Teneo®

Why 2024 is the Year for Resilience

Ten key considerations for the CEO agenda in 2024

Teneo Insights / January 2024

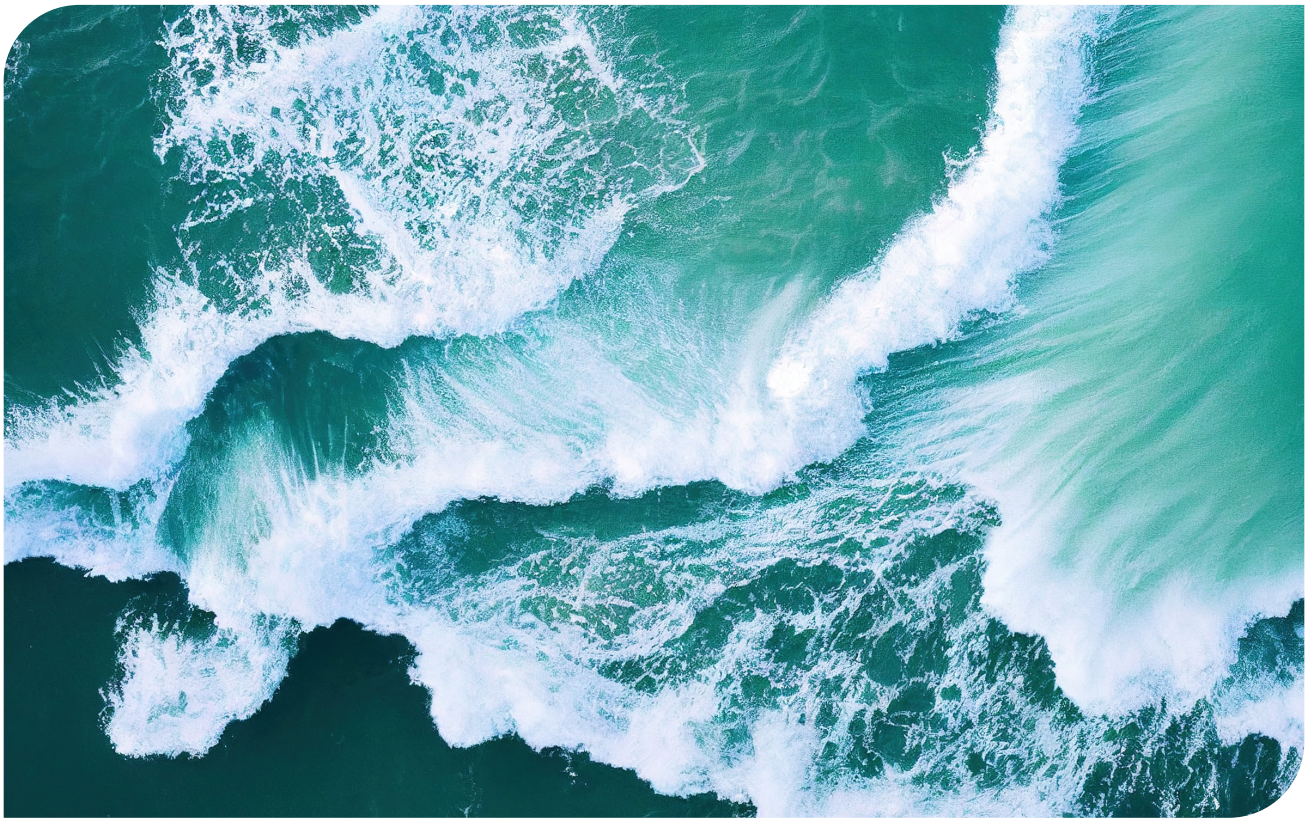
Introduction

As 2023 unequivocally laid bare, companies today face an ever-expanding and highly volatile risk landscape that demands more attention from its leaders. As we step into 2024, public and executive attention will have to balance persisting global conflicts and tensions with growth and innovation, with far-reaching implications.

Similarly, rapid advancements in artificial intelligence and other emerging technologies will require robust analysis to ensure that any benefits associated with adoption are considered alongside the risks. The year ahead will also present challenges from extreme weather and cyber risks to a heightened terrorism threat environment and potential civil unrest against the backdrop of a global record election year.

