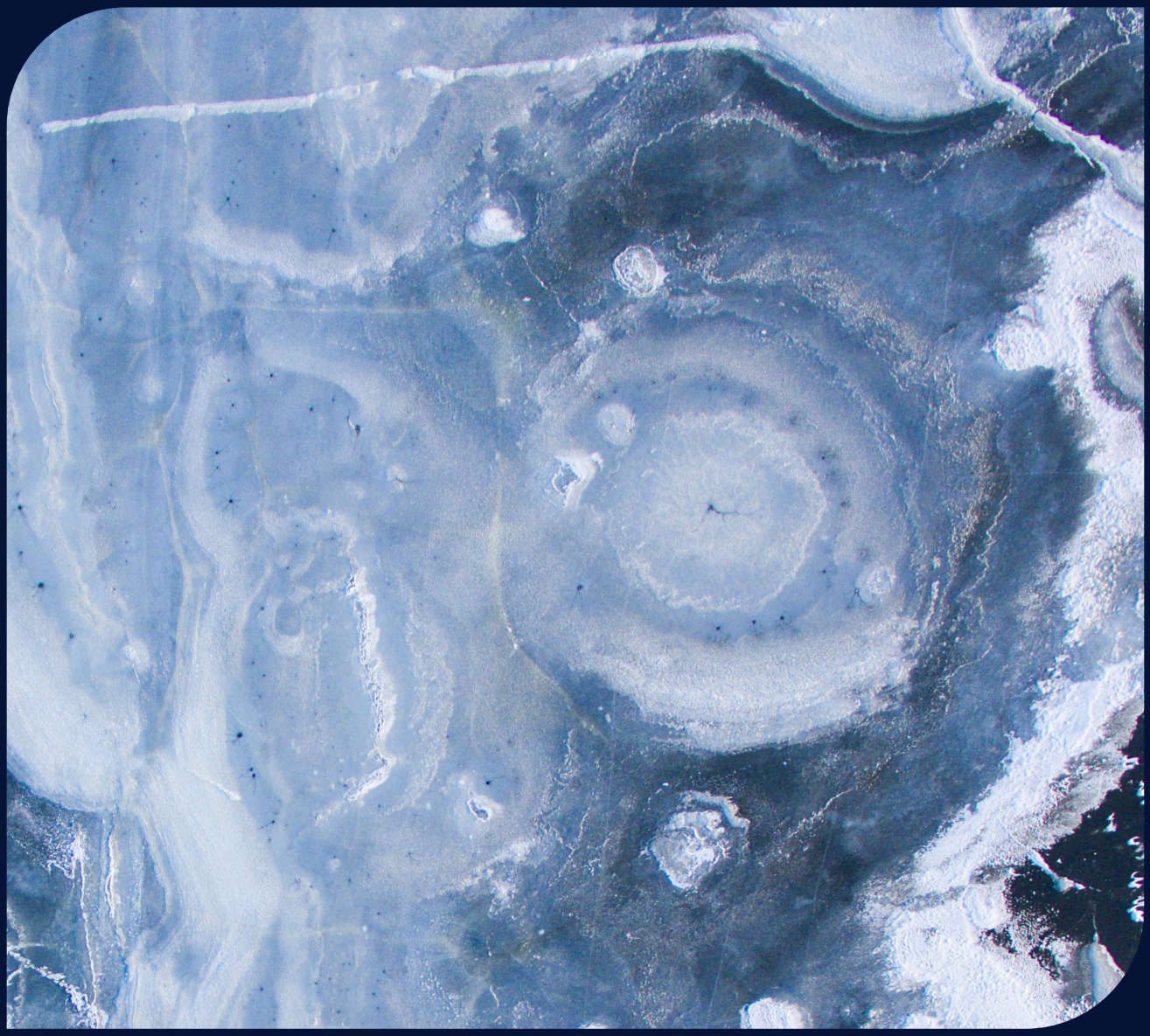
Teneo®

Risky Business: What We See in 2023

Teneo Insights / February 2023



Contents

Teneo Risk Advisory

As expected, the first few weeks of 2023 have been volatile and eventful, with escalating domestic and geopolitical tensions, a catastrophic earthquake and ensuing aftershocks, and the proliferation of generative artificial intelligence into the mainstream with yet unclear outcomes. We expect the rest of the year to follow in similar suit, with recessionary pressures, cyclical bouts of COVID-19 and war in Europe all continuing to amplify and further stress the security, reputational and operational risks facing C-suites and their organizations. Looking ahead, CEOs and corporate boards must remain steadfast in their resiliency planning and mitigation efforts.

