2026

Global risk & resilience outlook

Future-ready strategies for the expanding risk zone

everbridge™

Table of contents

Foreword

When I talk with leaders around the world, one theme keeps coming up: the nature of risk is changing. Disruptions are more frequent, move more quickly, and are more connected than ever before. For example, impacts from a cyber incident can ripple through supply chains, operations, and employee safety in minutes. Risks don't wait their turn, and they collide - creating an expanding risk zone which is redefining organizational resilience.

That's why the ***2026 Global risk & resilience outlook*** is so timely. It helps leaders see how these converging risks are reshaping business continuity, and offers practical ways to stay ahead of them. The focus of this report is future-readiness: helping our customers build the systems, culture, and confidence they need to respond faster and recover stronger.

Resilience today isn't a static plan. It's an organizational mindset that connects people, data, and action across the enterprise. The strongest organizations are embracing that shift by using purpose-built AI, automation, and decision-ready intelligence to move from reaction to anticipation. That's the foundation of **High Velocity Critical Event Management**: helping organizations know earlier, respond faster, and improve continuously.

The goal is not just to survive disruption, but to thrive through it. Use this report to challenge assumptions, start new conversations, and accelerate your own path toward true resilience in 2026 and beyond.

Dave Wagner
President & Chief Executive Officer, Everbridge

Executive summary

The global risk landscape of 2026 is marked by increasing complexity and deeply interconnected threats spanning industries and regions. This reality requires a strategic evolution from traditional business continuity to comprehensive organizational resilience. Organizations face mounting challenges that require adaptability and swift, decisive responses to a constantly evolving threat environment. In this context, resilience is no longer a compliance requirement - it is an integrated, strategic asset essential for sustained operations and competitive advantage.

Today's global threats often emerge across systemic risk clusters, impacting social, operational, and financial domains. This interconnectedness creates new vulnerabilities, requiring organizations to rethink traditional approaches to risk management and build true future-readiness. Gartner underscores this urgency, projecting that by 2027, 60% of organizations will not fully adopt organizational resilience principles, leaving them vulnerable to global technology threats.

As business operations grow more complex, organizations are exposed to significantly higher levels of risk. We call this the "expanding risk zone," where the frequency and intensity of critical events reshape boardroom priorities and challenge continuity. Enterprises must now prepare to address risks that are simultaneous and interconnected, requiring a shift from reactive incident response to proactive, high-velocity critical event management.

Findings from the **Everbridge Global Risk Survey**, conducted in October 2025, expose significant vulnerabilities in organizational resilience. Alarmingly, half of all respondents report lacking a formal critical event management strategy, and almost a quarter confess they never test their continuity plans. Identified weaknesses further include insufficient employee training, limited technology investment, and a notable lack of confidence in crisis communication channels. With cybersecurity now ranked as the foremost threat, these insights unequivocally highlight the critical imperative for organizations to adopt proactive, technology-driven strategies to effectively prepare for and manage today's complex risk landscape.

This report identifies 10 critical global risks for 2026 and provides a strategic framework to enhance organizational resilience and safeguard operational continuity, underscoring the vital roles of advanced risk management and strategic investments in building a future-ready enterprise.

Implications for business continuity and resilience

The following section details 10 of the top risks anticipated for 2026, analyzing their direct impact on an organization's ability to maintain operational resilience and ensure business continuity.

01

Cyberattacks and systemic cyber risk

As organizations accelerate digital transformation and expand their dependence on connected technologies, the global cybersecurity landscape has reached a pivotal point - one marked by increasing sophistication, frequency, and severity of threats targeting the backbone of business operations. Over the past decade, cyber risk has grown exponentially, fueled by the proliferation of IT systems, third-party vendors, and distributed workforces. This expanding risk zone brings greater vulnerability not only to core systems, but also to critical supply chains and operational technology.

Modern cyberattacks are multifaceted: organizations now face ransomware proliferating through global networks, AI-driven malware adapting in real time, and deepfake-enabled social engineering targeting executives. Attackers exploit vulnerabilities within interconnected supply chains, shared digital platforms, and cloud ecosystems, creating concentrated risks that can paralyze entire industries. State-sponsored actors and organized criminal groups increasingly focus on sectors deemed vital to economic and national security - notably energy, transportation, healthcare, and finance - leveraging advanced zero-day exploits, phishing campaigns, and persistent threats.

The financial and operational consequences extend far beyond traditional data loss. For example, a single high-impact cyber incident can halt digital services for months, disrupt critical deliveries, and have cascading effects downstream, affecting customer trust, revenue streams, and regulatory compliance.

Against this backdrop, organizations must adapt by modernizing security controls, boosting monitoring and cyber hygiene, and integrating cyber resilience into foundational risk management and continuity planning. Success depends on establishing a culture of preparedness, ensuring continuity of operations during attacks, and accelerating recovery amid escalating threat complexity.

