Teneo®

Resilience and Intelligence 2026 Outlook:

Operating Through Disruption

Teneo Insights / February 2026

Foreword
The Persistent Risk Era

As we enter 2026, every sector, geography and boardroom faces the shared reality that risk is no longer episodic – it is persistent. The question leaders now face is not whether disruption will occur, but whether their organizations are prepared to navigate and, in fact, capitalize on recurring challenges.

Teneo's Risk Advisory business' Resilience and Intelligence 2026 Outlook focuses on key considerations for leaders across resilience and physical security, strategic intelligence, public safety, cybersecurity, climate risk and family office concerns by highlighting what matters most: risk exposures that compound quickly, blind spots created by assumptions and actions that convert reactivity to proactivity.

A consistent theme runs through the most significant takeaways for the new year, with success benchmarked not by which leaders have the most policies, tools or reassuring narratives, but by who challenges current frameworks, integrates people, process and technology and adjusts to a new normal of anticipating and maintaining flexibility in the face of challenging developments.

At Teneo, this imperative persists across domains. In the corporate resilience arena, leaders underestimate insider threats and lack structured response frameworks. Throughout strategic intelligence initiatives, domestic and international volatility present risks with organization-by-organization impacts, creating the requirement to separate relevance from noise. For public safety organizations, the allure of cutting-edge security technology and artificial intelligence cannot compensate for sound policies and integrated operational frameworks. Likewise, privacy concerns in the cybersecurity context are entering a more demanding period of accountability, with business and regulatory consequences for organizations that lack strategic governance. For family offices with unique sensitivities and security concerns, visibility itself has become a risk vector, where physical, cybersecurity, travel and family concerns all combine. Across it all, climate risk is no longer restricted to ESG conversations, with cascading impacts throughout infrastructure and markets creating a new operational reality.

While these dynamics manifest across different functional areas, they represent connected components of the same risk environment. Despite the promise of sustained disruption in 2026, leaders have an opportunity to implement sound policies, technology and strategic frameworks that will promote their organization's ability to anticipate risk and succeed in challenging moments.

William J. Bratton
Executive Chairman
Risk Advisory
william.bratton@teneo.com

Courtney Adante
President
Security Risk Advisory
courtney.adante@teneo.com

Contents

Persistent Enterprise Risk Requires Investments in Verification, Insight and Readiness

As 2026 brings enduring risk, the organizations that perform best in this ever-evolving environment are not those with the thickest policies or the most reassuring assumptions, but those that invest in verification, insight and readiness. Four areas in particular will define the resilience gap between leaders and laggards in the coming year.

Executive protection is no longer optional

Executive protection (EP) has crossed a threshold. What was once treated as a niche service of convenience for a handful of senior leaders is now a core component of enterprise risk management, reputation protection and business resilience.

Threats to executives are more frequent, more personalized and more publicly amplified. Social media, political polarization, labor activism, litigation exposure and grievance-driven violence have collapsed the distance between a perceived slight and real-world harm. The myth that executive protection is about status, optics or executive ego has been decisively disproven.

In 2026, the most effective programs will be those that integrate risk intelligence, travel security, digital exposure management and crisis communications into a single operating model. Executive protection is no longer just about physical safety, it is about preventing a single incident from becoming a cascading reputational event.

Organizations that continue to treat EP as a reactive or standalone function, focused more on convenience than the threat environment, are taking unnecessary, avoidable and visible risk.

Workplace violence: The insider threat that is still with us and expanding

Despite years of data, training modules and post-incident reviews, workplace violence, particularly insider-driven violence, remains one of the most misunderstood and poorly managed enterprise risks.

The uncomfortable truth is this: most incidents are not sudden, random or unforeseeable. They are preceded by behavioral anomalies, grievance signaling, policy friction or personal destabilization that goes unrecognized, or worse, unacted upon.

In 2026, organizations must move beyond awareness training and toward structured threat management. This framework entails real behavioral threat assessment, cross-functional case management and leadership willing to intervene early rather than defer to human resource processes alone.

The cost of getting this wrong is not just physical harm, it is moral injury, litigation exposure, regulatory scrutiny and lasting damage to organizational trust. Insider threat is not a security problem alone; it is a leadership problem.

Security technology: From capability to credibility

The security technology landscape has never been richer or more confusing. AI-enabled video analytics, real-time intelligence platforms, gunshot detection, access control, body-worn cameras and mass notification tools are advancing rapidly, but technology alone does not create resilience.

In 2026, the differentiator will be integration and disciplined use, alongside use cases that create business value outside the security vertical, not novelty. Too many organizations have accumulated tools without clarity on how they support prevention, response or decision-making. Technology that is not operationalized creates false confidence. And false confidence is one of the most dangerous risk conditions in physical security.

Leading organizations are investing in platforms that support confirmation over assumption: real-time visibility, verifiable data and the ability to rapidly validate what is happening on the ground. Security technology is no longer about monitoring; it is about enabling faster, better and defensible decisions when it matters most.