Facing a New Year of Challenges

Companies today are facing an ever-expanding risk landscape that demands more attention from executives. On the security front, growing levels of both violent and petty crime are becoming significant enough to warrant the closure of franchise stores, while the increasingly remote nature of business is exposing companies to new and expanding cyber vulnerabilities from internal and external actors. Meanwhile, the growing politicization of domestic and global issues is prompting new vectors of risk around company reputation as customers begin to judge brands and their respective leadership by a corporation's public response – or lack thereof – to sensitive topics, such as the invasion of Ukraine, vaccine mandates, LGBTQ+ rights and abortion restrictions.

Operationally, although the world is three years removed from the initial outbreak of COVID-19, we assess supply chain disruptions will continue to impact businesses well into 2023, with domestic policies and the Russia-Ukraine war further exacerbating difficulties surrounding the global movement of goods. These operational challenges are compounded further by the potential of a global recession in 2023.

In the following pages, Teneo Risk will look across the risk spectrum – focusing specifically on security, reputational and operational risks – and assess the challenges most likely to impact companies and executives in the new year. As organizations face unprecedented threats in 2023, we aim to give CEOs and their companies the tools, analysis and intelligence to anticipate future risks and better prepare for unforeseen business disruptions on the horizon.

Security Risks to Businesses

As the global economic and social fallout of COVID-19 persists, political differences and societal tensions intensify and violent extremism proliferates, we assess that businesses will continue to face a volatile threat landscape in 2023. Domestically, violent crime rates have continued to rise, creating an increasingly unstable security environment for businesses that operate in urban areas, as murder, assault and robbery levels grew in 30 major urban areas in the first half of 2022 compared to that of 2021.[1] Relatedly, companies have continued to grapple with pervasive levels of petty crime, such as theft and vandalism, that increasingly detract from yearly revenues. The loss to retail businesses primarily due to external theft grew approximately USD 5bn year-over-year.[2] We assess that economic challenges stemming from war in Europe and rocketing inflation will further complicate the global security environment for corporations, as recessionary pressures lead to more layoffs and, by extension, a growing risk of insider threats from terminated or current employees. We further assess that cybersecurity concerns will remain a serious potential threat as the growing reliance on cloud computing and remote work make businesses and unwitting personnel a prime target for malicious actors.

"In a time of growing uncertainty on the global front, where the 'new normal' proves itself to be a state of constant flux, organizations must now contend with the fallout of persisting crime and outbursts of domestic unrest. Since 2020, growing rates of petty and violent crime continue to challenge businesses' security outlook. As such, risk managers and corporate security leaders must review their organization's crisis management and business continuity plans in anticipation of crime, protests, unrest and related challenges. Businesses operating in major cities must oversee comprehensive intelligence and resilience planning and prepare for escalations at a moment's notice. Coupled with global developments, 2023 will pose a host of persisting and emerging challenges."

Commissioner Bill Bratton,
Executive Chairman, Risk Advisory, Teneo

Insider Threat

Rising employee layoffs, most acutely felt in the tech industry, will add to the growing insider threat environment that has already seen insider threat incidents increase 44% over the last two years.[3] Insider threats, whether caused deliberately by angry employees looking to retaliate against a company or accidentally by careless workers who do not follow proper cyber and physical security policies, pose significant security risks to an organization. Looking ahead, we assess that organizations that are not able to minimize the security risks posed by an insider threat, such as the sabotage of company systems, theft of intellectual property and confidential information, or human error that can lead to stolen credentials, will be

1. Jake Horton, US Crime: Is America Seeing a Surge in Violence? BBC News, October 24, 2022
2. Loss Prevention Research Council and National Retail Federation, 2022 Retail Security Survey (National Retail Federation, 2022)
3. Insider Threats (Still) On The Rise Proofpoint, February 7, 2022

left most vulnerable to the ongoing risk of an insider attack. As the financial impact from an insider threat has grown 34% since 2020, with the cost of addressing an insider threat hovering around USD 15mn in 2022 versus just USD 11mn two years ago[4] and the cost of resolving credential thefts increasing from USD 2.79mn in 2020 to USD 4.6mn in 2022,[5] we further assess that the repercussions of remedying successful insider threats will continue to cost companies time and larger portions of their operating budgets.

