in the system—extra capacity that enables rapid response regardless of which future business model emerges.
6. **Stakeholder communication and trust** must be established before crises occur. Resilient organizations invest in stakeholder mapping and relationship building during stable periods, creating clear escalation, notification and reporting processes that maintain confidence in any scenario.

**Risk professionals must transition from protecting against known risks to becoming resilience architects who build organizational capacity to succeed in any future.**

Resilience also requires focusing on fundamentals that transcend the Four

Worlds scenarios. Customers will always demand quality products, competitive value and reliable delivery regardless of whether markets become fragmented, divided, sustained or accelerated. By anchoring investments while building scenario flexibility around them, organizations can create stable foundations for uncertain futures.

## THE RESILIENCE IMPERATIVE

Risk professionals must transition from protecting against known risks to becoming resilience architects who build organizational capacity to succeed in any future. This transformation requires abandoning the comfortable predictability of single-point planning in favor of frameworks that embrace uncertainty as a competitive advantage.

Effective risk management functions act like brakes on a sports car: They do not slow the vehicle down—they enable it to move faster with confidence. By pressure-testing initiatives against multiple scenarios, risk professionals can identify fragile assumptions and build robust alternatives that withstand various future conditions. This approach requires the integration of risk management directly with scenario-planning processes rather than treating it as an afterthought.

Organizations must embed multiple perspectives into scenario planning beyond simple best-case and worst-case thinking. They should include key stakeholder viewpoints to develop a holistic understanding of what each scenario means for their business, then build the architectural resilience to thrive regardless of which future emerges. The organizations that thrive will be those that prepare for multiple futures simultaneously, treating uncertainty not as a problem to solve but as a new normal to navigate indefinitely. R

**Ric Opal** is segment leader for cyber and IT solutions at BDO.

*Shutterstock / LAHMZ*

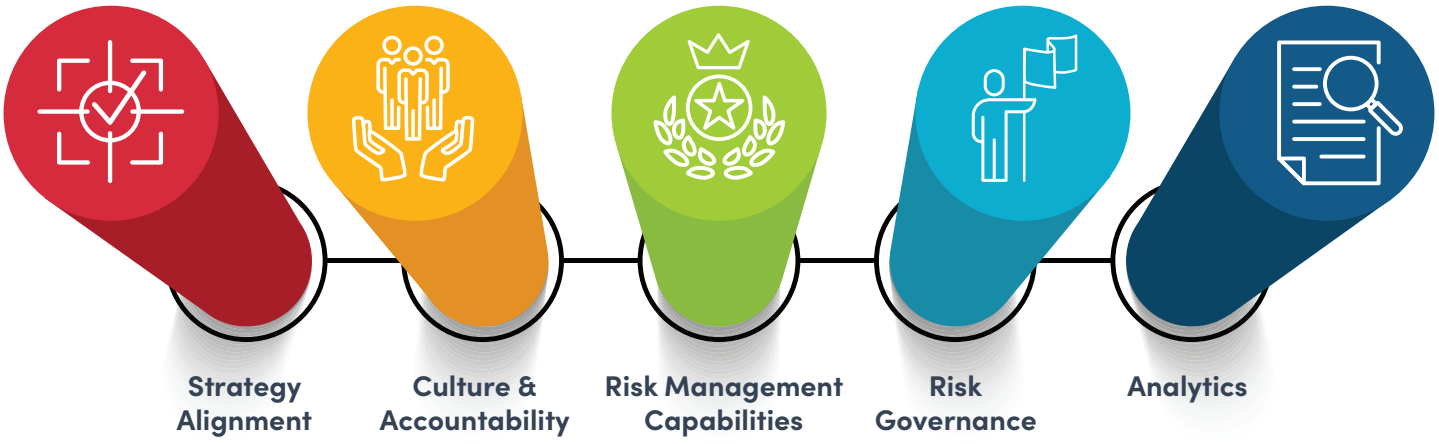
MEMBERS GET FREE ACCESS

# RIMS Risk Maturity Model®

## How does your organization compare?

Unlock the full potential of your organization with the RIMS Risk Maturity Model®! This powerful tool establishes your current risk maturity baseline and empowers you to identify the optimal risk maturity level for navigating change and futureproofing your organization.

Evaluate your organization against five pillars and 35 attributes deemed essential for success by leading risk management experts. Ready to discover how your organization stacks up?




**RIMS MEMBERS GET FREE ACCESS.**

Get started today at **www.RIMS.org/RMM**.

75 YEARS RIMS the risk management society®


by
Morgan O'Rourke
and Hilary Tuttle

**In 2025, organizations worldwide faced a broad range of risks, including natural disasters, climate change impacts, trade policy turmoil, reputation risk, cybersecurity threats, and legal and regulatory concerns. Our annual review looks back on some of the year's most notable risk events, highlighting top challenges risk professionals had to address in 2025 and events that will shape the risk landscape moving into 2026.**

## Los Angeles Wildfires Devastate Southern California [1]

***January 7***

A series of wildfires burned 57,000 acres of the Los Angeles metropolitan area, killing more than 30 people, forcing 200,000 to evacuate, and destroying more than 18,000 homes and businesses, including the houses of many celebrities. The fires were more severe due to acute drought conditions in Southern California and strong Santa Ana winds that reached hurricane force in some areas. Most of the damage came from the two largest fires, the Palisades and Eaton fires, which took three weeks to fully contain. Cumulative insured losses from the wildfires reached $40 billion and economic damages were estimated to be as high as $250 billion, making it not only the costliest wildfire, but one of the costliest natural disasters of any type in U.S. history. In August, researchers from Boston University and the University of Helsinki found that the fires may have ultimately caused an estimated 440 total fatalities when including indirect deaths from smoke and air pollution and disruptions to critical healthcare and other public services.

## 67 Killed After American Airlines Plane Collides with Army Helicopter

***January 29***

Moments from landing at Reagan International Airport outside of Washington, D.C., an American Airlines flight and a U.S. Army helicopter collided in midair, killing all 67 people aboard the two aircraft. The tragic accident was the deadliest air disaster in the United States since September 11, 2001. President Trump publicly blamed the Biden administration and "woke" policies for the incident, citing DEI hiring initiatives that have long been in place, but provided no evidence of any lack of qualifications or wrongdoing on the part of pilots or air traffic controllers. Indeed, the Trump administration implemented cuts and hiring freezes in the Federal Aviation Administration, despite federal officials warning for years about an overtaxed and understaffed air traffic control system that could lead to disaster. Air traffic controllers continued to grapple with understaffing and systemic problems throughout the year. During the government shutdown in the fall, air traffic controllers were required to continue working, despite not being paid for weeks and being told they might not receive back pay when the government reopened. The Trump administration also ordered significant reductions in air traffic in 40 major markets, causing days of chaos, delays and cancellations for commercial, private and cargo flights.


