Take A Unified Approach To Critical Event Management
An Integrated, Unsilod Approach Helps Companies Improve Operational Resilience
Companies Struggle To Respond To Critical Events

Companies invest significant resources in sophisticated controls to protect people, brand, and assets from critical events. These disruptive incidents (ranging from extreme weather to terrorist activity) increasingly lead to operational losses, brand damage, and concerns for health and safety. Despite investment, companies struggle to optimize their critical event management (CEM) operation, slowing down response time and creating potentially life-threatening confusion. As a result, companies are turning toward continuous resolution and a unified approach to CEM that links security and business operations.

In July 2018, Everbridge commissioned Forrester Consulting to evaluate CEM strategies. We found that a unified approach to CEM improves response and diminishes negative outcomes.

Company location
- All companies are based in the US with operations in at least one other region.

Position
- C-level: 14%
- VP: 22%
- Director: 64%

Industry
- Financial services: 26%
- Manufacturing/CPG: 26%
- Oil and gas: 24%
- Technology: 23%

Revenue
- $500M to $1B: 42%
- $1B to $5B: 39%
- Greater than $5B: 20%

Note: Percentages may not total 100 because of rounding.
Companies Need To Prepare For The Inevitable

Critical events are not only common, they’re next to inevitable: 100% of the companies we surveyed suffered at least one critical event in the past 24 months. In fact, companies often dealt with multiple critical events in that timeframe (over four, on average). The types of critical events varied widely from natural disasters (the most common) to active shooters (rare, but still an occurrence at 1 in 10 surveyed companies). The range of critical event types, including associated causes and consequences, further elevates the role of CEM and necessary tools to ensure a timely and well-coordinated response.

“To the best of your knowledge, how many discreet critical events of any type has your company suffered in the past 24 months?”

- One to three critical events: 34%
- Four to six critical events: 60%
- Seven to 10 critical events: 6%

On average, firms experience four events every two years.

“From which of the following types of critical events has your company suffered in the past 24 months?”

- Natural disaster/ extreme weather (33%)
- Theft of physical/ intellectual property (28%)
- IT failure of a business-critical system (25%)
- Cyberattack (24%)
- Utility outage (24%)
- Executive protection threat (23%)
- Brand/reputational crises (23%)
- Supply chain disruption (22%)
- Terrorism or acts of terror (14%)

Base: 214 critical event management and operations executives in the US at enterprises with global operations
Source: A commissioned study conducted by Forrester Consulting on behalf of Everbridge, September 2018
Critical Events Disrupt Operations, Damage Brands, And Jeopardize Lives

The importance of effective CEM cannot be overstated: Whether it’s a severe tropical hurricane or a ransomware attack, critical events hinder ongoing operational activity and put personnel at risk. Companies have a responsibility to shield their employees, customers, partners, and investors from serious physical and financial harm.

Adding further complexity, the damage and the recovery can’t be siloed. For example, one business traveler described how he and his coworkers are regularly subjected to violent car robberies when traveling in Central America due to the valuable devices and data his team is tasked with transporting. Employee safety is a top concern, but the cyber risks of stolen data and compromised devices are also key corporate threats.

*The complex ripple effects of even one critical event can result in widespread and severe organizational damage.*
Companies Worldwide Deploy A Unified Approach, Seeking Better Capabilities For Event Detection And Response

Companies are increasingly taking a unified approach (also known as the cross-functional fusion center approach) to combating the widespread damage of critical events. These companies work across business units, combining internal resources, technology, and business services, such that operations have responsibility for detecting and managing events beyond strictly securing facilities. However, the maturity of tools and procedures used to arm their approach is broad; interestingly, in areas where many are excelling, like social media monitoring, one-third see the need for improvement.

*In response to growing pressure, firms seek a unified approach to CEM. Alongside mature tools and metrics, this approach can potentially diminish the effect of events.*
A Maturity Disconnect — Performance Metrics Fall Short

While most companies in our study have implemented a unified approach and have begun maturing their tools and procedures, the metrics they track reveal a maturity disconnect — companies are not as mature as they believe they are. We found that under half of companies track the cost to repair, replace, or improve systems following an event, which can be considered the minimum standard for metrics tied to CEM. The percentage of companies tracking other metrics only decrease from there, from measuring mean time to detect, respond, and recover from events, to lost revenue. Only 30% measure their performance on something as simple as the number of critical events per year.

The disproportionate focus that companies put on measuring the overall cost of events, compared to metrics that track the success of their CEM strategy to minimize damage and loss year-over-year, is proof that companies have more work to do before they can call themselves mature. Without mature metrics, companies will find it difficult to understand what tools and procedures are making the difference, and therefore, how they may be wasting a valuable investment.
Those With A Unified Approach Are Better Prepared, But Even They Can Do More With Their Data And Analytics

The shift toward the unified, integrated approach is proven to be the right strategy: We found that companies without this approach are even further behind in maturing their CEM tools, procedures, and metrics. However, the data tells us that even those with a unified approach are still struggling with robust measurement, particularly in mean time to detect and respond and lost revenue. Without more rigorous metrics, companies are likely to squander their otherwise sensible investment — losing the edge they have over the competition.
Unified Approaches Are Worth The Investment — They Dramatically Improve Time To Detect And Respond

To continue to stay ahead of the competition and get the most from their investment, companies must continue to optimize not only their tools and procedures, but the formal metrics they use to measure outcomes as well. In return, companies with a unified approach will see a return on their investment in the form of reduced mean time to identify, know, fix, and resolve events — the real measures of a successful CEM strategy. Companies that work to integrate their approach across silos also report a significant reduction in the impact that critical events have on safety, reputation, and revenue.
Companies Without A Unified Approach Have More To Gain Than They Realize

There may be no greater benefit to the unified approach than the improved ability to protect the lives of employees and customers in crisis. However, the benefits don’t stop there. More than half of these companies see improved critical event reporting, improved communication workflows, and better-defined roles and responsibilities of the personnel involved in CEM — all of which contribute to a more efficient organization overall.

Interestingly, when companies without a unified approach were asked what they might gain by adopting the approach, they significantly underestimated the benefits across the board. This suggests that those who have yet to integrate their response and management of events are not fully aware of what their approach lacks, as well as the potentially dangerous consequences that could arise as a result.

Companies who take a unified approach are more mature, efficient, and prepared to handle critical events.
Conclusion

A unified approach to CEM — connecting siloed units in continuous event resolution — meets the demands for rapid response and speedy incident remediation. Companies without this approach are far behind, missing out on significant operational benefits. However, companies with a unified approach cannot become complacent and fail to further optimize their tool set and metrics. Good intentions and the adoption of a unified approach are not enough — companies must seek out best practices in tools and metrics to continuously improve their CEM. They should look to their peers and partners to ensure they have best practices in place and then work to follow them.

Endnotes


2 In the custom survey, critical incident fusion center was defined as a unified approach to critical incident planning, mitigation, response, and remediation across business units and functional silos (such as security, risk, operations, and IT) using a combination of internal resources, technology, automation, and business services.