Critical infrastructure resilience: You cannot protect what you do not inspect

Finally, critical infrastructure resilience will demand renewed focus in 2026, not just at the policy level, but at the physical and operational edge.

From data centers and utilities to logistics hubs and remote facilities, too many organizations rely on outdated assessments, self-reported compliance or theoretical controls. In an era of climate volatility, supply chain disruption and targeted attacks, this approach is no longer sufficient.

Resilience requires onsite insight. It requires inspection, validation and independent assessment of real-world conditions, especially in locations that are remote, lightly staffed or assumed to be "low risk." Assumption is the enemy of resilience. Confirmation is the standard.

Organizations that invest in scalable inspection, assessment and validation capabilities will outperform those that rely on spreadsheets, attestations and hope.

In 2026, leaders must challenge programmatic assumptions

In 2026, effective risk management will favor organizations that are clear-eyed about their exposures, disciplined in their preparation and willing to challenge long-held assumptions. Corporate resilience is no longer about avoiding disruption; it is about demonstrating credibility under pressure. The question leaders should be asking is not "Do we have a program?" It is "Have we proven it works?"

Brian Stephens
Senior Managing Director and Head of Resilience and Security Solutions
brian.stephens@teneo.com

Strategic Intelligence as Decision Advantage

Disruption is no longer episodic. It is a defining feature of today's operating environment.

Geopolitical volatility, domestic and ideological polarization, rapid technological acceleration and social grievances now intersect in ways that are persistent, fast-moving and increasingly difficult to disentangle. For board and executive teams, the challenge lies not in anticipating or predicting every disruption. Rather, it lies in sound judgment: helping leaders understand what matters to their organizations, why it matters and what decisions it should inform – long before events force decisions under pressure.

As we look to 2026 and beyond, the organizations best positioned to succeed – to navigate disruptions and crises, absorb geopolitical and domestic shocks and withstand sustained public and societal scrutiny – will be those that are relentless in tailoring intelligence to their own priorities, assets and vulnerabilities. In this ever-dynamic environment, strategic intelligence is not a luxury – it is a necessity.

Geopolitical volatility is constant: Its consequences are not

Global developments from the first few weeks of January have already underscored the persistence and breadth of geopolitical volatility. Renewed large-scale strikes in Ukraine, shifting Saudi-UAE dynamics in Yemen, escalating instability in parts of West Africa, renewed unrest in Iran and recent U.S. actions in Venezuela – to name a few – illustrate how geopolitics and global security developments are unfolding in parallel, at pace and across regions and issue sets.

These developments also do not translate into uniform risk. Their implications vary significantly depending on organizational footprint, priorities, stakeholder exposure and risk tolerance, reinforcing the need for strategic and actionable intelligence that distinguishes relevance from noise.

In Venezuela, for example, energy companies may weigh investment potential against political stability and security risk, while financial institutions may assess prospects for debt restructuring, asset recovery or early-mover advantage alongside heightened governance and security concerns. Organizations with regional exposure must also consider potential impacts of political and security uncertainty going forward, as well as impacts on labor flows, supply chains, operational continuity and physical security.

Even organizations without direct exposure may experience second- and third-order effects. Reputational considerations further complicate decision-making: some firms will face scrutiny for moving too quickly into a fragile environment, while others may be criticized for failing to engage at all.

The critical point is this: none of these implications are generic. Every organization must weigh its own operational, reputational, political and security risks against opportunities at hand. Strategic intelligence enables leaders to decipher this complexity and translate geopolitical disruption into informed, defensible decisions.

Artificial intelligence is transformative – Risk and opportunity are not universal

Artificial intelligence presents a similar challenge. Public discourse often treats AI as a singular opportunity or disruption. In practice, AI-related risks and opportunities vary by industry, geography and business model. Developments that may be existential for one organization are peripheral for another. Emerging copyright and intellectual property cases, for example, are likely to reshape risk calculations for media, entertainment, technology platforms and data-intensive businesses, while leaving other sectors comparatively untouched. Similarly, federal action to override state-level AI regulation in the U.S. could materially alter compliance strategies for organizations operating across multiple jurisdictions, while mattering far less to firms with narrower exposure.

The common mistake is equating awareness with preparedness. Staying informed about AI developments does not, on its own, enable organizations to manage risk or capture opportunity. Preparedness depends on disciplined analysis of which AI developments intersect with an organization's data assets, regulatory exposure, workforce, brand and customers – and which do not.

Once again, the intelligence advantage is not knowing everything. It is knowing what matters most to the organization's strategy and acting on that insight with intent.

Domestic tensions are rising; Organizational exposure is expanding

Disruption is not confined to foreign theaters or emerging technologies. Domestic instability, driven by factors such as political polarization, grievance-driven activism and political violence, has become a material and persistent risk factor for organizations. Incidents in both the U.S. and globally in recent years have demonstrated the convergence of political, ideological and personal grievances driving targeted attacks against political figures, executives and symbolic institutions.