A 2025 Everbridge survey of global business leaders revealed that cybersecurity is the most significant threat for 53% of organizations.

What's happening

Cyber threats are evolving rapidly in frequency and complexity. Attackers are targeting suppliers and shared digital platforms, creating concentrated risk across entire systems and challenging traditional security perimeters.

Business impact

A successful attack can lead to significant operational downtime, revenue loss, and severe legal exposure, directly impacting recovery time objectives (RTOs). When operational technology (OT) is compromised, safety concerns escalate, and recovery can take months, severely testing an organization's resilience. The average cost of a data breach has climbed to $4.44 million, but this figure does not capture the full extent of operational disruptions and long-term reputational damage.

Signals to watch

To maintain operational resilience, monitor for a surge in credential-stuffing and multi-factor authentication (MFA) fatigue attacks. Also critical are unusual activities within OT networks, security incidents impacting critical suppliers, and deepfakes targeting senior executives.

Strategic actions for future-readiness

Adopt proactive measures to safeguard business continuity. Implement 24/7 monitoring and active threat hunting. Strengthen identity security with robust MFA and least-privilege access policies. Isolate OT networks and conduct regular drills for ransomware and deepfake scenarios. Finally, mandate security attestations from all critical suppliers and prepare crisis communication templates to ensure a rapid, coordinated response.

Future-proof your cyber resilience

Download our "Cyber resilience 2026 and beyond" whitepaper now to stay ahead of tomorrow's cyber threats.

Access here

02

The dual edge of AI

Artificial intelligence is one of the most transformative forces shaping both risk and resilience in today's enterprise landscape. Its advances have unlocked unprecedented opportunities for innovation, productivity, and predictive insight - providing organizations with sophisticated tools for anticipating, detecting, and managing critical events. AI-powered platforms can accelerate decision-making, enhance crisis communications, and drive operational efficiency through automation.

Yet this same technology significantly amplifies the risk landscape. Malicious actors have weaponized AI to automate reconnaissance, rapidly scale sophisticated attacks, create highly convincing phishing schemes, and power the emergent model of Ransomware-as-a-Service (RaaS). Increasingly, AI-generated deepfakes are being deployed to deceive employees or bypass executive controls, and the volume and complexity of machine-driven threats are outpacing the ability of many organizations to respond with conventional controls.

The inherent paradox is that organizations are quickly adopting AI-powered capabilities to strengthen operational resilience, while simultaneously struggling to keep pace with the risks - ranging from data leakage and model drift to unexplainable or biased AI-driven outcomes and regulatory scrutiny. The accelerated adoption of generative AI, often ahead of robust governance frameworks, further compounds exposure to compliance breaches and reputational harm.

Organizations must recognize that the dual edge of AI demands a future-ready approach: proactively harnessing AI for business continuity and resilience, while continuously investing in oversight, risk management, and response mechanisms that address AI's evolving threat profile.

> "AI-driven threats are evolving. Leaders must prepare for deepfakes and automated attacks, while keeping humans in the loop for critical decisions."
>
> Pamela Larson, Chief Security Officer, North America, Everbridge

What's happening

AI is simultaneously intensifying cyber threats and enhancing defenses. Attackers use AI for automated reconnaissance and sophisticated malware, while organizations often adopt AI faster than they can establish strong governance and control frameworks to ensure its responsible use.

Business impact

Incident frequency and severity are increasing, directly challenging business continuity. Uncontrolled generative AI use can lead to data leaks, biased outcomes, and compliance breaches, undermining an organization's resilience posture. Deloitte projects that generative AI could inflate fraud losses in the U.S. to $40 billion by 2027.

Signals to watch

For proactive risk management, look for unusual automation patterns in access and network logs. Monitor for reports of generative AI abuse and model drift. Be alert to third-party model changes that alter behavior, and review evolving regulatory standards for AI in critical functions.

Strategic actions for future-readiness

Implement a robust AI governance framework with clear risk appetites. Inventory and classify all AI models and use cases, performing red-teaming and model validation pre-production. Mandate human-in-the-loop for critical decisions to ensure oversight. Conduct executive deepfake drills, especially those linked to payment and public relations workflows, to prepare for sophisticated social engineering attacks.

> Discover how purpose-built AI enhances crisis management with faster decisions, improved resilience, and predictive insights.
>
> Download your free whitepaper: "The four pillars of AI in managing high-stakes critical events"

03

Natural disasters and climate-driven extremes

The growing frequency and intensity of extreme weather events - ranging from hurricanes and wildfires to heatwaves, droughts, and floods - now represents a formidable challenge to operational and organizational resilience. Organizations worldwide face direct disruptions, but also profound indirect impacts that cascade through supply networks and regional economies. Recent data underscores the urgency: the UNDRR's Global Assessment Report indicates that insurance payouts related to natural disasters now average 1.9% of the world's annual GDP, and what used to be "once in a century" floods are occurring far more often, putting unprecedented strain on infrastructure and emergency response systems. In the past year alone, 69% of incidents tracked by the Everbridge Risk Intelligence Monitoring Center were climate-related - including wildfires, extreme heat, earthquakes, floods, tornadoes, and hurricanes. Real-world examples, such as the $131 billion in estimated losses from a single Los Angeles wildfire and the record-setting wildfire seasons across the EU, further demonstrate how climate-driven disasters are increasing in magnitude and frequency.