Getty / Anadolu

## Target Takes $12.4 Billion Hit After Walking Back DEI Commitments

***February 28***

The Trump administration has been vocal about targeting and suspending or rolling back DEI programs across the federal government, and many companies have followed suit. While some customers favor these moves, there has also been major consumer backlash against companies that are walking back their commitments. After making headlines for DEI commitments amid the Black Lives Matter movement, Target abandoned several DEI-related programs in January, including ending its "Belonging at the Bullseye" initiative to cultivate career development among employees of color, withdrawing from the Human Rights Campaign's Corporate Equality Index on LGBTQ+ inclusion, and "evolving" a program to promote supplier diversity in its procurement processes. Many consumers felt betrayed by the move, which drew negative press and prompted a boycott that appears to have had a notable impact. Target's stock plummeted by over $27 per share by the end of February, losing more than $12.4 billion in market value.

## Tornado Outbreak Causes Record $11 Billion in Damages

***March 13***

A widespread tornado outbreak struck the Midwestern and Eastern United States, killing 43 people and causing

$11 billion in damages over a four-day period. In terms of total damages, it was the costliest outbreak on record. Severe convective storm (SCS) activity including tornadoes reached an all-time high in 2025. As of December 10, the NOAA Storm Prediction Center had recorded 1,543 tornadoes in the United States this year, a 13% increase over the 15-year average of 1,368 during the same period. In the first nine months of the year, Gallagher reported economic losses from severe convective storms reached $61 billion, of which $42 billion was insured, making it the fourth-costliest SCS loss year for insurers. During that period, the United States saw 17 different billion-dollar SCS loss events, including an April outbreak of 157 confirmed tornadoes and flash flooding that caused $4.1 billion in damages as well as a May tornado outbreak that caused $5.9 billion in damages.

### Myanmar Earthquake Kills 5,300, Causes Widespread Destruction [2]

March 28

In one of the year's deadliest natural disasters, a magnitude 7.9 earthquake struck near the city of Mandalay in Myanmar, killing more than 5,300 people and injuring 11,000. Another 100 people were also killed in neighboring Thailand when the quake caused the collapse of a skyscraper that was under construction in Bangkok. In Myanmar, more than 48,000 homes and thousands of government buildings, schools, mosques, monasteries, bridges and other infrastructure were destroyed. While the quake caused an estimated $12 billion in economic damages in the country, Aon reported that less than $100 million was insured due to low insurance penetration rates. According to the World Economic Forum, the disaster exposed systemic risk factors

in the impoverished country, including unsafe housing and underenforced building codes, insufficient disaster planning, underfunded health systems, and a lack of social or fiscal safety nets.

### President Trump Announces Sweeping Tariffs at "Liberation Day" Press Conference [3]

*April 2*

On what he dubbed "Liberation Day," President Donald Trump signed an executive order imposing a baseline 10% tariff on imports from almost all U.S. trading partners around the world and higher reciprocal tariff rates of up to 50% on countries that were deemed to have the highest trade deficits with the United States. In response, global stock markets crashed and countries threatened steep retaliatory tariffs of their own. Days later, the Trump administration announced a 90-day pause of all country-specific tariffs, except for those imposed on China, and expressed a desire to negotiate separate trade deals with each country. The dramatic see-sawing around tariffs and uncertain trade policy continued throughout the year as President Trump threatened or imposed new levies on goods from various countries, including close trading partners, only to change position or amend terms later. While the administration has said that the tariffs will raise trillions of dollars in revenue, they have created major challenges for the broader economy and specific businesses, which have had to adjust their operations and determine how much of the cost to pass on to customers. Indeed, by October, according to Goldman Sachs, U.S. consumers were bearing as much as 55% of the costs of the tariffs as prices for goods and services continued to climb. Costco and other businesses have sued the

federal government seeking refunds on the duties collected, claiming the tariffs were levied illegally. The Supreme Court is currently weighing whether the president has the authority to unilaterally set tariff rates as the Constitution specifically grants Congress the power to assign and collect duties and regulate foreign commerce. The Trump administration has tried to seize this power on the grounds that it considers the trade imbalance a "national emergency."

### Ransomware Attack Wreaks Havoc on British Retailer Marks & Spencer

***April 19***

Iconic British retailer Marks & Spencer (M&S) was hit by a major ransomware attack that caused acute operational disruption from April into July. The attack forced the company to suspend online transactions, which typically account for £3.8 million ($5.1 million) in sales a day, and for in-store customers, store staff had to resort to pen and paper for billions of dollars' worth of food and clothing orders after shutting down automated stock systems. This also led to bare shelves and considerable reputation impact from frustrated customers, in addition to higher waste and logistics costs. Within a month, M&S lost £1 billion ($1.3 billion) of its stock market value, and the firm estimated the attack would cost about £300 million ($401 million), of which it hoped to recoup about £100 million ($134 million) from insurance. The attack is thought to have been carried out by the hacking group Scattered Spider, which used social engineering tactics to target a third-party vendor and ultimately gain access to M&S systems. Hackers also attacked British retailers Co-op and Harrods in 2025, prompting many retailers around the world to race to boost cyber defenses.

### Canadian Provinces Declare States of Emergency over Wildfires

***May 28***

On May 28 and 29, the Canadian provinces of Manitoba and Saskatchewan declared month-long states of emergency due to a number of concurrent wildfires deemed out of control. The fires were exacerbated by a local heatwave that broke 125-year records in Winnipeg. Some of this year's fires started as holdover fires from the record-breaking 2023 wildfire season.