Domestic Extremism

Extremist groups continue to expand their ranks and presence around the country, posing an increasing security threat to businesses. As of late 2022, extremist activity is on pace to top that of 2021, with armed demonstrations driven by white nationalism and anti-LGBTQ+ sentiment increasingly conducive to outbursts of violence.[6] A recent Department of Homeland Security assessment has identified that the U.S. remains in a heightened threat environment going into 2023 with the intensification of political issues and current events continuing to motivate threat actors to commit acts of violence. As protests from far-right militias and militant social movements such as Antifa have become nearly five times more likely to turn violent than traditional political protests,[7] we assess that the normalization of violence as a political tool will leave corporations and their personnel contending with a domestic security environment that continues to pose a persistent and significant threat to organizations' security in 2023.

Crime

Violent crime rates have continued trending upward, as ongoing impacts from the COVID-19 lockdowns, increasing gun ownership[8] and deteriorating police-community relations continue to take their toll on public safety. Persisting petty street crime in major cities, evolving bail reform and police staffing shortages have further compounded public safety challenges. A review of business losses attributed to crime between 2020 and 2021 identified organized retail crime as growing 26.5% and becoming a leading cause of retail sales losses, accounting for almost USD 94.5bn last year.[9] With a weakening economic outlook and growing inflation, we assess increasing crime levels will remain a top security concern for businesses in 2023.

Cybersecurity

Crippling cyberattacks have amplified the security risks facing companies as threat actors continue to find new avenues to hack corporations. Ransomware, malware and viruses are routinely introduced to company systems by unwitting employees unversed in proper cyber hygiene practices. Meanwhile, cybercriminals continue to exploit credentials to gain access to company systems, with 71% of companies blaming stolen account information on a system breach.[10] Moreover, we assess the growing online business model is leaving companies increasingly exposed to nefarious cyber-actors looking to leverage less protected technologies, such as the Internet of Things, to breach security protocols and steal sensitive company data. Separately, businesses increasingly must consider and assess potential risks generated from their third-party affiliates, ranging from suppliers, technology systems and supply chain resources. With businesses suffering 50% more cyberattacks per week in 2021 versus 2020,[11] and 41% of polled security executives doubting their organization's own ability to keep up with the risks posed by new technologies,[12] we assess cyber should remain a top security concern for CSOs and CISOs in 2023.

---

4. Ibid.

5. Ibid.

6. The Economist, America's Far Right Is Increasingly Protesting against LGBT People January 13, 2023

7. Roudabeh Kishi, From the Capitol Riot to the Midterms: Shifts in American Far-Right Mobilization Between 2021 and 2022 ACLED, December 15, 2022

8. Statista, Gun Ownership in the U.S. 1972-2022 December 7, 2022

9. Loss Prevention Research Council and National Retail Federation, "2022 Retail Security Survey."

10. Chuck Brooks, Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know Forbes, June 3, 2022

11. Ibid.

12. Ibid.

Reputational Risks to Businesses

Increasing public scrutiny in the wake of a more conscientious customer base has resulted in heightened risk to a brand's reputation, as companies' growing reliance on online communications like social media opens them to new threats stemming from mis- and disinformation campaigns and insider threats. C-suite-level business leaders have increasingly weighed in on issues once thought to be confined to the political sphere, directly situating their organizations in hotly contested debates. Conversely, consumers have also actively sought to uncover the perceived political perspectives of a company's C-suite team and, in turn, have associated those political viewpoints with the overall perspectives of the entire company. As executives contend with the intersecting challenges of a greater online presence and socially conscious consumer base, a range of reputational risks will persist, and likely intensify, well into 2023.