> "Climate change is no longer a distant threat - it's here, reshaping risk for every organization. We are honored to work with the UN Office for Disaster Risk Reduction at such a pivotal moment of ongoing climate challenges. Helping to build resilient communities and organizations is core to our mission."
>
> Dave Wagner, President & CEO, Everbridge

What's happening

Extreme weather is no longer sporadic or isolated - its effects are now persistent and systemic. Such events increasingly disrupt transportation, logistics, and utility networks, and their secondary consequences, such as poor air quality, water scarcity, and grid instability, further challenge an organization's ability to protect people, physical assets, and supply chain continuity. As rebuilding timelines lengthen and insurance coverage becomes more selective, the chronic risk of interruption is rising.

Business impact

Companies are experiencing more frequent facility outages, production halts, and workforce displacement due to these hazards. Insurance premiums are rising, coverage terms are becoming more restrictive, and operational recovery can be delayed by shifting environmental baselines. The financial and operational impact extends well beyond immediate damages, eroding profitability and stretching the limits of current resilience strategies.

Signals to watch

To ensure future-readiness, organizations should closely monitor seasonal forecasts across all regions of operation, pay attention to wildfire smoke indexes, drought and grid-stress alerts, and regularly review updated flood and hazard maps. Early recognition of local emergency declarations and shifting insurance industry guidance is critical for timely planning and adaptation.

Strategic actions for future-readiness

Strengthen facilities and create defensible perimeters around critical assets. Secure backup power and water, testing logistics for maintaining supplies. Develop asset-aware evacuation plans and flexible work-from-anywhere policies to ensure employee safety and business continuity. Diversify key suppliers geographically and review insurance coverage to enhance financial resilience.

> Architecture, engineering and construction firm, Burns & McDonnell, uses Everbridge to navigate critical events by providing impact zone visibility, enabling efficient communication, and ensuring safety during weather-related emergencies.
>
> Watch the customer video here to find out how

04

Geopolitical conflict

Geopolitical instability and the weaponization of economic policies - such as tariffs on critical minerals, export restrictions, strategic subsidies, and the widening use of sanctions - are among the most pressing risks organizations must manage. These developments do not occur in isolation; modern geopolitical risk results from a complex interplay of geoeconomic rivalries, trade disruptions, sociopolitical unrest, and the strategic use of digital infrastructure. Together, these intertwined threats accelerate volatility and threaten core aspects of operational resilience.

The cascading effects of geopolitical conflict can directly disrupt trade flows, create choke points at critical shipping lanes, and introduce sudden and severe volatility in global commodities and energy markets. When a major conflict arises or trade policy shifts, essential inputs may become inaccessible or heavily delayed, while currency fluctuations and shifting insurance markets drive up costs and complicate financial planning. Regional conflicts can force rerouting of goods, expose companies to new compliance or sanction requirements, and leave organizations with stranded inventory or production outages. In some cases, regulatory fragmentation triggered by geopolitics can create additional barriers to market entry or force organizations to overhaul established supply chains in response to shifting export controls or growing regionalization.

The impact is acutely felt in supply chain resilience. Organizations relying on single-region sourcing or just-in-time inventory models find themselves especially vulnerable when geopolitical risk materializes: access to suppliers can be abruptly cut off, and alternative sources may be scarce or costly. This highlights the urgent need for a holistic risk intelligence approach that recognizes how quickly localized geopolitical events can escalate into global operational disruptions.

Discover how organizations effectively navigate geopolitical instability. Through proactive risk monitoring, strategic planning, and resilience-building, leaders are empowered to mitigate disruptions, protect assets, and maintain operational continuity.

Watch the on-demand webinar: Navigating global risk and geopolitical instability

What's happening

A combination of tariffs, export controls, and sanctions is reshaping global trade. Simultaneously, regional conflicts are disrupting vital shipping lanes and international insurance markets, creating unpredictable challenges for business continuity.

Business impact

Businesses face persistent volatility in transit times and freight costs, while market access can shrink rapidly. Supplier stability is increasingly precarious, and evolving regulations amplify compliance burdens, making proactive supply chain management essential for resilience.

Signals to watch

To maintain operational awareness, monitor maritime security advisories, canal throughput metrics, and updates to international sanction lists. Track fluctuations in commodity prices, freight costs, and war-risk insurance premiums.