Getty / VCG Andriy Onufriyenko Manuel Augusto Moreno

Also known as "zombie" or "overwintering" fires, holdover fires are peat fires that continue from year to year, smoldering under the snow during the winter and then growing more intense when the weather warms. Scientists believe zombie fires may become more common due to the impacts of climate change as they more frequently occur after hotter summers, which lead to drier subterranean vegetation and soil—the fuel these fires consume when hibernating underground. Ultimately, 2025 was the second-worst wildfire season in Canadian history, with the Canadian government reporting over 6,000 wildfires in almost every province and territory, burning a total of over 8.3 million hectares (20.5 million acres). From April through October, the risk and impacts of wildfires forced the evacuation of more than 85,000 people, including over 45,000 people from 73 First Nations communities. Smoke from the fires caused hazardous air quality across both Canada and parts of the United States and even polluted the air as far away as Europe.

### Courts Rule in Favor of Tech Companies in AI Copyright Cases

***June 24***

A U.S. district court judge ruled that Anthropic did not violate authors' copyrights when it used their books to train its AI tool Claude, categorizing the training process as "fair use," a legal doctrine that permits repurposing copyrighted work if it is substantially changed. Later that week, another judge ruled in favor of Meta in a suit brought by a group of authors that unsuccessfully argued that Facebook's parent company had violated their copyrights when training its AI system. However, the judge in the Meta case provided hope for authors and creative professionals in future AI suits. In "many circumstances," the judge said the use of copyrighted material in AI training would be considered illegal and that companies "will generally need to pay copyright holders for the right to use their materials," Indeed, in September, Anthropic agreed to pay a $1.5 billion settlement to the group of authors in the original class action suit for using their pirated books to create a central library for AI training. Currently, there are more than 40 pending cases that have been filed by copyright holders against AI companies in the United States, alleging infringement of content ranging from books and newspaper articles to images and music.


### Italian Court Sentences Executives to 141 Years in Prison for PFAS Pollution [5]

***June 26***

A group of 11 former executives of the Italian chemical company Miteni were sentenced to a total of 141 years in jail after they were found guilty of polluting the groundwater and soil of a 70-square-mile area in Northern Italy's Veneto region with per- and polyfluoroalkyl substances (PFAS). The chemicals contaminated the drinking water of 350,000 people in 21 towns and, according to a 2024 study in the journal *Environmental Health*, contributed to an estimated 4,000 excess deaths in the region from various forms of cancer and cardiovascular disease. The court also imposed over €75 million ($88 million) in civil penalties to compensate affected individuals and public entities and to pay for future cleanup and remediation efforts. A host of regulations banning or restricting the use of PFAS, often called "forever chemicals," were implemented or proposed around the world in 2025, including in Canada, the European Union, Australia, New Zealand and Japan. Many U.S. states also implemented PFAS bans or restrictions. At the federal level, rules governing PFAS reporting and contaminant levels in drinking water have been enacted in recent years, however, some of these requirements were eased or delayed by the EPA in 2025 to reduce the financial burden on businesses.

### 135 People Killed in Texas Floods [6]

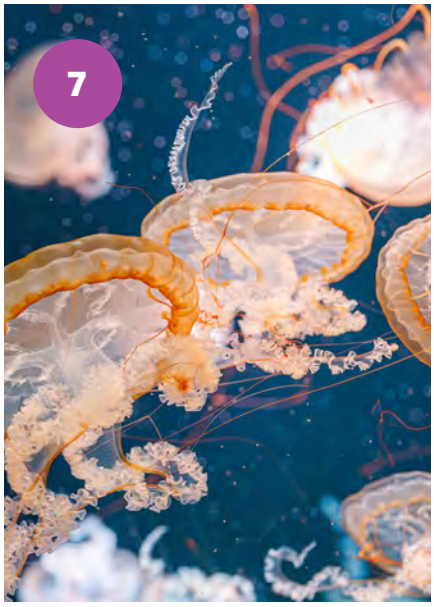
***July 4***

At least 135 people were killed by flash flooding in central Texas after the equivalent of four months' worth of heavy rain caused the Guadalupe River to rise 26 feet in just 45 minutes. Fatalities were primarily concentrated in Kerr County, where the 117 killed included campers and counselors at the Camp Mystic summer camp. Several factors contributed to the severity of the flooding, including the effects of climate change, the ineffectiveness of weather forecasts and evacuation alerts, and delays in disaster response efforts.


### Jellyfish Swarm Shuts Down French Nuclear Power Plant [7]

***August 11***

One of France's largest nuclear power plants was forced to partially shut down when a massive swarm of jellyfish clogged the intake pipes that feed the plant's cooling system. The blockage at Gravelines Nuclear Power Station triggered safety systems to automatically shut off four of the six reactors at the site, but according to the plant's operator, there was "no impact on the safety of the facilities, the safety of personnel or the environment." In early September, another swarm of jellyfish entered the pumping station filters at another French nuclear plant, forcing a shutdown that temporarily cut the facility's electricity generation in half. Over the past two decades, jellyfish have disrupted power plant operations in similar incidents in Scotland, Sweden, Israel, China, Japan and the United States. Marine experts believe these swarms are exacerbated by climate




change and warmer ocean surface temperatures, which lead to larger and more active jellyfish populations.

### EU Fines Google $3.5 Billion for Antitrust Violations

***September 4***

The European Commission fined Google €2.95 billion ($3.5 billion) for violating antitrust laws by favoring its own online display advertising technology services to the detriment of rival service providers. It was the EU's second-largest antitrust fine after a €4.3 billion penalty against Google in 2018. As required by the commission, Google has proposed several changes to its ad tech business in the EU to eliminate conflicts of interest. The penalty was part of a larger EU crackdown on tech sector business practices. In April, the European Commission fined Apple €500 million ($587 million) and Meta €200 million ($235 million) for violations of the Digital Markets Act, which establishes data transparency and interoperability requirements for large tech companies to ensure fair competition in digital markets. In December, Elon Musk's X was issued the first-ever penalty under the consumer-focused Digital Services Act. The company formerly known as Twitter was fined €120 million ($141 million) for the deceptive use of its "blue checkmark" to identify verified users, the lack of transparency of its advertising repository and the failure to provide access to public data for researchers.