Increasingly, individuals are targeted not for specific actions, but for what they represent: a policy position, an industry or a perceived societal inequity. This shift has profound implications for organizations. Executives and senior leaders should no longer be the sole focus of concern. Any employee may face heightened exposure if they become closely associated with controversial policies, decisions or public messaging.

This reality reinforces the need for proactive strategic intelligence that assesses reputational, political and security risks tied to organizational policies, activities and narratives – well before tensions escalate into crisis.

Crisis is inevitable – Intelligence shapes the outcome

Disruptions cannot be eliminated, but impact can be minimized and outcomes can be shaped. No amount of anticipatory intelligence can prevent disruption or crisis entirely. What it can do is cut through the noise in moments of acute uncertainty and determine how effectively organizations respond when crises occur.

During periods of acute disruption, several dynamics reliably hold true. Information environments become saturated with misinformation and disinformation. Decision-makers face intense pressure to act quickly, often with incomplete and conflicting information. Stakeholders – employees, investors, customers, regulators and the public – demand clarity, confidence and reassurance.

In these moments, timely and reliable intelligence is indispensable. Intelligence must shift from anticipation to execution. Real-time analysis, narrative tracking and scenario-based decision support enable leaders to prioritize actions, allocate resources and communicate with credibility.

Organizations that enter crises and disruptions with a clear understanding of their unique risk exposure and priorities – and with intelligence functions deeply embedded in their response structures – are better positioned to protect their people, assets, operations and reputation, while also identifying strategic opportunity amid disruption.

Intelligence as a strategic enabler

Looking ahead, the defining challenge for organizations is not the presence of disruption, but whether leaders will recognize early indicators, understand their relevance and act with intent. Strategic intelligence provides that edge. When intelligence is tailored, anticipatory and relentlessly focused on the "so what" and the "now what," it moves beyond insight and becomes a strategic enabler. In an environment defined by uncertainty, the advantage does not come from certainty or prediction, but from judgment informed by intelligence.

Naureen Kabir
Managing Director and Head of Strategic Intelligence and Crisis Situations
naureen.kabir@teneo.com

The Risk of Mistaking Technical Capability for True Security

As security technology advances, solutions require a holistic approach to integration

As we look ahead in 2026, conversations around security will increasingly be dominated by artificial intelligence's role in security technology and AI's role in automating public safety solutions. AI is positioned as the next breakthrough solution – faster detection, smarter analytics and predictive capabilities. These tools are powerful, and in many cases necessary, but the danger lies in mistaking capability for security.

Much like gates, guards, weapons and sensors, AI is a force multiplier – not a solution in isolation. Regardless of the technology of the day, security failures typically occur because systems were disjointed, people were unprepared, processes were unclear, intelligence was misunderstood or leaders hesitated to make a decision. The future of public safety and security will not be decided by who adopts the most advanced technology, but by who integrates it best.

Cutting-edge technology must be fused with people, processes and leadership into a unified system designed for real-world complexity. Without that integration, there will always be failure.

Well-trained, alert personnel with clearly defined roles and accountability are irreplaceable. AI can surface insights, but humans must interpret context, recognize nuance and act under surprise pressure.

Next generation technology heightens the importance of sound procedures

Processes will matter more than ever. As technology becomes more sophisticated, clear procedures for routine operations, escalation and crisis response are essential. AI may identify anomalies, but without disciplined processes, those signals can be ignored, misunderstood or acted upon too late.

Intelligence and awareness will also separate leaders from slow movers. AI technology excels at data aggregation, but understanding threats requires insight into human behavior, intent and environmental dynamics. The most advanced systems will still fail if leaders do not ask the right questions or challenge assumptions.

Finally, leadership and culture will define resilience. In moments of uncertainty, technology does not make decisions, leaders do. A strong security culture, where responsibility is shared across the organization, ensures that technology enhances judgment rather than replaces it.

As AI technology continues to reshape the security landscape, the question for 2026 is not "What technology do we have?" but "How well do our people, processes, intelligence and leaders work together when it matters most?" Security has never been about tools alone. The future will be no different.

David Cagno
Managing Director and Head of Public Safety Solutions
david.cagno@teneo.com

2026 and Cybersecurity: The Year of AI Corrections

2026 will likely be an instrumental year for cybersecurity in its evolution from an overhyped buzzword to a robust practice. In 2025, we saw the world come to grips with the non-negotiable need for strong cybersecurity, a tug-of-war between enforcement and litigation and artificial intelligence reach a tipping point as companies applied it haphazardly and without strategy.

At Teneo, we assess that 2026 will likely be a year of corrections – where AI usefulness depends on how strategically it is implemented, boards and insurers refuse to accept ambiguity on cybersecurity and regulators move from rule-writing to penalties. These throughlines will present themselves at every level of business as the world comes to grips with, and tries to keep pace with, the speed of technological progress.