Increased Public Scrutiny

The number of Fortune 500 CEOs on at least one social media platform has jumped from 39% in 2015 to 70% in 2022[13] and continues to climb. While this increased connectivity between executive leadership, employees and consumers enables an organization to foster an authentic dialogue, it also gives clients a new ability to appraise a company's leadership 24/7. This in turn poses an increased risk to a company's reputation, as one errant comment on social media could harm a company's reputation. A host of sensitive topics in 2022, including the re-litigation of *Roe v. Wade*, the Respect for Marriage Act and record-breaking migrant border crossings have contributed to the growing trend of executives weighing in on socio-political issues. Increased public scrutiny of CEOs has been a key driver for chief executives taking a public stand on important societal problems, a trend we assess will persist in 2023. While weighing in on an important issue may be necessary due to public pressure and drive reputational benefit, it can also present reputational challenges from a variety of stakeholders. In 2022, Disney faced severe and widespread condemnation on social media for publicly opposing new Florida legislation related to LGBTQ+ issues.[14] Contrarily, silence on certain political issues also poses a significant reputational risk, potentially inviting accusations of complacency. In 2023, we recommend executives remain attuned to the reputational impact of participation (or lack thereof) in public discourse.

"Increased public scrutiny of CEOs has been a key driver for chief executives taking a public stand on important societal problems."

13. Sprout Social, #BrandsGetReal: Brands Creating Change in the Conscious Consumer Era, July 2, 2020

14. Sarah Whitten, Disney CEO Bob Iger Addresses 'Don't Say Gay' Fallout, Importance of LGBTQ Inclusion in Stories, CNBC, November 29, 2022,

Disinformation and Misinformation

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. Although social media platforms have enhanced content moderation policies to counter the proliferation of dis- and misinformation, disparate approaches to content moderation and ever-evolving internal platform policies routinely leave account users as the first line of defense when trying to ensure the safety of their brand online. For example, despite numerous changes to Twitter's user authentication system as a new way to combat "inauthentic activity," malicious online actors took advantage of the new process to impersonate corporate Twitter accounts. A false account, @EliLillyandCo, posted that they were now offering free insulin, causing mass confusion and significant disruption to Eli Lilly, which had to offer an official apology. As a result of the disinformation, shares of Eli Lilly dropped 6%, reducing its market cap by almost USD 1bn.[15] With an estimated 97% of Fortune 500 companies relying on social media for communications and brand advertising,[16] these risks will continue to remain at the forefront of executive and board concerns going forward.

Insider Threat

In addition to security risks stemming from insider threat situations, organizations can also face significant reputational risk as a result of insider threat-related actions. Businesses that pride themselves on security and privacy can have their brand image irrevocably damaged if an insider threat leads to a leak of private user information. A 2022 Microsoft Insider Risk Report found that, on average, companies view "damage to a brand or reputation" as the second highest impact to an organization from an insider risk event, just behind "theft or loss of customer data."[17] Although it is easy to quantify the growing financial impact of a single insider risk incident based on the value of loss and the cost of recovery, companies often struggle to quantify the ripple effects of such an event on their reputation in the long term. Further, 2022 saw the intensification of a relatively new type of insider threat, in which former employees increasingly vocalized post-layoff frustrations via high-trafficked media outlets. This was best exemplified by former high-ranking tech executives publishing op-eds or conducting news interviews.

15. Ben Adams, Eli Lilly Pulls Twitter Ads after Blue Check Fallout: Report, FiercePharma, November 15, 2022

16. Sprout Social, #BrandsGetReal: Brands Creating Change in the Conscious Consumer Era.

17. Building a Holistic Insider Risk Management Program, Microsoft (Microsoft Security, 2022)

Cybersecurity

In addition to impacting a company's security, data breaches divulging sensitive company or user information have the added risk of damaging an organization's reputation. Outside of the incurred financial losses from trying to remedy a data breach, including containing and cleaning up after a ransomware attack, as well as increasing cyber insurance costs, companies face consequences related to brand image and business revenue due to decreased customer confidence in the organization. Recent accelerated digital transformation across the world has resulted in more user privacy data and Personally Identifiable Information (PII) placed on company cloud networks and digital applications. This data has also been increasingly used for business monetization purposes with or without consumer knowledge. Data breaches of these networks and applications not only harm brand reputation but can also potentially expose a company's breach to data protection laws. T-Mobile currently faces a proposed class action that alleges it failed to exercise "reasonable care" in safeguarding the sensitive private information of millions of consumers from a data breach reported in January 2023.[18] This comes after a similar breach of T-Mobile customer information just two years prior. In 2021, 53% of organizations indicated that their brand and reputation were damaged following a ransomware attack.[19] With ransomware costs projected to grow from USD 20bn in 2021 to over USD 260bn in 2030,[20] we assess that the continued proliferation of ransomware and phishing attempts, which increased 61% over the first six months of 2022 alone,[21] mean that the two most significant drivers of data breaches will remain a high-priority risk for corporate leaders to monitor in the near and long term.