Each of these trends necessitates CEOs to focus on building organizational resilience grounded in anticipatory intelligence analysis and meticulous crisis preparedness to ensure compelling strategies for organizational resilience. While the threat landscape in 2024 may be riskier than ever, the good news is that the whole executive suite has a role in supporting the CEO to ensure a diverse range of expertise and thought leadership is brought to bear in the resilience strategy. By proactively adopting strategies to anticipate, mitigate and respond to these trends, leaders cannot only overcome, but thrive in this environment, turning potential challenges into new opportunities.

Outlined in the following pages are ten trends and threats that we assess corporate leaders will have to contend with in the year ahead, as well as our approach on how best to tackle these and the risks they present head-on.



Contents

01. Executives will face increased pressures to take a public stance on controversial issues

There was no shortage of domestic and global issues in 2023 that prompted waves of public scrutiny and stakeholder activism, putting significant pressure on corporations and their leaders to take a public stance on controversial topics and developments.

Last summer, several retailers and brands faced backlash and financial consequences over their LGBTQ+ merchandise and policies before and during Pride celebrations in June, as well as related calls from stakeholders and activist groups for other corporations and their executives to weigh in.

Similarly, the Israeli-Palestinian conflict has demonstrated the spotlight on corporations to weigh in on the conflict and BDS (Boycott, Divestment, and Sanctions) campaigns have become prominent in response to Israel's operations in Gaza.

In the year ahead, we expect key stakeholders – including customers, employees and investors – to continue to judge companies and brands, and their respective leadership, by a corporation's public response – or lack thereof – to controversial domestic and global developments.

Ongoing tensions in the Middle East and the upcoming U.S. presidential election will most certainly require executives to be thoughtful in what and how they communicate. The challenge will be to have a coordinated response that proactively considers the reactions of significant stakeholder groups, as well as the associated risks.

02. The AI race and the rush to adopt new technologies will tempt companies to prioritize innovation over robust risk analysis

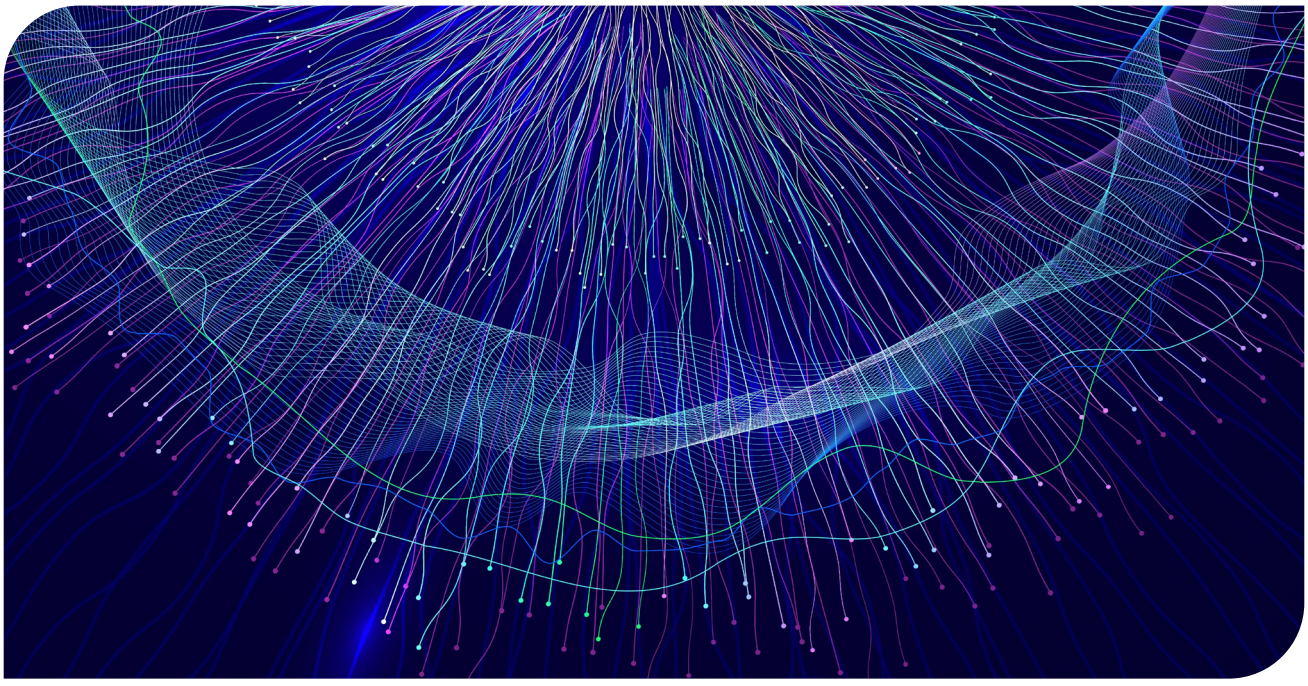
The fervent pursuit by companies to adopt generative AI following the release of ChatGPT has been a defining feature of 2023. While this focus has fostered greater innovations and efficiencies, the haste to adopt new technologies has created an environment of reluctance to first properly assess potential risks, which in turn has led to reputational and legal challenges, security vulnerabilities and ethical quandaries.