As AI becomes useful at scale, its paradox becomes real

Failure to adopt AI will render your company obsolete. At the same time, integrating AI in arbitrary ways, for ad hoc needs or solely to stay relevant, leaves your company vulnerable to real-world, existential cyber incidents. This means the only option is strategic oversight and long-term planning. Companies need C-suite level vision and oversight, with single-voice roadmaps that benchmark progress, budget allocation and expectations and appetite for risk when it comes to adopting automated tools and standards.

Emerging litigation frameworks highlight the growing risk of failing to strategically integrate AI systems. Even as regulatory frameworks on AI develop, the U.S. Securities and Exchange Commission has acted against firms for both overemphasizing the robustness of AI processes and exaggerating related internal controls. Private litigation has followed this trend, with law firms increasingly launching securities class action suits related to how inflated AI claims and undisclosed limitations impact company value.

Internal AI functions are also increasingly posing legal challenges, particularly across corporate tools such as Microsoft's Copilot or Google's Gemini, which are used to draft emails, summarize chat threads and compile meeting notes. All of these functions may become relevant in forensic investigations and related litigation, further underscoring the need for sound governance.

While all these dynamics pose risks, they also present opportunities. As companies integrate automation with purpose and vision, a methodical approach to testing, governance development and legal planning is essential. For large firms with a national presence and investments in critical infrastructure, the broad adoption of AI also creates an opportunity to lead the industry in understanding and mitigating AI's strain on energy systems. The moment of opportunity is now for those seeking to set the standard for managing AI's impact on the U.S. grid.

Verifiable accountability: Why everyone needs to get real on privacy

Companies today face a growing body of case law and regulation that requires verifiable accountability. This means being able to provide on-the-spot clarity about what sensitive data sits in a company's systems, what that data is, how it is protected and who is liable if those systems fail. On the other side, consumers are being forced to confront an increasing number of tools and datasets that expose their sensitive information, as well as a growing range of ways that data can be exploited. Meanwhile, liability and responsibility are shifting toward individuals, with heightened requirements for corporate executives even as private individuals face new burdens to protect themselves.

The year 2025 featured notable developments to compel accountability. In April, JPMorganChase fired a warning shot to its vendors: get serious about cybersecurity and data privacy or we will not work with you.[1] Others across industries followed suit. At the start of this year, new provisions under the California Consumer Privacy Act (CCPA) came into effect, increasing executives' responsibility in the case of data breaches or mishandling of sensitive data.[2]

An increasing focus on enhanced governance frameworks follows 2025's banner year for data breaches, with some 16 billion records exposed – equivalent to two records for every person on Earth. What set data breaches in 2025 apart was not a spike in zero-day exploits or sophisticated malware, but rather the overwhelming reliance by malicious actors on identity-based access. Stolen credentials, abused OAuth tokens, social engineering and poorly governed SaaS permissions emerged as the primary entry points. In many of the most consequential cybersecurity incidents of the year, no malware was deployed and no firewall was breached. Attackers simply authenticated successfully and operated as legitimate users.

Security research published throughout 2025 consistently showed that credential theft accounted for more than 60 percent of initial access in large-scale breaches. Ransomware groups streamlined their operations into dependable double-extortion models, while infostealer malware quietly sustained an underground market for credentials and session tokens. By year's end, data breaches no longer appeared as isolated breakdowns but as evidence of systemic exposure across modern digital environments.

This trend highlights a mismatch with emerging regulatory frameworks like CCPA. Systemic, corporate failures define the problem, but leadership is left to deal with the incident's aftermath. This dynamic calls for a proactive, robust strategy that clearly articulates expectations for data protection across the enterprise. Likewise, in the individual realm, the era of no exposure is over. Both corporations and individuals must distinguish between acceptable and unacceptable exposure levels and implement sustainable, realistic and continuously monitored guardrails to maintain them.

Technical scrutiny becomes the bare minimum for transactions

From the hard lessons following the free-money era of 2020–2022, to those who invested in AI vaporware between 2023–2025, and the legal ramifications for companies crippled last year by cyberattacks due to data mismanagement, the world today requires that technical due diligence be conducted at every level of a sales or investment cycle.

For investment, it is critical to secure partners who understand the market and governance structures. For purchases, conduct technical testing of products and software before investing. For vendors, maintain tailored and relevant standards for the companies with whom you engage and recognize that blanket requirements often serve as roadblocks rather than defenses.

If all you have is incident response, you are already behind

Teneo's Risk Advisory team works with our clients to capitalize on the growing chasm between companies that react to cyber incidents and those that plan for them, monitor for them and gain distance from their competitors by smartly integrating best-in-class technology. In 2026, ensure your company maintains industry-appropriate compliance and vetted vendors; develop a roadmap for cybersecurity maturity with substantive budgeting; and stay ahead of the technological curve without purchasing or investing in vaporware.

Elizabeth Buckley
Managing Director and Head of Cyber and Technical Solutions
elizabeth.buckley@teneo.com

1 An open letter to third-party suppliers

2 CCPA - Effective January 1, 2026

Climate Risk is No Longer a Forecast – It is a Business Reality

For years, climate risk seemed to live comfortably in the future tense. It was modeled, disclosed, scenario-tested and deferred. Climate risk sat alongside other long-term concerns: important but distant, something to be managed over decades rather than quarters. That distinction no longer holds.