"Cybersecurity has to include a holistic and clear approach that lays out threats and vulnerabilities and the specific risks they pose to the company. This means that communication of the most significant risks is clear to the C-suite, board and decision makers and maps to security and business needs. The entire cybersecurity environment must include business partners, third parties and others with the capability of impacting the company's networks and data. It also means that both cyber and physical security components have to work in tandem. There is no magic formula, but a competent cybersecurity strategy that encourages continuous practice and lays out the defensive priorities (to protect 'the Crown Jewels' of the company) can provide a good basis for resource and skill requirements and return on investment."

Rhea Siers, Senior Advisor, Teneo

18. Corrado Rizzi, 2023 T-Mobile Data Breach Sparks Class Action Lawsuit, ClassAction.org, January 25, 2023

19. Sam Curry, Report: Ransomware Attacks and the True Cost to Business, June 2021

20. Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031, Cybercrime Magazine, June 2, 2022

21. Ibid.

Operational Risks to Businesses

We have detailed the rising complexities and challenges companies and CEOs face in mitigating risks generated from risk vectors from a physical and reputational security perspective. However, these risk vectors also have an impact on a company's ability to operate in a regular capacity. We therefore assess continued aftershocks of COVID-19, the conflict in Ukraine and other geopolitical tensions, rising economic headwinds, cyberattacks and supply chain disruptions will persist through 2023 and present operational challenges for businesses moving forward. This will require leadership to consider preparation via proactive and reactive threat management and strengthening of operational competencies.

Economic Headwinds

As the world confronts intersecting shocks in geopolitics, energy and commodities markets, with stubbornly persisting inflation, the global economy may find itself in a recession in 2023, amplifying businesses' operational risk outlook. Teneo Risk assesses that disruptions to global supply chains will continue to impede business operations in the new year, constituted by port holdups and reduced container availability, surging prices and product shortages. Amid these challenges, transnational trade cooperation may grow elusive, furthering trade disruptions, while cybercriminals will seek to exploit growing logistical vulnerabilities. Relatedly, inflationary pressures have prompted rate hikes by central banks,[22] limiting access to the capital imperative for investments in business operations. These shocks and resulting fallouts will challenge business leaders to shore up business continuity plans and operational competency measures to adjust for changes in supply chain, workforce and economic conditions. We assess that businesses that fail to proactively review business continuity plans and pressure test them for turbulent disruptions ahead will face significant operational setbacks.

Cyberattacks

As technology continues to evolve and become more central to company operations, so does the severity and impact a cyberattack can have on a business. Cyberattacks have wide-ranging consequences for a company ranging from physical security and reputational impact to operational consequences. Recent data suggests that around 21% of global organizations experienced a ransomware attack in 2022. Of those, 43% had a significant impact on their business operations.[23] We assess cybercriminals will continue to become more sophisticated in 2023 as they look to target cloud computing, Internet of Things technologies and vulnerabilities exposed by inherent human errors. To contend with the ever-changing cyber threats facing companies, we recommend organizations establish robust cyber policies that address internal cyber best practices and technology protocols. These internal audits and adaption of new cyber policies and best practices will also need to be pressure tested and applied to third-party affiliates associated with a business. Additionally, corporate leaders will need to consider the growing regulatory impacts of cybersecurity incidents. Globally, data privacy regulators increasingly expect organizations to be accountable for personal data governance. As more data incidents occur and investigations are conducted, we assess regulators will increasingly issue increased penalties to companies failing to put adequate protection measures in place to safeguard customer and employee information.