As CEOs and their teams consider implementing new AI and technological solutions, they must consider comprehensive risk assessments that account for all the potential reputational, operational and security challenges and appropriately weigh the benefits of rapid innovation and adoption with the associated risks and costs.

In December, the European Union (EU) reached an agreement on proposed regulation for AI. The AI Act is the first comprehensive, global set of risk-based regulations and requirements centered on transparency, accuracy, human oversight and other crucial components.

While the deal by EU policymakers signals progress in efforts to appropriately consider the risks associated with AI technologies, the Act does not go into effect until 2025, leaving many questions related to whether technology will far outpace the intended safeguards, hence rendering them stale and ineffective.

Questions also remain about whether other governing bodies and countries will follow suit, whether regulations will stifle innovation, and what enforcement may look like. As corporate leaders consider how best to incorporate AI and emerging technologies into their operations, they must also reflect on the regulatory landscape and ensure they are effectively monitoring and complying with new and emerging regulations.



03. Disinformation campaigns, fueled by technological advancements, will exacerbate polarization

Rapid advancements in technology, including generative AI, coupled with laxer content moderation on several widely used social media platforms have created a digital environment ripe for the creation and propagation of mis- and disinformation campaigns that fuel and exacerbate existing polarized discourse, as well as target specific entities and individuals.

In both the Russia-Ukraine and Israeli-Palestinian conflicts, mis- and disinformation campaigns are abundant, inflaming global reactions to the conflicts with false claims and AI-generated footage that rapidly proliferate.

As we saw in 2023, the evolving social media landscape is increasingly situating brands and executives in the crosshairs of disinformation, deep fakes and evolving online threats as they propagate instantaneously across social media. Further facilitated by advancements in generative AI, the proliferation of disinformation and misinformation in the digital domain presents an unprecedented challenge in the year ahead.

Corporations and their executives will undoubtedly have to deal with malicious actors exploiting social media and other online platforms to disseminate adverse or misleading narratives to manipulate key stakeholders.

Regular, robust communications from trusted representatives will remain critical to mitigating the threat these campaigns pose; however, as deepfake and other technology advance, organizations will also need to consider further mitigations such as comprehensive training, watermarking and closed-portal communications.

04. Global conflicts will continue to drive instability

The new year begins with the Middle East in turmoil. As of this publication, the Israeli-Palestinian conflict has claimed around 20,000 Palestinian and 1,500 Israeli lives.[1] The vast majority of Gaza's 2.2 million residents have been displaced internally and around 130 hostages taken from Israel remain in Gaza.[2]

The humanitarian catastrophe will continue to have reverberations for years to come and the regional security paradigm has radically shifted, with regional actors – particularly Iran and its Hezbollah and Houthi proxies – seizing on the current conflict to further antagonize adversaries and destabilize the region, with the potential for further escalation ever-looming. The consequential disruptions to global markets and trade routes – further evidenced by the recent targeting of ships in the Red Sea by the Houthis – diplomatic relationships and alliances between nation-states and international governing bodies will continue to impose challenges for businesses, governments and humanitarian efforts alike.

Meanwhile, the war in Ukraine rages on. Russia's invasion of Ukraine and the subsequent robust sanctions response – the most far-reaching since the 1930s – disrupted the global recovery from the pandemic, driving significant economic and operational challenges across regions and industries for all of 2023. With little hope for serious peace negotiations – as indicated by President Putin's recent comments which stated that his objectives in Ukraine remain unchanged, as well as the difficulty for Ukraine's allies to sustain the same level of financial support as previously – the war is set to continue well into 2024 and beyond. Its continuance will by necessity continue to factor into how corporations think about the region's stability and the ongoing implications for their respective industries and supply chains.