Strategic actions for future-readiness

Integrate geopolitical intelligence into strategic planning and sourcing decisions to build a more resilient supply chain. Establish pre-approved rerouting and mode-switching protocols. Cultivate a diversified, multi-regional supplier base and evaluate near-shoring opportunities to mitigate concentration risk.

Building organizational resilience in times of geopolitical instability

Delve deeper into the evolving geopolitical landscape and its security implications. Learn how to anticipate risks, adapt swiftly, and emerge stronger.

Access the whitepaper now

05

Business interruption from supply-chain shocks

Supply chain disruptions have become some of the most profound and pervasive threats to organizational stability and resilience. Far from being isolated challenges, these are systemic shocks that can undermine business continuity across entire industries and geographies. In today's global landscape, supply chains are highly complex and interconnected, meaning that a single disruption can rapidly propagate, halting production, disrupting sales channels, and creating costly delays at scale.

Such disruptions can originate from various sources: port congestion, labor shortages, transportation bottlenecks, and the unavailability of critical raw materials can all quickly destabilize even the most robust supply chain networks. The ripple effects extend beyond physical goods - digital supply chain vulnerabilities are now a critical concern. Many organizations depend heavily on third-party IT providers for core operations, making digital outages or cyber incidents a point of systemic risk. A disruption at a single provider can trigger a "digital domino effect," rapidly spreading operational chaos and affecting business continuity for multiple enterprises simultaneously.

These shocks have severe operational and financial implications. Production may hit standstill, lead times increase, contractual obligations are missed, and both cash flow and long-term customer trust can be seriously damaged. The cascading impact is especially acute in industries reliant on just-in-time inventory and lean operational models, amplifying the exposure of organizations to events well beyond their immediate control.

> "It's critical to have a clear picture of your entire supply chain... where raw materials originate, the locations and distributors they pass through, and where finished goods will travel."
>
> Tracy Reinhold, Global Chief Security Officer, Everbridge

What's happening

Disruptions at physical hubs (such as ports and logistics centers), as well as digital infrastructure providers, are accelerating. Heavy reliance on a small number of suppliers or digital partners creates critical single points of failure, leaving organizations vulnerable to systemic disruptions and prolonged downtime.

Business impact

Disruptions can halt production, cause companies to miss service-level agreements, trigger significant revenue loss, and test the organization's ability to recover effectively and efficiently. The growing prevalence of digital vulnerabilities further raises the risk, as outages with third-party IT providers may compromise large portions of the supply chain.

Signals to watch

For proactive supply chain resilience, monitor rising lead times, allocation notices for critical components, changes in global logistics routes due to geopolitical events, and reports of outages from digital service providers. Keeping a close eye on the financial and operational health of critical suppliers is also essential.

Strategic actions for future-readiness

Adopt dual- or multi-sourcing for critical supplies to build redundancy. Build buffer inventories for essential products. Pre-negotiate alternative logistics routes and modes to minimize downtime and ensure operational continuity during disruptions.

06

Misinformation and disinformation

The proliferation of misinformation and disinformation represents one of the most rapidly accelerating and significant risks to organizational resilience in 2026. False narratives, deepfake content, and manipulation of information ecosystems are increasingly leveraged to attack both private and public sector entities. These threats extend far beyond reputational damage - misleading or maliciously crafted content can disrupt crisis communication, impede effective crisis management, and lead to tangible operational incidents. Such disruptions in the information landscape directly erode internal alignment, undermine leadership credibility, and create confusion across stakeholder groups - whether employees, partners, customers, or the broader public.

Accelerated by advances in AI-powered tools that make creating convincing misinformation easier and cheaper, the volume and impact of fabricated stories and manipulated media continue to grow. Targeted campaigns can drive customer defection, disrupt supply chains, and prompt regulatory scrutiny. The collapse of trust, especially during critical events, can slow organizational response, fuel internal conflict, and damage long-term relationships with both customers and partners.

The World Economic Forum's Global Risks Report recently identified "misinformation and disinformation" as the most severe global risk over the next two years, reflecting its power to undermine decision-making and destabilize markets on a global scale. Operationally, organizations have experienced first-hand the consequences of such attacks. For example, the recent deepfake livestream impersonating Nvidia's CEO reached over 100,000 viewers before it was stopped - highlighting the speed at which these risks can escalate, and their potential to inflict significant brand and financial losses.

> "Transparency builds resilience. Trusted organizations earn stronger customer loyalty, higher employee engagement, and more robust investor confidence even in volatile markets."
>
> Jeremy Capell, Chief Trust Officer, Everbridge

What's happening

False narratives and deepfakes rapidly erode trust. Adversaries increasingly target brands and executives to disrupt crisis response and manipulate markets, making authenticated communication a cornerstone of resilience.

Business impact

Investor and customer confusion rises, fraud losses escalate, and decision-making slows. This poses a critical threat to brand trust and operational stability.