### ICE Raids Georgia Hyundai Plant [8]

***September 4***

Agents from U.S. Immigration and Customs Enforcement (ICE) conducted a raid at a Hyundai Motor Group plant in Ellabell, Georgia, arresting 475 workers in what the U.S. Department of Homeland Security (DHS) described as the largest single-site immigration enforcement operation in the agency's history. More than 300 South Korean nationals were detained, straining diplomatic relations between South Korea and the United States and raising questions around the willingness of foreign businesses to invest in the United States in the future. The raid was part of the Trump Administration's aggressive campaign of immigration enforcement, which began in January with ICE agents across the country detaining suspected undocumented immigrants in workplaces, schools, hospitals, courthouses, parking lots and other public spaces. By September, DHS said that two million immigrants had been deported or had left the country on their own. The administration's policy has sparked protests because of the violent tactics of immigration agents, the legality of deportation operations, and the lack of due process afforded to detainees, some of whom were actually documented or U.S. citizens. Business owners have also expressed concerns about the risk to their operations due to a shrinking labor force and growing fear among many workers. Experts from the nonpartisan Peterson Institute for International Economics warned that, by 2028, mass deportations could reduce GDP by as much as 7.4% and raise prices for consumers by 9.1%.


### Trump Administration Claims Link Between Tylenol and Autism [9]

***September 22***

Despite a lack of scientific evidence to back up his claims, President Trump asserted that use of the pain reliever Tylenol during pregnancy was associated with an increased risk of autism. "Taking Tylenol is not good. I'll say it—it's not good," Trump stated in a press conference. The president further indicated that the FDA would be notifying physicians to stop recommending acetaminophen (the generic name for Tylenol) during pregnancy and would look into changing warning labels on the medication. The president's unprecedented move of tellling people not to use an American company's products had negative impacts on both the company and consumers. Tylenol maker Kenvue along with a host of medical organizations and experts refuted the administration's

*Getty / Marco BertoRello, Brandon Bell, Kamil Krzaczynski; Shutterstock / Minakryn Ruslan*

claims, citing decades of studies and data supporting the safety of acetaminophen. The medication is used by more than half of pregnant women worldwide to ease pain. The reputation fallout for Kenvue was swift as the company's stock dropped 7.5% immediately after the announcement, reducing the company's market value by $2.6 billion. The state of Texas also sued Kenvue and its former parent company, Johnson & Johnson, for deceptively marketing Tylenol to pregnant women despite the alleged links to autism and other disorders. In October, U.S. Secretary of Health and Human Services Robert F. Kennedy, Jr., slightly walked back some of the claims, saying that the evidence did not prove definitively that Tylenol caused autism but that it is "very suggestive."


### Record U.S. Federal Government Shutdown Causes Widespread Disruptions

***October 1***

The federal government shut down after Congress failed to pass required appropriations bills or a temporary funding measure, causing significant disruptions to the economy, millions of households, and business and government operations across the country. Democrats wanted the necessary appropriations or funding bill to include extensions of health care subsidies to control health insurance costs for low- and middle-income Americans. Republicans refused to pass a measure that included such provisions and would not negotiate any such subsidies until the government was funded, leaving the parties at an impasse. From a macroeconomic perspective, the shutdown could have significant long-term impact. Analysts from EY estimated the shutdown could shave 1% to 1.5% off the nation's GDP, and the Congressional Budget Office estimated the shutdown could cost the economy between $7 billion and $14 billion in lost output that will not be fully recovered, even with the government reopening. The shutdown also had a serious human toll, forcing one million federal workers to go weeks without pay, leaving many people without jobs, suspending key social services and threatening federal benefits such as SNAP (food stamps). For businesses, the shutdown created major operational challenges like freezing work done via federal contract, delaying payments, and slowing processes that require approvals or government processing, such as permits or data releases. Travel, transportation and tourism also saw significant interruptions, longer wait times, service reductions, and decreases in demand due to uncertainty. The shutdown finally ended on November 12 after a record 43 days, though the current funding agreement will only last through January 2026. The agreement to fund the government did not address ACA subsidies, which could lead to health insurance increases of up to 26%, potentially bringing costs to levels that would make coverage unaffordable for millions of Americans.

### NFIP Lapses, Freezing New Policies and Threatening Home Sales

***October 1***

As part of the government shutdown, the National Flood Insurance Program was allowed to lapse. Existing policies stayed in effect, but new policies were not issued and renewals were not processed. This had notable implications for real estate, developers and homebuyers as having a flood insurance policy is required for federally-backed mortgages in high-risk areas. With policies not processed during the shutdown, this caused thousands of real estate transactions to be delayed or put at risk of cancellation. Lenders were advised that they could continue making loans, but would be responsible for flood determinations and risk management. The NFIP was extended when the government reopened, but true to form with this often-debated program, Congress only passed a short-term extension for the program rather than long-term reauthorization. The current extension will expire on January 30, 2026.


Getty / Bloomberg Dimitar Dilkoff; Anadolu

### French Crown Jewels Stolen from the Louvre in Brazen Daytime Heist [10]

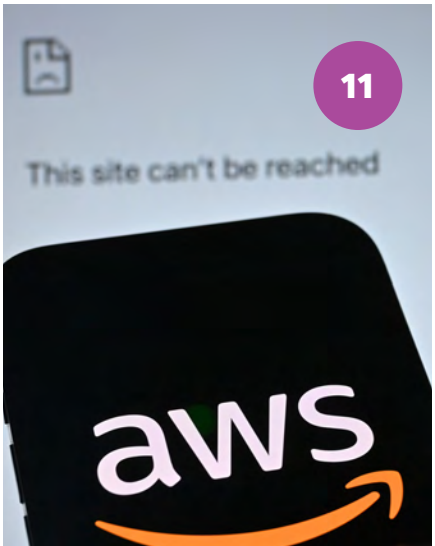
***October 19***

In the span of seven minutes on an otherwise ordinary Sunday morning, four thieves pulled off what some have called "the heist of the century," stealing priceless pieces of the French crown jewels that date back to the Napoleonic era. As the museum was opening, thieves dressed as construction workers drove up to the building in a truck outfitted with an extendable ladder. They climbed the ladder to reach a second-floor balcony, then used an angle grinder to cut through a window into the gallery housing the jewels, broke into display cases and took nine pieces of gem-encrusted jewelry. They then used the ladder to escape, attempted to set fire to their truck, and rode off on motorbikes. Many were captivated by the case and its sensational details, which seemed more like the plot of a heist movie than a news event. As French investigators raced to find the thieves before they could melt down the pieces and sell the jewels, the public also pored over details of the case and major security lapses at one of the world's most famous museums like the lack of security cameras in the gallery or the surveillance system with the obvious password "Louvre." Two suspects were arrested on October 26 as they were about to leave the country and authorities are still hunting for the other two thieves.