These two wars alone – let alone other brewing global, regional and local tensions across the world – demonstrate the significant impact that regional conflicts can have on our interconnected world, serving as persistent sources of uncertainty and volatility while undermining global security and stability.

In the face of this disruption, corporate leaders require truly anticipatory and tailored intelligence and analysis specific to their unique risk profiles and operating environments. Although commentary and analysis about the global security landscape and geopolitics at large abound, generic assessments no longer suffice. Instead, leaders need tailored analysis – coupled with robust scenario planning that takes into consideration clear indicators and signposts and their associated impacts – to ensure they are appropriately considering and mitigating the global risks most relevant and impactful to them and their businesses.

1 Pressure mounts to scale back war as Gaza death toll nears 20,000 (nbcnews.com)

2 Israeli hostage accounts increase pressure to rescue those still in captivity : NPR

05. Elections and political instability will fuel civil unrest

2024 is set to be an unprecedented year for global political contests, with 50 countries scheduled to hold elections. Perhaps most critically, the U.S. presidential election is scheduled for November 5 and the latest polls suggest a match-up between President Biden and former President Trump.

Elections are also set to take place in Pakistan, Tunisia and Indonesia – all countries that have dealt with their share of polarized politics accompanied by frequent protests, civil unrest and related instability in prior years.

The potential for civil unrest, therefore, is ever present for the year ahead, potentially resulting in disruptions and challenges not just to governing political institutions and for law and order at the local and national levels, but also for corporations and their operations. Election-related unrest in the new year is also likely to feature and largely be driven by an unprecedented degree of digital polarization and mobilization.

Critical to identifying early warning signs, as well as the scale of unrest, is close monitoring of mainstream and fringe social media platforms to identify indicators of mobilization and escalation, as well as other key signals.

Corporations must develop robust digital intelligence and threat monitoring programs for any major locations relevant to their business operations and clearly define indicators and signposts that will alter their risk profile and hence require the finessing of existing risk management strategies or the adoption of new measures and policies.

06. The global terrorism environment will be further heightened

Hamas' horrific October 7 attack on southern Israel and the Israeli military's ensuing response have not only marked a turning point in the decades-old conflict in the Middle East but heightened the global and domestic terrorism threat environment once more.

Since October 7, several notable global terrorist organizations, including al-Qa'ida core, al-Qa'ida in the Arabian Peninsula (AQAP), the Islamic State of Iraq and ash-Sham and Hezbollah, have celebrated Hamas' atrocities and called for further attacks, including against U.S. targets both in the region and in the homeland. While developments related to Israeli-Palestinian relations have long been a rallying cry for global terrorist organizations, particularly those motivated by Salafi-Jihadi ideologies, the most recent conflict will serve as a significant catalyst for retaliatory actions in the region.

Globally, therefore, there will be a heightened potential for terrorist attacks in the year ahead, particularly attacks carried out or enabled by terrorist groups directly. These may include sophisticated, coordinated and directed attacks by terrorist groups operating in the greater Middle East and adjacent regions, as evidenced by the recent arrests of seven people, including four suspected Hamas members, on suspicion of planning attacks in Denmark, Germany and the Netherlands. While Hamas took the lead in launching the initial assault on October 7, multiple sources have pointed to the involvement of additional terrorist and militant groups who are continuing wage attacks in Israel, the region and Europe.

On the domestic front, the primary terrorist threat in the U.S. is likely to come from lone actors who are inspired and mobilized to act due to ideological motivations, calls to action by terrorist group leaders and propaganda dissemination across mainstream and fringe social media. It is worth noting that Hamas has called for attacks in the U.S.; the group has historically focused on attacks targeting Israel instead of supporting or directing attacks in the West.

06. The global terrorism environment will be further heightened (continued)

Meanwhile, other groups that are calling for attacks in the West, including AQAP, have previously demonstrated both intent and capability to attack U.S. targets. Potential indicators of lone actor attacks are likely to be more fervent calls for action by terrorist group leaders and their sponsors, many of whom have already called on supporters to carry out attacks. Federal and local intelligence and law enforcement agencies have already made several notable arrests related to such incidents or attempted plots and have indicated a significant number of similar investigations. Additionally, individuals and institutions perceived as symbolic of, or tied to, the conflict will continue to serve as attractive targets.