22. Central Banks Hike Interest Rates in Sync to Tame Inflation Pressures, IMF, August 10, 2022,

23. Mahima Jaiswal, Top 5 Cybersecurity Trends to Keep an Eye on in 2023, Security Boulevard, December 26, 2022,

Global Conflict

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. With little hope for serious peace negotiations, we assess the conflict will continue to present operational challenges in 2023. As the war in Ukraine has made abundantly clear, regional conflicts can have significant and far-reaching consequences. We recommend corporations remain attuned to a range of current and emerging geopolitical tensions to adequately assess and prepare for potential operational repercussions.

COVID-19 and Future Pandemics

The COVID-19 pandemic had unprecedented impacts on the global economy, labor markets and supply chains. We assess that the headwinds caused by COVID-19 and emerging subvariants will continue to impact business operations in 2023, forcing corporate leadership to account for persisting health crises and the ever-present threat of another pandemic severely disrupting operations. In the U.S., the most transmissible COVID-19 variant to date has recently set off a fresh wave of infections, evading immune defenses through a potent array of mutations.[24] Relatedly, China's abrupt pivot away from "zero-COVID" prompted a surge in infections across the world's most populous country, potentially paving the way for hundreds of millions of new cases generated in the country in the coming months, resulting in even more transmissible variants primed to spread globally.

Extreme Weather

Extreme weather events such as wildfires, flooding, droughts and hurricanes have reached unprecedented levels in 2022, with the United States alone contending with 18 "billion-dollar disaster" events, more than 7 million acres burned by wildfire, the worst drought in the American West in 1,200 years and the third-most destructive storm on record in Hurricane Ian.[25]

In addition to the loss of life and general human suffering, these events have resulted in catastrophic economic and infrastructure damage. We assess these weather phenomena will likely continue, and may even increase, in 2023. As the impact of weather-related incidents intensifies, we recommend business leaders reevaluate security and operational plans to adjust for more frequent and increasingly damaging weather events, considering how operations can withstand these events with as little disruption as possible. We further recommend this process range from physical location security assessments to reviews of external vulnerabilities generated from reliance on local infrastructure, such as employee transportation methods and power and electricity sources. For supply-chain businesses, this may include the development of adaptation strategies, such as moving critical logistics centers away from storm-prone locations to diversifying sourcing and distribution channels.

"The knowledge of disasters' inevitability requires executive leadership, especially CEOs and other C-suite executives to envision themselves as both risk and crisis managers. CEOs must incorporate basic design features into their organizations that embrace the idea that the worst-case scenario is possible again and again. And again. What then? The most effective way to ensure that the planning of today can adapt to the future is to continuously stress test the system. Stress tests, when enacted thoroughly, cannot be underestimated, adding purposeful variation to preparedness as it challenges any existing planning. Most importantly, these tests can expose where a response system has gaps or weaknesses, providing key analysis by putting operational issues under scrutiny."

Juliette Kayyem, Senior Advisor, Teneo

24. Johns Hopkins Coronavirus Resource Center. XBB.1.5 COVID Variant, n.d.

25. NOAA National Centers for Environmental Information (NCEI), U.S. Billion-Dollar Weather and Climate Disasters, 2023, n.d., DOI: 10.25921/stkw-7w73

The Way Forward in 2023

As detailed above, Teneo Risk assesses 2023 will present organizations with a robust threat landscape comprised of complex and intersecting security, reputational and operational risks. Going forward, we recommend CEOs, their risk managers and relevant executive leadership remain diligent in their resiliency planning and preparedness to counter these risks.

At Teneo Risk, we bring hands-on experience from roles in government and public affairs, macroeconomic policy and geopolitical risk, management consulting, military, intelligence, law enforcement, public health, and physical and cybersecurity – all of which enable a unique point of view on building and refining resilience. Our practice is rooted in decades of expertise and first-hand experience leading cities and organizations through the aftermath of both man-made and natural disasters, from cyberattacks, mass shootings and environmental crises to the 9/11 attacks and Hurricanes Sandy, Katrina and Andrew. We understand the challenges of anticipating and preventing risks to corporations and in turn build robust mitigation strategies rooted in data analysis, risk intelligence and experience, agile advisory adaptable to each organization's unique challenges.

Authors

Teneo Risk Advisory – Resilience & Intelligence

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 41 offices around the world.

teneo.com