### Thousands of Companies' Operations Halted by Amazon Web Services Outage [11]

***October 20***

A bug in its automation software caused outages for clients of Amazon's AWS web services, causing service interruptions that impacted a wide range of downstream platforms, including Atlassian, Signal, Snapchat, Fortnite, Roblox, Coinbase, Venmo and Ring. Cyberrisk analytics firm CyberCube reported that the incident directly affected 70,000 organizations globally and estimated cyber insurance losses of $38 million to $581 million from the outage. Mehdi Daoudi, CEO of internet performance monitoring firm Catchpoint, estimated the total financial impact of the disruption would be in the billions of dollars. The incident was particularly notable given the sheer ubiquity of AWS as a critical component of companies' operations. With approximately 30% market share, Amazon is the biggest cloud services provider. "This AWS outage underscores systemic cloud services provider concentration risk," CyberCube noted in a blog post. The losses will primarily be felt by companies, with the insurance industry fairly insulated from aggregation risk due to waiting periods before outages are covered. "With disruptions extending 15 to 16 hours and most waiting periods in the 8 to 12-hour range, this outage could represent a moderate cyber (re) insurance event," CyberCube noted.




### Hurricane Melissa Becomes Strongest Atlantic Storm to Ever Make Landfall

***October 28***

Hurricane Melissa made landfall in Jamaica as a Category 5 storm, killing 54 people and causing widespread damage to more than 215,000 structures as high winds and torrential rain tore roofs and walls from municipal buildings, businesses, schools and homes. The country sustained an estimated $10 billion in damages from the storm. With its 185-mile-per-hour winds, Hurricane Melissa was not only the most powerful storm of the 2025 season, but was tied for both the second-strongest hurricane on record and the strongest to ever make landfall in the Atlantic. Overall, the 2025 Atlantic hurricane season was less active than expected, however, its three Category 5 hurricanes marked the second-highest number of Category 5 storms in a season behind only 2005, which saw four. Collectively, 2025 storms killed 134 people and caused $10.5 billion in damages, almost entirely caused by Hurricane Melissa.

### Layoffs Hit "Recession-Like Levels," On Par with Pandemic and 2008 Financial Crisis

***November 6***

In October, layoffs surged to levels typically seen in recessions, according to a report from Challenger, Gray & Christmas, a firm that tracks workplace

reductions. Employers had announced over 1.1 million layoffs by the end of October, which the report noted was the highest number since the pandemic recession and on par with job cuts during the Great Recession in 2008. Layoffs were slightly lower in November, but still up 24% from job cuts in the same month last year. Year-to-date, the November report found job cuts at a five-year high as employers had announced 1,170,821 job cuts, up 54% from the same period last year and the highest total since the onset of COVID in 2020. According to the firm's data, the most common factors employers cited for the announced layoffs were: restructuring, artificial intelligence, market and economic conditions, tariffs, and the "DOGE impact" (direct and downstream effects from the Department of Government Efficiency's federal cuts earlier in the year). The current economic environment and uncertainty about tariffs and other key operational factors appear to be having a significant impact on the labor market that shows little sign of abating in the near future. Through November, U.S. employers announced 497,151 planned hires—35% fewer than the number announced at this point in 2024 and the lowest total since 2010.


Getty / Visual China Group

### 159 Killed in Hong Kong Housing Complex Fire [12]

***November 26***

Eight high-rise residential towers were scorched in a massive fire at an apartment complex in Hong Kong, ultimately killing at least 159 people. The buildings were in the midst of a months-long renovation project, so they were covered in bamboo scaffolding and protective netting intended to prevent debris from falling onto people below. Unfortunately, this safety measure ultimately proved catastrophic. The netting used was not up to fire safety codes, contributing to the fire's rapid spread from building to building. Initially, samples of the netting taken at ground level appeared to be up to code, but samples taken higher found material that failed safety standards, suggesting to investigators that contractors may have cut corners to increase profits. Authorities also believe employees from a fire service installation contractor may have deactivated some fire alarms during maintenance. Local authorities are investigating claims of corruption and negligence regarding the renovation work and Hong Kong's anti-corruption body and police have arrested at least 21 people, including engineering consultants, construction company directors and fire service installation workers. Officials have ordered contractors across Hong Kong to review the safety of similar materials at hundreds of other buildings under renovation, requiring them to submit detailed reports along with quality certificates and test results for any protective netting.

### Starbucks to Pay Largest Worker Protection Settlement in NYC History

***December 1***

Officials announced the largest worker protection settlement in New York City history when Starbucks agreed to a $38.9 million settlement over violations of a city law guaranteeing fair working conditions. An investigation by the city's Department of Consumer and Worker Protection found Starbucks violated the law more than half a million times since 2021 by failing to provide stable schedules for workers. More than 15,000 hourly workers who worked between July 2021 and July 2024 will be eligible receive restitution payments under the agreement, with payouts of approximately $50 per week worked during that period. Under the Fair Workweek Law, which was passed in 2017, fast-food employers must give workers consistent week-to-week schedules, provide schedules 14 days in advance, and cannot reduce hours by more than 15% without "just cause or a legitimate business reason." Starbucks claimed the law is "notoriously challenging for businesses to navigate" and made a point of noting the violations were about compliance, not withholding wages or failing to pay partners. R

# RISK
# STAY AHEAD

Since 1954, *Risk Management* has provided readers with the latest in risk management news, insight and analysis.

Whether it is dynamic issues of cybersecurity, the emerging risk landscape, reputation risk, insurance, disaster preparedness or anything in between, **we are the authority** on information you need to meet the challenges of today's evolving business landscape.

Visit **RMmagazine.com** for our article archive.


RISK MANAGEMENT

# How to Overcome Cognitive Biases in Risk Management

by Shreen Williams, Jason Rosenberg and Lisanne Sison

**Risk professionals often take comfort in** frameworks such as COSO ERM and ISO 31000 because they provide structure, discipline and a sense of order for organizations and their assurance capabilities. Regardless of the framework or the level of structure it may provide, there is one component that cannot be removed from the risk management process: human bias.

Biases are shortcuts in our thinking, helping us make quick decisions. Unfortunately, those decisions are not always the right ones. While biases may help us make faster decisions in times of uncertainty, they can also distort judgment. In high-stakes environments like critical business decision-making, even the slightest distortions can lead to strategic blind spots, wasted resources or surprises that have a severe impact.