Climate risk reflects two realities: the potential for physical climate impacts to disrupt operations and financial performance, and the potential for societal responses to an organization's climate impact to affect governance, reputation and value.

In 2026, climate risk is now a real-time operating condition for businesses and the global economy. It is disrupting markets, infrastructure, labor and capital flows today. At the same time, it is reshaping how organizations are evaluated by investors, regulators, customers, employees and communities across geographies. What makes this moment different is not simply the intensity of climate events, but the way their effects cascade across systems and trigger immediate market, regulatory and societal responses. It is not about what the planet might do in 2040. It is about how organizations are exposed right now.

From isolated events to systemic disruption

In March 2021, a single container ship lodged sideways in the Suez Canal halted nearly 12 percent of global trade for six days.[3] The blockage was not climate-driven (although a sudden gust of wind was suggested as a contributing factor), but it revealed a defining characteristic of modern risk: highly optimized global systems now fail nonlinearly. Small disruptions can generate outsized consequences when infrastructure, logistics and markets are tightly coupled. Climate events increasingly behave in similar ways, with broader scope and deeper persistence.

In 2022, catastrophic flooding submerged roughly one-third of Pakistan.[4] Beyond the immediate humanitarian crisis, the economic consequences reverberated globally. Pakistan is a major producer of cotton, and flood damage disrupted textile manufacturing and international apparel supply chains.[5] Domestically, food inflation surged and fiscal pressure intensified, with an estimated loss in gross domestic product (GDP) of around 2.2 percent of FY22 GDP as a direct result of the floods. The International Monetary Fund explicitly linked the floods to macroeconomic instability, inflation and heightened sovereign risk, illustrating how climate shocks translate directly into financial and capital-market concerns.[6]

In 2023, Canadian wildfires sent smoke across North America and into Europe. Air quality deteriorated thousands of miles from the burn zones. Airports closed, outdoor labor slowed and health systems absorbed additional strain.[7] Public health authorities documented respiratory and productivity impacts far from the fires themselves, underscoring how climate risk increasingly crosses borders without moving assets or supply chains.[8] These events differ in geography, development context and exposure, yet they share a common pattern. The primary hazard was not the primary loss driver, but rather the cascading effects.

This pattern is now well established in climate science. The Intergovernmental Panel on Climate Change has warned that compound and cascading risks dominate climate outcomes, as physical hazards interact with economic, social and infrastructural vulnerabilities to produce systemic disruption rather than isolated damage.[9]

3 Egypt's Suez Canal blocked by huge container ship

4 Pakistan: Flood Damages and Economic Losses Over USD 30 billion and Reconstruction Needs Over USD 16 billion - New Assessment

5 An unprecedented crisis is leading Pakistani Textile & Apparel sector towards uncertainty

6 An unprecedented crisis is leading Pakistani Textile & Apparel sector towards uncertainty

7 Widespread Smoke from Canadian Fires - NASA Science

8 Canadian Wildfire Smoke and Asthma Syndrome Emergency Department Visits in New York City | Asthma | JAMA | JAMA Network

9 IPCC_AR6_SYR_SPM.pdf

Infrastructure was not built for this

Critical infrastructure is already showing signs of stress under this new operating environment. In November 2025, a cooling system failure at a CME Group data center triggered a multi-hour shutdown of derivatives trading worldwide, affecting equities, commodities, foreign exchange rates and futures markets simultaneously.[10] The incident was not caused by a storm or flood, but it exposed a vulnerability that becomes more likely in a warming world. Data centers, power grids, ports, telecommunications networks and logistics hubs were engineered for historical climate conditions. Many now operate outside those design assumptions.

Energy and infrastructure authorities have warned that extreme heat, drought, storms and flooding increasingly threaten cooling systems, power availability and system reliability across regions and income levels.[11] The risk is not simply physical damage; it is also interruption, with impacts propagating rapidly through financial markets, supply chains and digital systems.

The new reality, and the state of the science, is this: critical infrastructure is now vulnerable to failure modes for which organizations have not prepared. Scientific bodies including the IPCC, WMO, UNDRR and Chatham House warn of increasingly cascading climate risks, where multiple hazards compound into systemic failure. Peer-reviewed scientific analysis describes climate-driven "compound and cascading risks" as a dominant global threat.[12]

In practice, scenarios may look like:

1. Extreme heat creates grid stress, leading to potential data center failures and market disruption.
2. A storm surge causes flooding at cable landings, resulting in cable outages and degradation of global internet connectivity.
3. Wildfire smoke leads to airport shutdowns, impacting logistics and shipping providers and causing supply chain paralysis.
4. A drought causes river levels to collapse, straining energy production and shipping operations and triggering commodity shocks.
5. Flooding contaminates drinking water, creating unsafe conditions and impacting entire communities and public health.