The upcoming presidential elections in November 2024 have also set the stage for a potential resurgence of domestic far-right activity in the year ahead. In the three years since the January 6, 2021, attack on the U.S. Capitol, more than a thousand participants have been arrested and prosecuted, with several key organizers and their respective groups – particularly the Oath Keepers and the Proud Boys – significantly disrupted and their capabilities denigrated. Nonetheless, with the republican primaries and the general election slated for this year, statements and actions by former President Trump will serve as both a catalyst and key indicator for how his supporters, including more extreme elements of his supporter base, may behave. In prior years, we have seen concerning rhetoric and thinly veiled commentary from the former president serve to mobile far-right groups and their supporters. At best, such rhetoric will serve to further polarize the electorate and shore up support for himself, and at worst, it will incite violent action as demonstrated in 2021. In addition, continued antisemitic and Islamophobic discourse on social media related to events in Israel and Gaza may further polarize the electorate and serve as catalysts for violence.

Against this backdrop, organizations must ensure seamless coordination across corporate human resources, security, communications and physical operations to understand their vulnerability to a potential terrorist action, as well as the organization's duty of care and planned response to such an attack. This type of proactive planning will help protect the organization against disruption while protecting its most critical asset – its people.

07. Cyber threat actors will continue to target critical industries and infrastructure

Cyber intrusions – driven by financial or criminal motivations or as a tool of war and aggression – continued to be effectively employed by a diverse array of threat actors in 2023, targeting critical industries and infrastructure.

These intrusions were marked by sophisticated cyber-attacks carried out by nation-states, criminal organizations and hacktivist groups, and all have the potential to create significant damage. With continued global conflict and rapid technological innovations, the year ahead will require companies to undertake robust cyber risk assessments and develop comprehensive strategies and safeguards that will appropriately protect their systems and digital assets.

Meanwhile, on December 18, the Securities and Exchange Commission (SEC) began requiring public companies to disclose how they manage cyber risk – including how they assess threats and their potential impact – in their 10-Ks, as well as requiring companies to report any cyber intrusions that are likely to have a material impact on the company's operations to the SEC within four business days.

The new reporting framework also places greater emphasis on the disclosure of board oversight related to cyber risks and the importance of crisis planning and communications in the event of cyber breaches.

With the implementation of SEC disclosure rules, corporations will no longer have the luxury of waiting until a robust forensic investigation can be done and to conduct appropriate analysis and messaging with expert reviews. A cyber breach may hence rapidly become a market-moving crisis event and potentially lead to further financial and reputational implications without adequate planning and preparation.

Going forward, organizations must have a documented and practiced crisis management plan in place to pull together key stakeholders, streamline information flow and guide decision-making. These plans must be tested and fortified through crisis simulation exercises to work out inefficiencies and build muscle memory while there is space and time to do so.

> AI can be a tremendous part of the toolkit to counter cybercrime and other cybersecurity threats. However, AI raises significant challenges that must be addressed in the enterprise cyber strategy. AI can increase the attack surface and raise risk so the integration of AI into a company's network security architecture must be carefully planned. Companies will therefore require deep cyber and operational bench strength across their entire security architecture, together with robust risk assessment and mitigation processes and protocols. We often say that cybersecurity consists of "people, process and technology" – and AI integration certainly must meet that standard.

Rhea Siers
Senior Advisor, Teneo

08. Extreme weather patterns will persist, creating unprecedented disruptions

2023 was likely the hottest year on record, driving extreme weather events around the world such as persistent and devastating storms, massive wildfires and other extreme weather patterns that pressured global infrastructure resilience and prompted worldwide disruption.