Biases can show up at any stage of the ERM process lifecycle, from process design to risk identification and assessment to risk monitoring and reporting. Cognitive biases can appear in many forms, including boards choosing complicated solutions that only look impressive, leaders explaining away mistakes and placing the blame on others, or teams of people going along with the group rather than speaking up to provide their own perspective.

It is not enough to simply be aware that biases exist throughout risk management processes. The real challenge for risk leaders is to proactively identify biases and develop mitigation strategies to minimize biased decision-making and support risk-informed decisions. Eight of the most pervasive biases shaping ERM today are complexity, innovation, self-servicing, overconfidence, anchoring, confirmation, framing and groupthink. By exploring these biases and the scenarios in which they manifest, risk professionals can better develop pragmatic techniques to counter their effects and limit their impact on business decisions.

## When Complexity and Innovation Become a Crutch

Consider a hypothetical scenario: A company's board of directors decides to hire an external risk management consultant to evolve its capabilities and maturity level. The consultant completes the engagement and delivers a complex, jargon-filled, COSO-aligned framework with multiple taxonomies and negligible practical advice or resources to help the company implement the consultant's recommendations and ensure adoption from its internal stakeholders. Risk identification stalls because the framework is far too complicated for frontline employees to apply. The assumption is that

Shutterstock / Andrii Yalanskyi

complexity is automatically better. This is **complexity bias** at work.

Complexity bias leads organizations to favor overly complicated solutions over pragmatic solutions. This bias is often accompanied by **innovation bias**, in which the newest version of a framework like COSO ERM is perceived as inherently superior, regardless of whether it drives actual improvements to existing capabilities.

These biases can have significant impact on risk governance. Making things too complicated can confuse frontline employees, delay progress and give stakeholders a false impression that their risk management capabilities are more advanced than they actually are. By making frameworks unusable for frontline teams, these biases can overcomplicate governance, undermine risk identification, and make it more difficult to establish risk frameworks and structures.

To overcome complexity and innovation biases, keep it simple. In risk governance discussions, ask yourself: Could I explain this framework to a new employee in less than two minutes? If the answer is no, it is too complicated, and complexity bias may be in play. Address the bias by trimming the extras and focusing on what really matters. Specifically, summarize risk governance structures and frameworks into one-page resource documents. Then, check with risk champions situated throughout the organization's ecosystem to validate whether the documents are digestible and accessible enough.

## Falling Into the Self-Serving Trap

Imagine a company that is launching a new product. If it succeeds, leaders credit their foresight. If it fails, they blame regulators or "unforeseen" market shifts. After-action reports are shallow and lessons learned are rarely integrated into the ERM process. This is **self-serving bias**—attributing wins to ourselves and losses to external factors.

In strategy discussions, self-serving bias can lead to selective storytelling. Leaders may take too much credit for successes and downplay outside factors. This creates a false sense of confidence and prevents the company from learning from its mistakes, ultimately weakening the organization's overall strategy and future decision-making processes.

**Overconfidence bias** amplifies this problem. Decision-makers often overestimate their predictive abilities, underestimate downside risks and allocate resources based on optimism rather than balanced analysis of objective data. For example, a CFO may project best-case market growth while ignoring signals of regulatory headwinds.

Self-serving bias makes it more difficult to manage the ERM process. Strategic choices ultimately become management actions, including resource allocation, performance review and lessons learned. This is where self-serving attributions distort accountability and prevent organizations from integrating failures back into their risk programs.

To combat this bias, pair every major decision and postmortem review with an independent, objective challenger who is empowered to poke holes—not rubber-stamp—the narrative. This objective challenger could be a dissenting board member, an activist shareholder or an external advisor. Require teams to document both "management-controlled factors" and "external factors" before closing reviews to help ensure balance and accountability. The goal is not to obstruct or criticize, but to achieve objectivity to identify opportunities for improvement.

## Anchoring Too Strongly on First Impressions

During a risk assessment, the first concept or idea mentioned can often "anchor" the rest of the discussion, even if it is arbitrary. For example, imagine a company holds an executive team risk workshop to address concerns of a potential cyber disruption event. The CISO tells the group that there is a 25% probability of a cyber disruption event materializing. Despite objective evidence showing the likelihood is actually higher, the number arbitrarily introduced then sets the tone for discussions. This is **anchoring bias**.

Anchoring bias frequently occurs in risk assessment workshops and budget allocation meetings. Once an initial anchor is set, it is tough for participants to move beyond it, even when better data becomes available. Anchoring bias can complicate risk assessments where risks are evaluated and scored as initial anchors can distort probability and impact judgments.

To prevent anchoring bias when facilitating workshops and meetings, consider sending all participants pre-reads that provide insights into the process and specific risks that will be evaluated or discussed. Use structured materials that require anonymous input from multiple perspectives like finance, operations and legal. Also make sure to calibrate results in validation sessions to reduce reliance on the first number put on the table.

## Seeing What We Want to See

Consider a company where the chief risk officer reviews quarterly risk dashboards. Most indicators show stability, so they ignore a dissenting data set suggesting an emerging third-party vulnerability because it conflicts with their preferred narrative. This is **confirmation bias**—favoring information that supports what we already believe.

Confirmation bias is especially prevalent in situations where no consideration is given to alternative data and information, regardless of source or availability. Left unchecked, confirmation bias blinds risk management teams to new threats. It perpetuates outdated risk registers, discourages escalation and can leave organizations more vulnerable to severe risks. Confirmation bias interferes with risk monitoring where data and metrics are tracked. When organizations dismiss contradictory signals, they fail to detect changes in exposures or emerging risks.

To avoid confirmation bias, do not just look for evidence that supports your individual perspective. Instead, look for what might

prove it wrong. Rotate teams that are assigned to challenge attitudes and assumptions. They should act as adversaries to uncover blind spots in your organization's defenses and challenge the efficacy of your organization's internal control mechanisms. If your organization has an internal audit function, that team could also be well positioned to provide this insight. In every decision-making discussion, require leadership to provide at least one fact or example that challenges the current thinking, and review at least one opposing fact or example during each meeting.

## Framing the Same Data for Different Decisions

After conducting a risk assessment, imagine a company's CISO reports to its board of directors that its system uptime is 95%. The board of directors and company leadership feel the targeted system uptime is adequate and use that data to reduce resource allocations for the company's IT business function.

Alternatively, the CISO could have reported to the board that their system downtime is 18 days a year. As a result, the board of directors and the company's leadership would demand urgent resource allocations for the IT business function.

