everbridge®

9 Steps TO CRITICAL EVENT MANAGEMENT IMPROVEMENT

Many organizations are being asked to respond more quickly and decisively to critical events – e.g., workplace violence, severe weather, supply chain disruptions, etc. –, but with fewer resources. Without an end-to-end process to manage the entirety of these events, it's nearly impossible to satisfy this mandate. As a result, security, operations and risk management professionals lack the time needed to react or even avoid the negative consequences of these events.

This paper explains why the traditional approach to managing emergencies and business disruptions is outdated, and shares a holistic approach to Critical Event Management (CEM) that enables a more unified, efficient, distributed, automated and collaborative process.

WHY CRITICAL EVENT MANAGEMENT (CEM) MATTERS

Disruptive safety and operational events occur every day: think active shooters, IT outages, supply chain disruptions, to name a few. In fact, these events are on the rise.

Twenty-one states in the United States saw active shooter incidents in the two-year period from 2016 to 2017, ten more than in the previous two-year period, according to a new FBI report.[1] According to The Economist, the number of weather-related disasters worldwide has more than quadrupled to approximately 400 a year since 1970.[2] Moreover, terrorism attacks and risks are projected to increase around the world. According to the 2018 Business Continuity Institute: Horizon Scan Report[3] the top 5 Threats for 2018 are:

1. **Cyber attack**
2. **Data breach**
3. **Unplanned IT & telecom outages**
4. **Interruption to utility supply**
5. **Adverse weather**

Whatever their nature, in the simplest terms, events are considered critical when they impact one or more of the assets that matter to an organization (see figure 1).

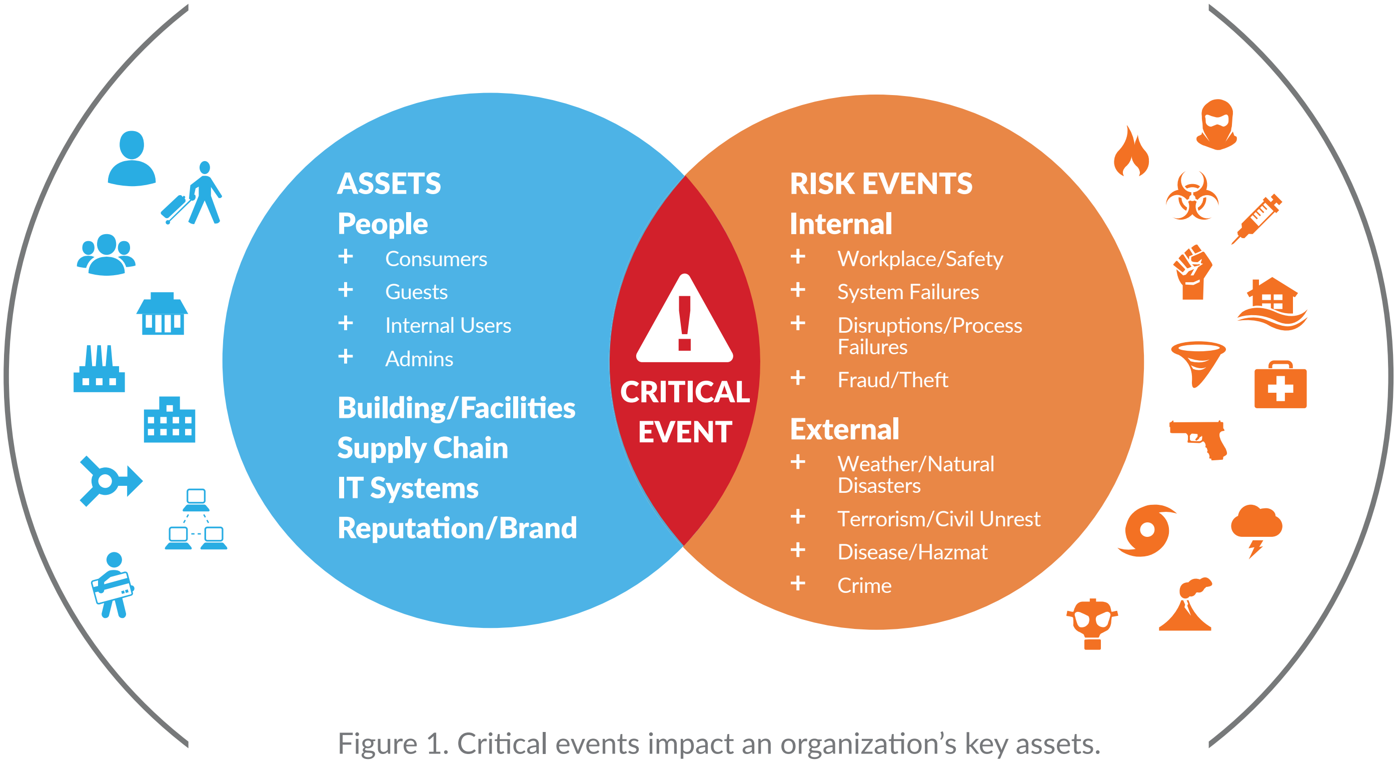


Figure 1. Critical events impact an organization's key assets.

Remember: A critical event doesn't necessarily equate to a major breakdown. For some businesses – such as financial services firms and retailers – a website that performs milliseconds slower is a critical event. While each organization will define critical events differently, the aim is to minimize or even mitigate the impact.

Unfortunately, many organizations struggle to achieve this goal. They are being asked to respond more quickly and more decisively, but with fewer resources. However, without an end-to-end process for dealing with critical events, it's nearly impossible to satisfy this mandate.