10 Cooling crisis at CME: A wakeup call for modern infrastructure governance | Network World

11 Climate Resilience for Energy Security

12 Ten new insights in climate science 2024 - ScienceDirect

The second half of the risk equation

There is another dimension of climate risk that many organizations still underestimate. Climate risk is not only about how physical events impact companies. It is also about how markets, regulators, communities and other stakeholders respond to how companies prepare for, operate within and contribute to a changing climate. Investor scrutiny now activates within hours of climate-related disruption. Markets increasingly reprice expectations based on confidence in governance, preparedness and response capability – often before the full facts are established.

More than 90 percent of global institutional investors now integrate climate risk into investment, engagement or voting decisions, making climate exposure directly relevant to capital access and cost across markets.[13] At the same time, organizations face increasing scrutiny related to their environmental footprint. Public representations, operational choices and capital allocation decisions are assessed against real-world outcomes. Governance bodies increasingly treat climate preparedness as a matter of fiduciary oversight rather than reputational preference.[14] This dynamic is why climate risk has become a leadership test.

Managing physical exposure without preparing for market and societal response is insufficient. Focusing on disclosure or narrative without operational resilience is equally incomplete. In practice, these dimensions now converge, often under intense time pressure and public visibility.

Why traditional risk frameworks fall short

Many organizations continue to approach climate risk primarily as a modeling exercise or reporting obligation, and that approach lags reality. Traditional risk frameworks assume linearity, independence and recoverability. Climate risk increasingly violates all three assumptions because impacts are non-linear, risks converge across domains and recovery often introduces new vulnerabilities rather than restoring prior conditions.

In the United States alone, dozens of weather and climate disasters exceeded one billion dollars in losses in 2024, reinforcing that climate risk is already material to enterprise value.[15]

The most exposed organizations are not necessarily those in the most climate-sensitive geographies. They are those with concentrated infrastructure, single points of failure, fragile supply chains, slow escalation pathways and governance structures not designed for compounding risk.

A leadership imperative for business

The question facing leaders is no longer whether climate risk matters. It is whether their organizations are structured to operate through it. Organizations that continue to treat climate as a long-term sustainability issue or a compliance exercise are more likely to find themselves reacting under pressure, in public and at uncomfortable speed. Those who recognize climate risk as a systemic business condition, connect physical events with market and societal responses and treat it through a holistic lens are better positioned to protect continuity, credibility and value. Climate risk is present, global and compounding in severity and disruption. It is also reshaping the environment in which organizations operate. The remaining choice is between deliberate preparation and forced adaptation.

Courtney Adante
President
Security Risk Advisory
courtney.adante@teneo.com

13 Survey | 2024 Institutional Investor Survey on Sustainability

14 G20/OECD Principles of Corporate Governance 2023 (EN)

15 U.S. Billion-dollar Weather and Climate Disasters, 1980 - present (NCEI Accession 0209268)

Protecting Family, Assets and Reputation: Unique Risks for Ultra High Net Worth Individuals

As 2026 begins, the range of threats confronting Ultra High Net Worth Individuals (UHNWI) is broad and expanding, with bad actors increasingly seeking to leverage information for personal, financial or reputational gain.

Factors such as increased visibility, public exposure and perceived wealth can make UHNWI targets for various risks, including financial crimes, privacy breaches, personal safety concerns and reputational damage. Criminals and malicious actors may specifically target them based on perceived wealth, underscoring the importance of identifying potential vulnerabilities or other points of leverage that a bad actor may attempt to exploit.

Adopting a risk-based approach to threat management can help UHNWI, their families and family offices identify, mitigate and respond to this range of potential threats, protecting both the individual and affiliated institutions.

UHNWI face unique reputation-based concerns

Reputational concerns are a significant challenge for UHNWI given their prominent social status and visibility. The potential harm of persistent reputation-based risks extends beyond the targeted individual to include their family and business relationships, ultimately posing cross-cutting impacts across personal, professional and social fronts. As societal tensions around affordability and economic conditions persist in 2026, UHNWI are likely to face intensified scrutiny that can accelerate the compounding impact of reputational concerns.

Further, the current domestic political environment and public reactions to UHNWI's political actions introduce additional risks, necessitating a proactive and individualized assessment of potential security threats and associated mitigation efforts. For example, in July 2025, protestors gathered at OpenAI CEO Sam Altman's San Francisco residence to oppose his support for specific political figures and policies.[16] Similarly, in August 2025, activists from the Gulf South targeted the home of Citigroup CEO Jane Fraser to protest the financing of methane gas projects.[17]

These examples highlight several ways in which UHNWI face an amplified risk environment. Media and public attention around wealth, political actions, lifestyle and philanthropic activity can quickly shift from neutral to negative, increasing exposure to controversies that shape perception and invite sustained scrutiny. Associations with contentious topics, whether real or perceived, can become reputational flashpoints, especially when tied to politically sensitive issues, polarizing industries or values-based debates. Social media and online presence can also collapse the distance between private and public life, creating a wide surface area for misinterpretation, amplification and targeting, often with direct implications for UHNWI privacy and personal safety.