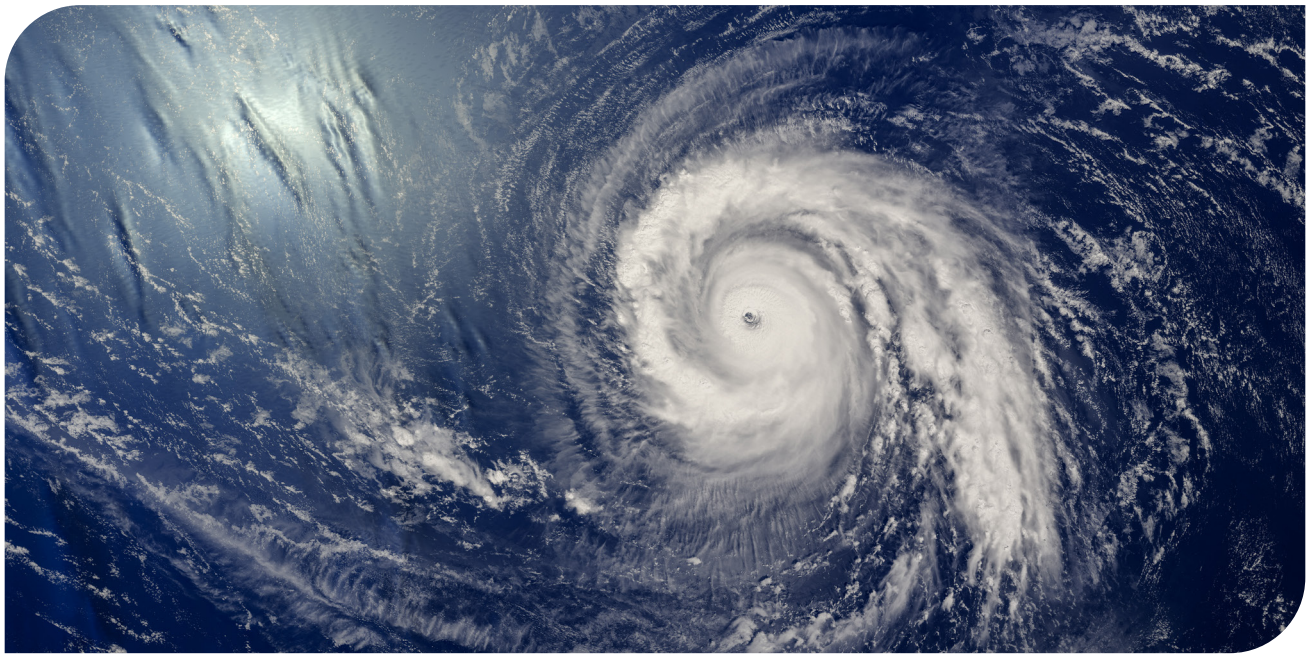
In the U.S. alone, there have been 25 confirmed weather/climate disaster events with losses exceeding $1 billion each.[3] With global temperatures poised to pass the 2°C limit enshrined in the 2015 Paris Agreement, the year (and years) ahead is unlikely to be any different and will hence require effective and actionable strategies to confront and tackle both near-term climate-driven threats and hazards, as well as to ensure longer-term climate resilience.

As climate change increasingly brings about more frequent and severe extreme weather events, corporations must proactively assess and address the potential risks and impacts on their infrastructure, operations and workforce. Comprehensive risk assessments will be essential to early identification of vulnerabilities in infrastructure, supply chains and operations.

These assessments should include leveraging appropriate risk intelligence capabilities to analyze historical weather data and collaborating with climate experts to understand location-specific climate risks and anticipate future threats.

This data-driven approach provides early warning indicators of relevant extreme weather events, empowering organizations to invest in infrastructure upgrades that can withstand extreme weather conditions, such as reinforcing buildings against storms or floods.

They can also help with developing comprehensive business continuity plans that include robust risk mitigation strategies to ensure resilience during extreme weather events and climate change impacts at large.



[3] Billion-Dollar Weather and Climate Disasters | National Centers for Environmental Information (NCEI) (noaa.gov)

09. Supply chain challenges, driven by global tensions, will continue to stress business operations

In our risk outlook for 2023, we noted that supply chain disruptions – driven by the fallout from the COVID-19 pandemic, the war in Ukraine, China-Taiwan tensions and other notable domestic and global dynamics – would continue to impact businesses well into the year.

While many corporations have sought and implemented alternatives to avoid dependencies on certain countries and industries, we nevertheless assess that global volatility and uncertainty will further exacerbate logistical challenges this year.

Reducing dependencies on one country or region may in turn create dependencies elsewhere, as evidenced by American businesses' manufacturing pivot from China, which has necessitated adaption to new regulatory environments and other logistical considerations. We, therefore, recommend businesses conduct regular scenario planning exercises to ensure that their business continuity plans are regularly stress-tested and strategies updated to reflect the most current and relevant intelligence.