Signals to watch

Monitor for executive impersonation, payment redirect attempts, and viral brand-related rumors. Track unusual spikes in inbound communications and identify coordinated narrative campaigns that could signal a targeted attack.

Strategic actions for future-readiness

Authenticate all executive communications through established, secure channels. Establish a rapid-response communications cell to manage information flow during a crisis. Train employees to recognize deepfakes and bots. Integrate media and social monitoring into incident response playbooks to ensure a swift, coordinated response.

> Explore the strategic power of openness and accountability to create stronger teams, build customer loyalty, and achieve sustainable success.
>
> Read the Everbridge blog post "Trust in a complex world: Why transparency is the key to resilience"

07

Regulatory fragmentation, tariffs and trade restrictions

The accelerating pace of regulatory change is dramatically reshaping the global risk landscape. Organizations today must contend with a rapidly evolving and increasingly fragmented patchwork of regulations, tariffs, and trade restrictions that create substantial operational uncertainty and elevate compliance risk to a board-level concern. Unlike previous eras where compliance was largely static and predictable, today's environment is characterized by diverging frameworks across jurisdictions - most notably on issues related to supply chain due diligence, operational resilience, cybersecurity, data privacy, and environmental standards.

Sanctions regimes, export controls, and localization mandates are updated with little notice, forcing continual adaptation and elevating the risk of inadvertent non-compliance. For complex, multinational enterprises, this regulatory volatility can disrupt cross-border operations, cause costly shipment delays, and constrict data flows essential for business intelligence and digital service delivery. Escalating compliance costs and resource requirements - especially in procurement, legal, and risk teams - are now the norm. Moreover, organizations face a rising likelihood of regulatory audits, enforcement actions, and reputational harm if their compliance capabilities cannot keep pace with emerging requirements.

The operational significance is profound: insufficient agility in this regulatory climate can jeopardize market access, trigger supply chain bottlenecks, and impair the ability to meet key contractual obligations - all of which undermine organizational resilience. The organizations best positioned to thrive will be those that synthesize compliance, trade, procurement, and risk management into a unified operational view, ensuring they can anticipate and respond to regulatory shifts before they escalate into business continuity threats.

> "To navigate the complexities of the compliance risk environment, focus on coordinating across risk management functions and efforts. Make building key capabilities a priority, and you'll be well on your way to enabling faster, more informed decision-making and improved risk management."
>
> Gartner

What's happening

Regulatory frameworks are rapidly diverging across regions, particularly concerning due diligence, operational resilience, and cybersecurity. Sanctions and export controls are subject to frequent changes, making compliance a moving target.

Business impact

This environment leads to escalating compliance costs and increased friction within supply chains. Data flows face constraints, and organizations experience a heightened risk of audits and enforcement actions, which can disrupt operations.

Signals to watch

To ensure future-readiness, regularly track new regulations in key regions and closely follow regulatory guidance. Stay informed through alerts from relevant industry associations.

Strategic actions for future-readiness

Establish a unified operational view that integrates Compliance, Trade, Procurement, and Risk functions. Maintain a proactive calendar of anticipated regulatory changes with clear accountability. Conduct scenario planning to address potential material shortages and data residency restrictions. Standardize supplier documentation to efficiently address evolving due diligence requirements and maintain business continuity.

> Regulatory demands are growing more complex and interconnected. Resilience isn't about checking a box; it's about building the muscle to adapt as rules change."
>
> **Dave Wagner, President & CEO, Everbridge**

Read the full blog post here: Embracing regulatory resilience

08

Macroeconomic and financial instability

Macroeconomic and financial instability is now a primary concern for organizations seeking to maintain business continuity and operational resilience. The global business environment is increasingly volatile, shaped by persistent inflation, fluctuating interest and exchange rates, and rapid shifts in fiscal and trade policy. These factors are no longer background variables, but central risks that directly affect working capital, credit access, procurement cycles, and revenue streams.

Organizations are under mounting pressure as inflation erodes real demand and compresses margins, while interest rate changes quickly increase the cost and uncertainty of financing. Policy shifts - such as new tariffs or subsidy programs - can disrupt trade flows and create unpredictability in cross-border operations. Compounding these headwinds are tightening liquidity conditions, heightened exposure to supplier defaults, fluctuating consumer demand, and compressed project timelines across the supply chain.

In this risk environment, even financially sound organizations may experience sudden cash flow pressure, increased costs, and simultaneous shocks to both supply and demand. Recent years have seen prominent firms revise profit guidance and project plans in response to adverse currency movements and trade restrictions, underscoring the pervasive impact of macroeconomic volatility on business strategy and long-term resilience.

> “Downtime is costlier than ever. A Gartner report found that the average cost of IT downtime is $5,600 per minute. For industries like e-commerce, financial services, and SaaS, these numbers skyrocket.”
>
> David Alexander, Chief Marketing Officer & GM of Digital Operations, Everbridge

What's happening

Inflation and volatile exchange rates are creating ripple effects across supplier networks, impacting everything from the cost of goods to project timelines.