From homes to family members, physical protection remains critical

Beyond reputational concerns, UHNWI are often at increased risk of physical confrontations, intimidation and targeting due to their prominence, business and political relationships, wealth and the valuable assets they possess. Similarly, residences and properties may be targeted for physical intimidation or coercion of the individual themselves.

Physical risks often concentrate around four factors. First, the wealth and perceived value of assets can make UHNWI attractive targets for criminal activity, with criminals seeking a wide range of items including artwork, jewelry, high-end technology, expensive vehicles or documents and data that can be exploited for financial gain or leverage. Second, public knowledge and media exposure related to an UHNWI's presence can inadvertently provide useful information about residences, travel plans and personal routines. In the digital age, malicious actors may compile publicly available information to support detailed pre-planning, enabling theft with a high degree of accuracy.

As an extension of pre-planning, and beyond theft or reputation-based concerns, activism centering on UHNWI's residences introduces physical security concerns related to property access. In August 2025, protestors responding to the Israel-Hamas conflict

16 Protesters rally outside of OpenAI CEO Sam Altman's San Francisco home for praising President Donald Trump, 'Big Beautiful Bill' - ABC7 San Francisco

17 A Week of Gulf South Solidarity in New York City - Inside Climate News

targeted senior Microsoft executives Satya Nadella's and Brad Smith's homes via the residences' borders with public waterways. These demonstrations highlight concerns related to activists' access to UHNWI's property for activism and messaging purposes, with Microsoft seeking FBI assistance following the protests.[18]

Further, an increase in swatting incidents, when an individual makes a false report to emergency services with the goal of triggering a large police response to a specific address, over the past two years spotlights the growing risk of malicious actors physically harassing, intimidating or injuring UHNWI at their homes.[19]

Third, security gaps at residences create openings for criminals to successfully execute their plans. Weak access controls, lack of robust surveillance coverage and limited resourcing for security personnel can all increase the risk of unauthorized entry and theft. Finally, insider access presents a unique concern for UHNWI. With personal and domestic staff often running critical household functions, the risk of both intentional exploitation and inadvertent information disclosure necessitates proactive oversight of household operations.

Cybersecurity as a cross-functional priority

Beyond physical risks, UHNWI also face significant cybersecurity-related concerns, including fraud, extortion, doxing and account takeover, due to their high-profile status and the valuable assets they possess.

The most common attack path begins with phishing and social engineering, where malicious actors impersonate trusted contacts, service providers or institutions to obtain credentials or sensitive information. From there, account compromise can cascade across email, social media and financial platforms, leading to identity theft, financial loss and reputational harm. The growing prevalence of deepfakes heading into 2026 further increases the credibility of scams and fraudulent requests.

Malware and ransomware also remain persistent risks, particularly when personal devices or home networks lack enterprise-grade protections. Insider threats, including employees, advisors or even family members, can create exposure through either malicious intent or accidental mishandling of sensitive digital information.

Another notable risk centers on efforts to dox UHNWI. In April 2025, cybersecurity firms identified a database of over 1,000 business executives' personally identifiable information, highlighting the risk of malicious actors attempting to leverage UHNWI's sensitive data for financial, political or physical targeting.[20]

Travel as a risk multiplier

Travel poses a distinct risk to UHNWI, as mobility increases visibility, predictability and reliance on unfamiliar environments. When traveling, UHNWI may become targets for threats ranging from theft and harassment to kidnapping and politically motivated violence.

Three dynamics are particularly important. First, personal security and safety risks can escalate quickly when on the move, from low-level harassment to robbery or kidnapping, especially when itineraries are publicly visible or routines become predictable. Second, privacy and information security risks increase through use of public Wi-Fi, device charging stations and hotel or venue networks, all of which can be exploited to access accounts or personal data. Third, frequent travel to global destinations elevates UHNWI's risk of encountering terrorism and political unrest, leading to potential indirect exposure even when the individual is not the intended target. Demonstrations, instability or localized violence can all disrupt movement and introduce sudden security threats.

Converged risk requires integrated protection

In 2026, the dominating reality for UHNWI is that risk is increasingly converging across the above themes. Reputational concerns, physical security, digital exposure and travel vulnerabilities all reinforce one another and can escalate quickly. The most secure approach must be both integrated and proactive: reduce unnecessary exposure, strengthen physical and cyber controls, promote effective staff management and maintain clear protocols for travel, so that security is not a set of siloed measures but a coordinated operating model.

