BTR: Critical Event Management Becomes a Strategic Imperative as Risk Landscape Intensifies

WASHINGTON, DC, UNITED STATES, October 16, 2025 /EINPresswire.com/ -- In 2025, enterprise resilience has shifted from a defensive posture to a core strategic capability. A convergence of threats — from geopolitical instability and extreme weather to cyber incidents and shifting compliance mandates — is redefining what it takes to keep people, assets, and operations safe.


David Wagner, Everbridge

Critical event management (CEM), once a niche operational discipline, is now emerging as a board‑level priority. Executives say that the modern business environment no longer produces rare “black swan” disruptions. Instead, unexpected crises have become a routine hazard of global operations.

“We don’t live in a world where black swan events are black swan events anymore,” said Bryan Barney, chief product officer at Everbridge in a BizTechReports vidcast interview for journalists. “They happen with a lot of frequency. Modern organizations must manage those events systemically, with the right tools and trained professionals, to maintain resilience.”

From Alert Systems to Lifecycle Risk Management

Historically, critical event response was reactive. Early CEM systems focused narrowly on disseminating alerts — notifying employees, customers, or the public during an emergency. But as operations became more complex and globally distributed, industry leaders recognized the need for a more comprehensive approach.

“The planning group and the chief security officer are coming together more tightly than ever

before," said Dave Wagner, president and CEO of Everbridge. "It's about making sure that when a critical event occurs, you're executing practiced motions — not starting from scratch."


Bryan Barney, Everbridge

Today's best practices in CEM, he contends, integrate four key lifecycle stages:

Early detection of emerging threats through continuous monitoring of global and local risk signals.

Impact assessment to determine potential effects on facilities, supply chains, personnel, and critical systems.

Coordinated response that aligns resources across departments and geographies.

Continuous improvement through post‑event analysis and scenario‑based training.

Rather than treating incidents as isolated problems, the new model embeds resilience into the organization's core operating framework. This aligns CEM more closely with disciplines like enterprise risk management, governance, and operational continuity.

> Like almost every industry, AI is poised to transform ours. It's particularly useful in generating risk events, helping you understand the world around you, and preparing for those threats."
>
> *Bryan Barney, Everbridge*

Governance and Regulatory Pressures

Corporate governance is also exerting growing influence over resilience strategies. Board members and risk committees increasingly demand visibility into how the enterprise is preparing for and responding to critical events. This mirrors the shift in cybersecurity oversight that began more than a decade ago with adoption of NIST and other frameworks.

"Boards are becoming much more sophisticated in their assessment of risk," Wagner noted. "Frameworks that originated in cybersecurity are now propagating into physical security, business continuity, and crisis management."

The regulatory environment is amplifying the pressure. In the European Union, the Digital Operational Resilience Act (DORA) is prompting financial services providers and other critical industries to formalize their resilience planning. Similar mandates in other jurisdictions are pushing organizations to document their ability to withstand operational shocks.

But Wagner cautioned against seeing compliance as a cure-all:

“Regulations matter, but the stories of success matter more — companies that invest in resilience not only avoid damage, they elevate their brand and strengthen market position.”

Cross-Functional Integration: Breaking Down Silos

One of the most significant shifts in CEM is the move toward cross-functional ownership. Effective response requires coordination among physical security, IT, facilities, supply chain, HR, communications, and legal teams.

“Critical events are almost always a cross-functional issue, and the response has to be cross-functional,” said Barney. “Getting modern organizations to operate that way isn’t always easy, but companies that take this seriously are getting quite good at it.”

Business continuity planning has become a focal point for this integration. Industry best practice calls for cross-departmental working groups to map critical processes, identify single points of failure, and create scenario-based mitigation plans.

Resilience as a Competitive Advantage

The economic case for resilience is gaining traction. Once viewed primarily as a cost center — akin to an insurance policy — resilience investments are now being evaluated for their contribution to long-term performance.

“It was Ben Franklin who famously said an ounce of prevention is worth a pound of cure,” Wagner observed. “In today’s environment, that same ratio — one to 16 — is about what the studies show when you invest in resilience.”

Independent benchmarking suggests that companies with strong resilience programs often outperform their peers during crises. In some cases, proactive communication and rapid service restoration have turned potential brand-damaging events into reputational wins.

“Avoiding a prolonged outage, protecting customer access, and keeping the lights on isn’t just risk mitigation,” said Barney. “It’s a competitive differentiator.”

AI Changes the Playbook

Artificial intelligence is beginning to reshape how organizations detect, assess, and respond to critical events. AI-driven risk intelligence platforms can monitor vast streams of structured and unstructured data — from weather reports and sensor feeds to social media chatter — to identify emerging threats earlier than human analysts alone.

“Like almost every industry, AI is poised to transform ours,” Barney explained. “It’s particularly useful in generating risk events, helping you understand the world around you, and preparing for those threats.”

Generative AI is also making it easier for non-technical staff to craft accurate, timely communications during a crisis. Automated recommendations, drawn from historical data and scenario modeling, can guide decision-makers under stress.

Still, both executives warn against over-reliance:

“We’re focused on the human decision-maker,” Wagner said. “The human in the loop will continue to be the most important part of a proper crisis response.”

Training and Scenario Simulation

Industry veterans stress the importance of practice. Tabletop exercises — structured simulations of crisis scenarios — are becoming more sophisticated.

“By joining business continuity planning with critical event management, the plan actually informs the response,” said Barney. “It keeps the plan current and front-of-mind for the people managing the security operations center.”

Rather than relying on static “three-ring binder” plans that may be outdated, organizations are turning to dynamic platforms that integrate live operational data into training. This helps keep response skills sharp and reinforces cross-functional coordination.

Market Outlook: Broadening Adoption

CEM adoption remains most advanced in large enterprises, critical infrastructure operators, and government agencies, where both regulatory pressure and risk exposure are high. However, market analysts expect adoption to broaden into the mid-market as AI-enabled automation lowers the expertise threshold.

“AI actually opens up the possibility of taking these solutions down-market,” Barney noted. “It doesn’t require as many well-trained people to operate the system effectively.”

Cloud-based platforms are making sophisticated capabilities more accessible, while the rise of “crisis manager” as a formal role within the C-suite is giving the discipline greater visibility and

authority.

The critical event management market is maturing from a niche operational specialty into a core pillar of enterprise strategy. The combination of a worsening global risk climate, intensifying regulatory demands, and new technology enablers — especially AI — is accelerating that shift.

Click here to read the Q&A based on this interview.

Airrion Andrews
BizTechReports
email us here