Business impact

Organizations can expect tighter liquidity, potential supplier failures, and project delays. The risk of simultaneous supply and demand shocks is elevated, testing the financial resilience of the entire value chain.

Signals to watch

Monitor Purchasing Managers' Index (PMI) trends, credit spreads, and critical supplier default indicators. Track new tariff announcements, foreign-exchange triggers in contracts, and payment term extension requests from partners.

Strategic actions for future-readiness

Conduct cash-flow stress tests and plan for rapid cost reductions. Diversify financing and maintain liquidity buffers. Utilize dynamic pricing and hedge FX risks. Implement early-warning dashboards and incident response protocols to mitigate disruptions and protect your own business continuity.

Learn how to build a more resilient organization and ensure business continuity

Discover risk assessments, tech integration, and strategies to align continuity plans with business goals. Get your free eBook now: "8 steps to an effective business continuity plan".

Access here

09

Talent shortages and skills mismatch

Technological shifts, demographic changes, and economic transitions are creating a critical skills shortage. This isn't just about a lack of people; it's about missing key capabilities required to run core business processes. When crucial roles remain unfilled or staff lack necessary skills, single points of failure appear, incident response times increase, and valuable institutional knowledge disappears. This leads to longer mean time to recovery (MTTR), missed recovery objectives, and stalled modernization efforts, ultimately eroding business continuity and organizational resilience.

By 2030, about one in six people worldwide will be over 60, accelerating workforce aging. Simultaneously, skills mismatches are growing. The World Economic Forum notes that most executives see both workforce overcapacity and severe shortages in critical areas like AI. A separate study revealed that 44% of executives cite a lack of in-house expertise as a barrier to AI adoption. Closing this skills gap is no longer just an HR task - it's a core continuity strategy essential for strengthening organizational resilience.

To safeguard continuity, organizations must map skills to critical processes, capture knowledge in playbooks, implement automation, and cross-train staff to build surge capacity. A blended approach of hiring, reskilling, and using managed services can address immediate gaps. It's vital to treat talent availability as a critical operational risk indicator.

> "At Everbridge, we talk a lot about resilience being a shared responsibility. It doesn't sit with one department. HR plays a big part, because how you support your employees in tough moments reflects who you are as a company."
>
> Cara Antonacci, Chief People Officer, Everbridge

What's happening

Aging workforces and rapid technological change are creating significant skills gaps in resilience-critical roles like operational technology (OT) security, reliability engineering, and data management. Attrition and poorly designed handoffs in remote work environments are also eroding institutional knowledge.

Business impact

Recovery times are increasing, recovery objectives are being missed, and modernization initiatives are stalling. Rising overtime demands are heightening the risk of employee burnout.

Signals to watch

Monitor vacancy durations for critical roles and watch for spikes in overtime and on-call demands. Identify subject-matter experts who are single points of failure. Track training backlogs and expired certifications.

Strategic actions for future-readiness

Align skills with critical processes and assets to address gaps. Create and maintain runbooks and cross-train teams. Use a mix of hiring, reskilling, and managed services to build capacity. Regularly assess bench strength and succession plans. Conduct after-action reviews to update playbooks and refine training.

29% of organizations cite insufficient employee training and awareness as the biggest weakness in their critical event management strategy.

(Everbridge Global Risk Survey, 2025)

10

Polycrises: Overlapping risks, exponential impact

Polycrises occur when multiple risks materialize simultaneously and amplify each other's consequences, creating complex, interdependent disruptions that surpass the scope of any single incident. Unlike isolated events, polycrises build on the convergence of global threats, each compounding the impact of the others. This phenomenon is becoming more common as our world grows increasingly interconnected. The probability of concurrent, cross-sector disruptions is rising, driven by dependencies in global supply chains, shared digital platforms, and critical infrastructure networks that transcend borders.

The effects of polycrises are nonlinear and exponential. For example, an armed conflict may sever supply chains and trigger inflation, just as severe weather devastates key manufacturing hubs, and cyber threats target distributed workforces. This convergence strains operational capacity, overwhelms crisis management protocols, and creates "decision fatigue" across leadership teams. In such a scenario, siloed or sequential response tactics quickly become outdated, as organizations must simultaneously address multiple, fast-evolving challenges.

Recent years have illustrated how cascading risks can paralyze entire sectors, dramatically extend recovery timelines, and erode stakeholder trust even among well-prepared organizations. Leaders are now contending with extended incidents, protracted downtime, and mounting financial losses across business units - a direct threat to both organizational resilience and long-term viability.

The World Economic Forum's Global Risks Report emphasizes that 85% of experts identify concurrent risk events as a defining challenge for the decade ahead.

What's happening

Interconnected global risks are colliding more frequently. Think of conflicts that lead to supply shortages, which then fuel inflation. Shared digital platforms also increase the chance of incidents spreading across borders simultaneously.