Brendan Johannsen
Chief Operating Officer and Head of Client Delivery
brendan.johannsen@teneo.com

18 Microsoft Asked FBI for Help With Israel-Gaza Protests - Bloomberg

19 The Escalating Threats of Doxxing and Swatting: An Analysis of Recent Developments and Legal Responses - National Association of Attorneys General

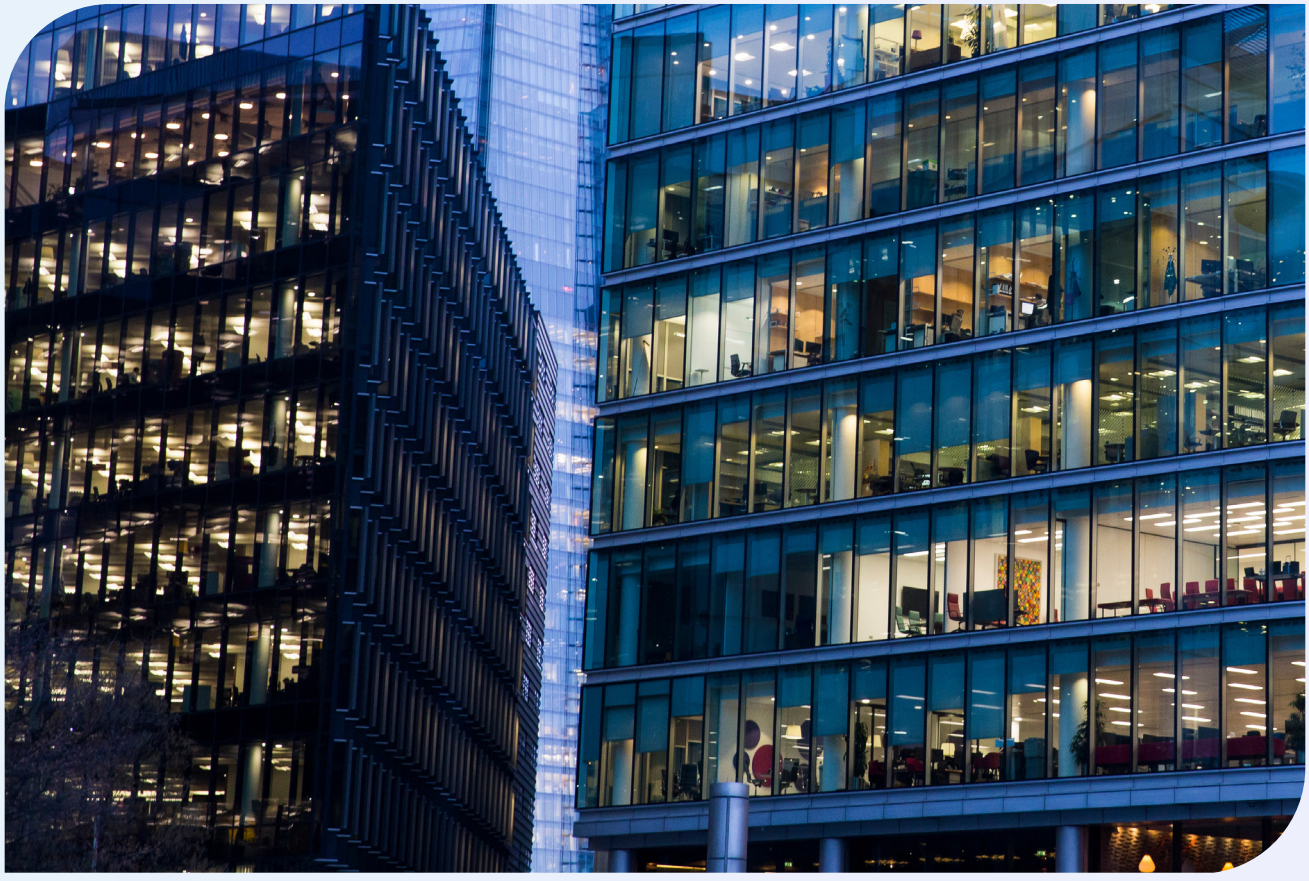
20 The CEO Database Exposes Information on Over 1,000 Executives | Flashpoint

From Insight to Action: How Teneo's Risk Advisory Business Approaches Resilience and Risk Management in 2026

As leaders confront persistent disruption and compounding risks, Teneo Risk poses three key steps to guide actions in 2026:

1. Establish verifiable readiness: Define central risks and develop corresponding inspection, testing, scenario planning and response capabilities that are measurable and iterative.
2. Build an integrated operating model for decision-making under ambiguity: Sync intelligence, physical security, cybersecurity, legal and administrative functions into a unified cadence that can adapt to dynamic conditions, including a changing climate. Leverage exercises to operate under shifting parameters by proactively identifying vulnerabilities, internal and external stakeholders and a coordinated response to emerging risks.
3. Govern artificial intelligence adoption and data management enterprise-wide: Create a single roadmap for AI implementation, with defined adoption thresholds, verification procedures and auditable controls.

Together, these steps are designed to move organizations from decision paralysis to the ability to operate through continual risk. In 2026, disruption will rarely arrive with complete information, clear timelines or neatly packaged impacts. Organizations must have integrated and proactive frameworks in place ahead of the next major disruption to effectively manage these challenges. The organizations that outperform will be those that treat readiness and risk management as a core operating discipline so they can protect people, operations and reputation while sustaining advantage when pressure is greatest.



Teneo®

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 and ESG.

The firm has more than 1,800 employees located in 45+ offices around the world.

teneo.com