Though they may both be accurate numbers, a system uptime of 95% resonates more positively with the company's decision-makers than 18 days of downtime per year. This bias is known as the **framing effect**, where the same data can change perceptions and decisions when simply packaged and presented differently.

Framing bias affects how leaders interpret the same data. Positive frames typically encourage risk-taking and negative frames push toward risk aversion. As the way data is presented often directly impacts the choices leaders make, shifts in framing can shape multimillion-dollar investment decisions.

Avoid framing bias by standardizing dashboards and using neutral language in reports to reduce unconscious conclusions and present risk information in a way that showcases both upside and downside. Encourage decision-makers to reflect on the data before reaching a conclusion.

## Betting Too Much on Gut Feeling

Consider another company where leadership is confident that their cloud migration will be seamless because their team has successfully executed projects before. They allocate minimal contingency funding, only to encounter months of delays and unexpected security gaps. This is **overconfidence bias** undermining resilience.

Overconfidence bias leads organizations to underestimate complexity, dismiss early warnings, over-rely on prior successes and overcommit to ambitious timelines. In risk assessments, this often leads to unrealistically optimistic scores, directly impacting how organizations allocate resources, establish timelines and execute risk responses.

To counter overconfidence bias, conduct premortems before all major initiatives, pretending that they have already failed and then working backwards to ask why. This "what could go wrong?" exercise helps uncover blind spots and hidden risks before decisions are locked in. Executive sponsors for the initiative should be able to explain why it could fail. Track variances between forecasted versus actual project outcomes to recalibrate future assumptions and allocate appropriate resources.

## Favoring Consensus Over Candor

Boards often pride themselves on consensus, but too much harmony can easily hide both upside and downside risk. Consider a company where board meeting discussions often grow tense, but if the CEO confidently asserts their perspective, dissenting leaders hesitate to challenge the CEO or present their opposing perspective. Instead, they nod in agreement with the rest of the collective group to avoid "rocking the boat." Decisions are unanimous, and critical risk exposures are ignored. This is **groupthink**—the preference for consensus over candor.

Groupthink erodes the quality of reporting and oversight. It silences minority opinions, narrows perspective and prevents boards from fulfilling their role as stewards of diverse stakeholder interests. Groupthink complicates the risk reporting process, where risk information is escalated to executives and boards. Suppressing dissent in reporting weakens oversight and masks exposures.

To overcome groupthink, adopt a formal "speak up" practice that encourages internal stakeholders at every level to speak freely, without any fear of retaliation or retribution. Implement a process for structured dissent, requiring a round of "what are we missing?" at every meeting. Allow anonymous submissions for alternative viewpoints and present them in future meetings to normalize candor and dissent. Embed psychological safety by rewarding dissent, not penalizing it.

## The Human Side of ERM

Leaders who can combat bias in real time can help position their organization ahead of its peers and competitors. Frameworks, dashboards and internal controls are essential, but they cannot eliminate the most unpredictable variable in any ERM program: people. Biases creep into strategy discussions, risk assessments and board reports, often without anyone realizing it.

Human biases will never disappear, so risk leaders must embed bias-awareness into every stage of the ERM process lifecycle, not as an academic exercise, but as a daily discipline. Start small by simplifying frameworks, running premortems, rotating teams assigned to challenge perspectives and assumptions, and normalizing and rewarding dissent. Over time, these practices can help create positive risk cultures, healthier governance and more effective risk oversight. R

**Shreen Williams** is founder and CEO of Risky Business SW, LLC. **Jason Rosenberg** is senior director of risk and resiliency at Autodesk. **Lisanne Sison** is managing director of ERM at Gallagher.

## MISDIRECTED EMAIL: THE WORKPLACE FAUX PAS WITH A SHOCKING PRICE TAG


According to a recent study by human behavior security firm Abnormal AI, one of the most damaging and overlooked enterprise cybersecurity threats stems from a simple mistake we all have nightmares about: sending an email to the wrong person. Of 300 security and IT professionals surveyed, 98% considered misdirected emails a significant cyberrisk compared to other risks like malware and insider threats. Misdirected emails are legitimate messages sent to the wrong recipient. While many might dismiss these as a harmless error in the modern workplace, misdirected emails can result in data breaches, regulatory violations, remediation costs and reputation damage. In fact, 96% of organizations experienced data loss or exposure from misdirected email in the past year, and 95% reported measurable business impact such as remediation costs, compliance violations or damage to customer trust. The violations can be costly: Abnormal AI reported misdirected emails accounted for 27% of all data protection incidents under GDPR last year, contributing to over $1.2 billion in fines worldwide.

"This is a visibility problem as much as it is a technology one," said Mike Britton, CIO at Abnormal AI. "Traditional tools cannot differentiate a legitimate customer email from a sensitive message going to the wrong recipient. Protecting data today requires more than defending against external threats—it means understanding and supporting human behavior."

**– Hilary Tuttle**

## Mental Health Tops List of Workplace Safety Injuries

According to a survey by Pie Insurance, the most common injuries experienced by workers at U.S. small businesses were mental health-related (22%), followed by slips, trips and falls (20%) and cuts, lacerations and punctures (18%). Given the prevalence of mental health-related injuries, it is perhaps no surprise that 32% of employees cited mental health as their primary workplace safety worry, surpassing traditional concerns like physical injury (20%), environmental hazards (9%) or equipment safety (4%). However, while 91% of employers were confident in their ability to address mental health issues, only 62% of employees shared that confidence in their employers. The impact of mental health extends beyond the workplace as 36% of employees reported that workplace stress and safety concerns affect their personal lives, leading to burnout, depression and physical symptoms. Almost three-quarters of employees (73%) said employer support would make a meaningful difference, citing flexible or remote work options, mental health day allowances, counseling services, and mental health awareness and safety training as possible solutions.