Business impact

When multiple incidents strike at once, traditional manual coordination fails, slowing recovery. Decision fatigue and resource disputes delay a return to normal operations and can damage stakeholder trust, undermining organizational resilience.

Signals to watch

Keep an eye on multi-region alerts for weather, cyber threats, and logistics. Track concurrent infrastructure and supplier incidents. Monitor for escalating travel and safety warnings that could impact your distributed workforce.

Strategic actions for future-readiness

Establish a single, shared view for all incidents through a common operating picture. Activate a cross-functional command center with clear decision-making authority. Pre-define emergency teams and conduct regular joint exercises that simulate simultaneous, cross-border scenarios to test your organization's resilience.

Everbridge survey insights

Uncovering critical gaps in organizational resilience

Building future resilience begins with a clear understanding of an organization's current preparedness. Everbridge conducted a global online survey to assess how leaders approach critical event management and readiness. The Everbridge 2025 Global Risk Survey, completed in late 2025, provides key insights into business continuity and operational resilience.

Strategic gaps

Half of respondents (50%) reported limited or no formal critical event management strategies, addressing disruptions only as they occur. **Additionally, 24% of organizations never test their business continuity or critical event management plans**, placing them at heightened risk during unforeseen disruptions. Only 31% of global leaders expressed extreme confidence in their organization's ability to effectively manage critical events. Such a deficit suggests that many organizations are ill-equipped to navigate the complexities of an expanding risk zone, potentially leading to magnified impacts during unforeseen crises and undermining resilience.

Training and technology deficits

Insufficient employee training and awareness emerged as the top weakness (29%), while 26% cited limited investment in tools and technology. Notably, 61% reported no investment in advanced technologies like AI or predictive analytics, underscoring a significant readiness gap.

Communication and accountability

Only 37% were fully confident in their organization's communication channels during a crisis. Moreover, a lack of clear communication protocols (16%) and insufficient formal budget allocation (64% allocate less than 5% of annual budget or are unsure) point to persistent vulnerabilities.

Top threats

Cybersecurity remains the most significant threat for 53% of respondents, followed by economic downturns, natural disasters, workforce challenges, and geopolitical conflicts.

These findings highlight the imperative for organizations to move beyond compliance-driven approaches and embrace proactive, high-velocity strategies for business continuity. By addressing these gaps in training, technology, and planning, organizations can strengthen their future-readiness and position themselves to respond more effectively to complex, evolving risks.

A five-stage resilience strategy

Building a resilient, future-ready organization

To achieve future-readiness, resilience leaders need an integrated, proactive approach that helps them know earlier, respond faster, and improve continuously - so they can keep their people safe and their organizations running. This requires a shift from siloed business continuity and disaster recovery efforts to a holistic organizational resilience strategy powered by high-velocity critical event management (CEM).

01 Plan: Anticipate with dynamic risk intelligence

Move beyond static reports. Use scenario planning and asset-aware intelligence to quantify potential impacts and prioritize resources before threats escalate. This proactive posture is the foundation of future-readiness, enabling leaders to operationalize foresight and strengthen business continuity from the outset.

02 Monitor: Maintain 24/7 situational awareness

Protect continuity with always-on monitoring across your people, sites, supply chain, and technology. AI-powered risk intelligence and contextual data layers help you see disruptions sooner - from severe weather to geopolitical events - and understand who and what is at risk, enabling faster, more informed decisions.

03 Alert: Communicate with clarity and speed

When every minute counts, deliver targeted, multi-modal notifications and fulfill your duty of care with confidence. A high-velocity CEM approach accelerates detection, assessment, and outreach, so you can move from hours to minutes in your response while protecting employees wherever they work or travel.

04 Respond: Orchestrate a coordinated incident command

Replace fragmented point solutions with a common operating picture to mobilize the right people and actions across security, business continuity, IT, and operations. Centralizing decision-making and resource deployment through a platform like Everbridge High Velocity CEM™ ensures an efficient and effective response, minimizing the impact on operations.

05 Improve: Learn and adapt after every event

Institutionalize continuous improvement with post-incident analysis and performance insights. A full-lifecycle approach helps teams refine business continuity plans, update playbooks, and strengthen organizational resilience over time.

By adopting this five-stage strategy, **executives can move from reactive risk management to a proactive state of future-readiness, safeguarding people and assets** while sustaining operations in 2026 and beyond.

Conclusion

Securing future-ready organizational resilience

The evolving global risk landscape requires organizations to fundamentally rethink their approaches to business continuity and operational resilience. As detailed in this report, the threats facing organizations in 2026 are more complex, interconnected, and unpredictable than ever before. From cyberattacks and AI-driven disruption to climate extremes, regulatory volatility, and workforce challenges, each risk area brings unique and compounded implications for organizations striving to safeguard people, assets, and business value.