Finally, and related to our assessment of extreme weather events above, we emphasize the importance of diversifying supply chains by sourcing materials, components and technologies from multiple regions to minimize dependency on regions or suppliers that might be vulnerable to specific climate and weather-related disruptions. As such, we recommend that business continuity and risk mitigation plans consider possible weather and climate-related disruptions and offer alternative routes for transportation and logistics, as well as consider inventory management that considers and can readily adjust to unexpected delays caused by extreme weather conditions.

10. "Vaccination fatigue" may disrupt the global workforce

As we enter 2024, influenza season is certainly upon us, with COVID-19 and respiratory syncytial virus (RSV) added to the mix, creating strains on workforce capacity.

Recent warnings from public health officials about declining enthusiasm for vaccinations could have significant implications for corporations and their people well into 2024. This necessitates a proactive effort to ensure that employees have access to updated information and the ability to obtain necessary immunizations, as well as thinking through the potential risks associated with declining vaccine enthusiasm.

In early December, the Centers for Disease Control and Prevention (CDC) issued an alert warning of the "urgent need" to increase domestic vaccinations against influenza, COVID-19 and RSV.[4] The alert noted that low vaccination rates and increases in domestic and global respiratory diseases could lead to additional, more severe diseases and increased healthcare capacity strains through the winter months.

The World Health Organization also recently re-issued its COVID-19 vaccination guidelines, noting that while the "emergency phase" of COVID-19 is over, continued immunization would reduce the likelihood of new variants emerging.[5]

Varying vaccination rates and waning enthusiasm for critical immunizations will have impacts on a company's workforce and potentially on cross-border travel, international collaborations and global business ventures. Declining vaccination rates may disproportionally expose certain demographics or regions to health risks, as well as create obstacles for workforce mobility and hence global business operations. Organizations will need to assess and implement policies and procedures that align with their workforce ethos and company values.

[4] Health Alert Network (HAN) - 00503 | Urgent Need to Increase Immunization Coverage for Influenza, COVID-19, and RSV and Use of Authorized/Approved Therapeutics in the Setting of Increased Respiratory Disease Activity During the 2023 – 2024 Winter Season (cdc.gov)

[5] https://www.who.int/emergencies/diseases/novel-coronavirus-2019/covid-19-vaccines/advice

Ensuring organizational resilience in 2024

The threats and trends noted above are by no means all-encompassing. We expect CEOs to deal with these and many more risks and challenges this year, all of which will reaffirm the need to prepare for and mitigate against both short- and long-term business disruptions that may challenge an organization's resilience. For executives charged with risk management, the global threat environment poses new and unique challenges, but at the same time, affords new opportunities to protect the value of the organization and lead resilient, transformative businesses.

Enterprise resilience is ultimately a business enabler and a driver for growth and innovation. At Teneo's Risk Advisory practice, our mission is to foster trust-based partnerships with our clients while helping them build resilience – via deep subject matter expertise, a threat-focused approach rooted in structured analytical techniques, industry-leading technological capabilities, and robust risk and crisis management experience – and to thrive in the face of a dynamic and ever-evolving risk landscape.

> CEOs and other C-suite executives must envision themselves as both risk and crisis managers. Critical to this is situational awareness. Before a crisis strikes – and it always will – CEOs and their teams must have built up the capacity to know what is unfolding in real-time during a crisis. CEOs must also embrace the idea that the worst-case scenario is possible again and again. The most effective way to ensure that crisis preparedness today can adapt to the future is to continuously stress test the system.

Juliette Kayyem
Senior Advisor, Teneo

Author

Naureen Kabir
Managing Director
naureen.kabir@teneo.com

For more information about enterprise resilience and intelligence, contact **TeneoRiskAdvisory@teneo.com**

Teneo®
The Global CEO Advisory Firm

Teneo is the global CEO advisory firm.

We partner with our clients globally to do great things for a better future.

Drawing upon our global team and expansive network of senior advisors, we provide advisory services across our five business segments on a stand-alone or fully integrated basis to help our clients solve complex business challenges. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other corporations, financial institutions and organizations.

Our full range of advisory services includes strategic communications, investor relations, financial transactions and restructuring, management consulting, physical and cyber risk, organizational design, board and executive search, geopolitics and government affairs, corporate governance, ESG and DE&I.

The firm has more than 1,600 employees located in 40+ offices around the world.

teneo.com