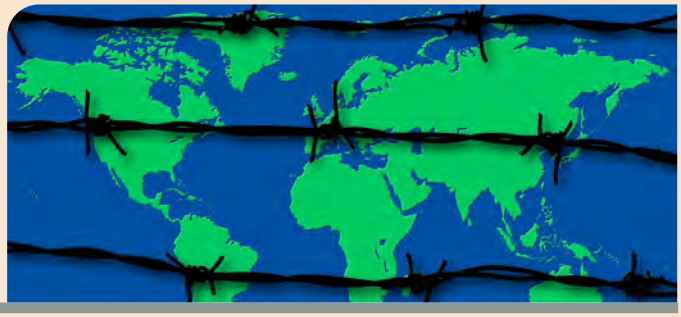
Shutterstock

**– Morgan O'Rourke**

## The Impact of Political Risk Losses

Geopolitical tensions and macroeconomic volatility are creating uncertainty around the globe, making political risk management and insurance increasingly critical. A Howden survey found that 51% of multinational companies suffered a political risk-related loss to their international investments between 2020 and 2025. The most frequently reported causes for losses were: difficulties exchanging local currency to repatriate funds (40%); foreign government interference with ownership rights (40%); and being forced to abandon foreign assets because of political violence (33%). Foreign government interference resulted in the costliest average losses at $19.8 million, followed by currency conversion issues at $16.4 million and political violence at $14.3 million. Companies with political risk insurance reported losses that were $1.4 million lower on average than those without coverage. In addition to insurance, 80% of companies are planning to adopt other risk management tools to help mitigate political risk losses like scenario-planning methodologies, geopolitical issue tracking and data analytics.

**– Morgan O'Rourke**



# Boost Your Risk Knowledge in 2026

Learn the ins and outs of trending topics at an interactive RIMS Virtual Workshop. Return to work with the confidence to apply your new skills.

## Intro to ERM for Senior Leaders

**January 8, 2026**

Gain a foundational understanding of enterprise risk management (ERM) processes, tools, and techniques for real-world business application.

## RIMS-CRMP Exam Prep

**January 14–15, 2026**
**March 10–11, 2026**

Prepare for the RIMS-CRMP exam and learn about the five core competencies of the RIMS-CRMP program.

## Managing Worker Compensation, Employer's Liability, and Employment Practices in the US

**January 21–22, 2026**

Meet new challenges related to worker risk by focusing on the fundamentals of workers compensation coverage and state-specific laws.

## Applying and Integrating ERM

**February 4–5, 2026**

Analyze the benefits and challenges of ERM, create an ERM agenda, and review real-world case studies.

## Fundamentals of Risk Management

**February 10–11, 2026**

Learn risk management basics and how you can create, protect, and realize enterprise value.

## RIMS-CRMP-FED Exam Prep

**February 17–18, 2026**

Prepare for the RIMS-CRMP-FED exam and learn about the three federal government domains.

## Risk Taxonomy for Effective Risk Management

**February 25, 2026**

Delve into the fundamentals of risk taxonomy and learn the process of classifying and managing risks.

## Facilitating Risk-Based Decision Making

**March 4–5, 2026**

Develop the ability to recognize the impact of perception on analysis and judgement and incorporate debiasing techniques.

## Risk Appetite Management

**March 25–26, 2026**

Learn how to develop a risk appetite framework that clarifies your company's position on risk taking.

View more upcoming workshops at

**www.RIMS.org/VirtualWorkshops**

RIMS
the risk management society

# TOP 10 EMERGING RISKS

For its annual *Future Risks Report*, AXA asked almost 3,600 risk experts across 57 countries to rank their top emerging risks based on potential impact to society over the next five to 10 years. Of the experts surveyed, 83% believe that the world is now more vulnerable than it was five years ago. There were signs of optimism, however, as 86% believed these emerging risks can be avoided with strong preventive action.


***Source:*** *AXA, Future Risks Report 2025*

## Geopolitical Risk Anxiety

A recent Beazley survey of 3,500 business leaders revealed a deepening sense of unease around the business impact of geopolitical uncertainty in 2025:

- **88%** agreed that the political landscape will affect their company's ability to trade profitably—up from **69%** in January 2025
- **83%** believed the current geopolitical and economic uncertainty will limit their company's growth plans—up from **68%** in January 2025
- **87%** expected to make changes to their suppliers and supply chains due to geopolitical tensions—up from **75%** in January 2025

***Source:*** *Beazley, Spotlight on Geopolitical & Economic Uncertainty 2025*

Shutterstock

## The 2025 Phishing Calendar

Cybercriminals often adjust their messaging to reflect common workplace subjects or calendar events like holidays. According to data from cybersecurity firm KnowBe4, these were the most frequent topics in phishing emails for each month of 2025:

**January:** Promotions, benefits and remuneration

**February:** Valentine's Day

**March:** Missed messages

**April:** Taxes, IRS and payments

**May:** Meta impersonation via Appsheet

**June:** Microsoft mailbox limit

**July:** Company impersonation

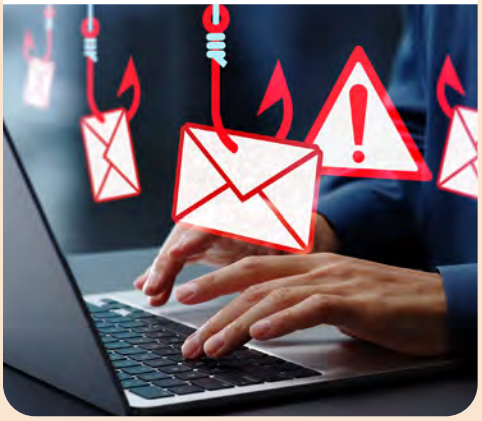
**August:** The U.S. Open

**September:** Start of the university academic year

**October:** Hijacking legitimate payment platforms

**November:** Multi-factor authentication

**December:** Holiday celebrations



RIMS members **save up to $604** on registration

PHILADELPHIA 2026

# RISKWORLD®

POWERED BY RIMS

MAY 3–6

# Connect. Cultivate. Collaborate.

## You've built your expertise—now it's time to strengthen your influence.

Join thousands of risk leaders, innovators, and visionaries at RISKWORLD 2026—the ultimate destination for advancing your career and transforming your organization.
Here's why you can't miss it:

- **Unparalleled Networking:** Connect with your peers and get direct access to key industry leaders from a diverse range of industries, roles, and countries.
- **Practical Tools & Solutions:** Explore innovations from 300+ solution providers to help you navigate the evolving risk landscape and safeguard your company's assets.
- **Top-Tier Education:** Propel your professional growth and gain a deeper understanding of issues like AI adoption, tariffs, and global disruptions in 100+ interactive sessions.

RISKWORLD 2026 is your ticket to stronger connections, actionable insights, and tools to advance your career and business. **Register today to secure your spot.**

**www.RIMS.org/RISKWORLD**