A central theme has emerged: resilience is not static, but an ongoing capability - one that integrates advanced risk management, investment in talent, continuous learning, and the adoption of high-velocity critical event management. The importance of embedding future-readiness into every facet of operations will only increase as risks multiply and converge, blurring the lines between isolated incidents and systemic threats. It is this proactive, data-driven, and integrated approach that empowers organizations to anticipate, withstand, recover from, and ultimately adapt to fast-moving disruptions.

Everbridge High Velocity CEM™, powered by Purpose-built AI, stands at the forefront of enabling this next generation of resilience. Its intelligent automation, real-time risk intelligence, and unified platform architecture position organizations to cut through operational noise, streamline response times, and maintain continuity - regardless of the event's scale or complexity. Serving more than 6,500 customers globally, Everbridge has demonstrated that scalable, enterprise-grade solutions are essential to meet the demands of the expanding risk zone.

As we look ahead, the challenge will be to maintain vigilance while fostering a culture of continuous improvement and cross-functional collaboration. Organizations that act boldly to operationalize future-ready strategies and leverage advanced solutions will not only survive uncertainty, but thrive - transforming adversity into sustained strength and opportunity.

Experience the power of Everbridge for yourself

Ready to transform how you manage critical events and strengthen your organization's resilience? Request your personalized demo to see Everbridge in action today. Call us at +1 (888) 366-4911 to speak with a resilience expert, or schedule a demo at everbridge.com/demo

Schedule a demo

Additional resources

High Velocity CEM webinar series

Gain expert guidance, practical insights, and real-world solutions to tackle both physical and digital threats. Our ongoing webinar series empowers your team to ensure business continuity and resilience in an ever-changing risk landscape.

Register here →

Rapid Resilience videos

Stay informed on critical global events with timely updates and expert analysis from Everbridge specialists. Our Rapid Resilience videos provide actionable strategies aligned with real-world developments, delivered as events unfold.

Watch here →

Thought leadership insights

Explore thought-provoking articles and videos from industry experts. Resilience isn't just about responding to crises - it's about anticipating challenges, adapting to change, and thriving in the face of disruption. Gain insights from leading voices shaping the future of resilient organizations.

View here →

Explore the Everbridge product suite

Discover Everbridge High Velocity CEM, the industry's most advanced critical event management platform. Combining automation, risk intelligence, and Purpose-built AI, it delivers resilience at scale. Explore our full product suite designed to support your organization in every step of its resilience journey.

Learn more here →

Take a virtual tour

See how Everbridge can transform your organization with a personalized demo tailored to your needs. Select your areas of interest, and we'll deliver a custom video showcasing the solutions that matter most to you.

Visit here →

Online resource hub

Access a wealth of knowledge, including whitepapers, analyst reports, online training, and in-person events. Our comprehensive resource hub equips you with the tools to navigate crisis management, ensure business continuity, and manage today's expanding risk environment effectively.

Explore here →

Appendix

Boardroom questions for building future-readiness

Building future-readiness requires proactive planning and tough questions at the boardroom level. Here are some key questions leaders should ask to ensure resilience across operations, technology, and emerging risks:

- Where are our **single points of failure** across people, sites, technology, and suppliers - and what is our **surge plan**?
- How quickly can we **detect, assess, notify, and mobilize** for our top five risks? Are playbooks current and exercised?
- What portion of **revenue and operations** is protected by tested continuity measures? Where are the gaps?
- How are we **governing AI use** and guarding against AI-enabled threats (deepfakes, automated attacks)?
- Which **geopolitical, regulatory, or climate exposures** are rising, and what **diversification options** are ready now?
- Do we have a comprehensive **crisis communication** plan, regularly updated and tested across scenarios?
- What are the potential impacts of a major **cyberattack** on core operations, and how confident are we in recovery time objectives?
- Are there potential vulnerabilities in our **supply chain**, and what alternates (suppliers, lanes, modes) are pre-approved?
- Is our organization truly **resilient and future-ready**?

everbridge™

Empowering Resilience

About Everbridge

Everbridge is the global leader in Critical Event Management (CEM), helping organizations achieve a true business resilience advantage. With Everbridge High Velocity CEM™, our customers accelerate response times, minimize disruption, and maintain operational control amid today's most complex threats. Using Purpose-built AI, decision-ready risk intelligence, and full lifecycle automation, Everbridge enables organizations to know earlier, respond faster, and improve continuously with confidence.

Everbridge... Keeping People Safe and Organizations Running™

Visit Everbridge.com

Read our company blog

Follow us on LinkedIn

Follow us on X

Everbridge delivers a business resilience advantage with High Velocity CEM™, powered by Purpose-built AI and decision-ready intelligence to accelerate response, reduce downtime, and protect what matters most.
Request a demo at everbridge.com/demo or call +1 (888) 366-4911.

WP-EN-GlobalRiskAndResilienceOutlook2026 _11.17.25