As a result, security, operations and risk professionals need more time to react or even avoid the negative consequences of these events. Critical Event Management (CEM) enables a unified, efficient, distributed, automated and collaborative process for managing critical events.

UNFORTUNATELY THE OLD WAY DOES NOT ALWAYS WORK

In most cases, organizations are trying to deal with critical events using manual processes and disjointed systems. As a result, they are unable to efficiently and effectively manage these events.

In an environment characterized by disjointed processes and information, organizations are often grappling with too much data, making it extremely challenging to arrive at a basic understanding about an event. Complicating matters is that few organizations excel at keeping track of their people and assets in transit – think workers and equipment on the road and in the field.

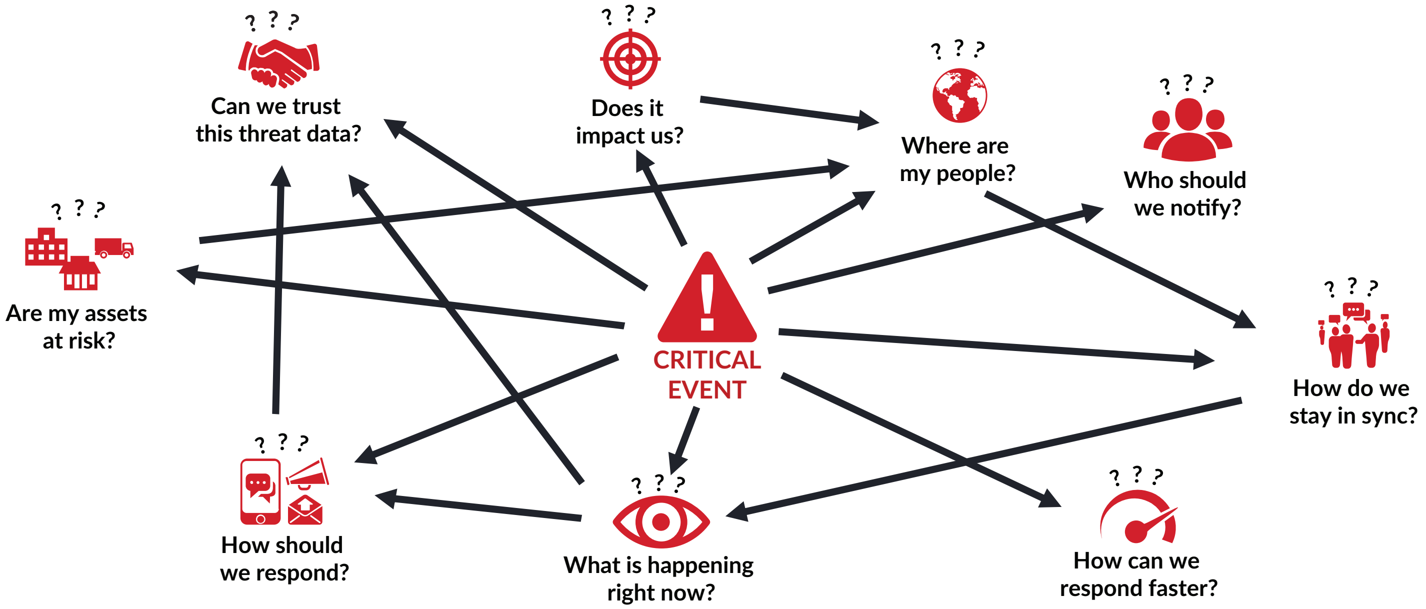


Figure 2. Disjointed processes lead to a slow, reactive response

Combined, these make resolution slow, unclear and reactive, and actually increase risks. Employees might be in harm's way and operations could be disrupted. In turn, customers lose confidence in the organization, threatening brand value and revenues. Just as important, a slow, reactive response increases the costs posed by these events. Consider that just the cost of IT downtime averages $8,900/minute.[4] No wonder businesses worldwide suffered $535 billion in losses in 2016 due to critical events.[5]

By adopting a proven, 9-step approach, organizations can improve their response to critical events.

1 DEVISE A PLAN

It seems simple enough to develop a CEM plan, but the plan must be comprehensive in order to be effective. It starts with a general plan that expands to cover various types of crises differing in scope and is mapped to appropriate resources and response activities. According to recent research from the Business Continuity Institute, 86% of organizations have emergency plans.[6] The graph below highlights the most frequently activated plans from that same research report.

"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%)
- Active shooter (11%)

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

Figure 3.

Given the types of threats it may face, organizations should:

- Appropriately categorize critical events by type, predictability, cause and scope, while differentiating between routine emergencies and crisis events.
- Determine how the organization will deal with each event, and who will take the lead.

The plan should include severity levels that dictate the composition of the relevant response teams so it can be activated as quickly as possible.

If the organization has crisis management plans in place, ensure it is operational in nature based on predictability. For example, if the organization operates in a hurricane-prone region, develop a hurricane plan, including one to deal with office closings. If the organization operates in multiple locations, ensure the plans are standardized. In today's mobile world having digitized plans readily accessible by mobile device is key when responding to critical events while out of the office.

"Routine" Emergency vs "Crisis" Emergency[7]

"Distinguishing "routine" vs "crisis" emergencies can inform your response strategy. A routine emergency does not mean "easy." On the contrary, a routine emergency can be very difficult and challenging. In this context, "routine" refers to the relative predictability of the situation that permits advanced preparation. The risk presented by the situation was included in your risk profile and you probably have created appropriate plans, developed relevant training and completed exercises for routine emergencies. In short, your business and technology continuity and disaster recovery plans are filled with strategies to manage them.

In contrast, a "crisis" emergency is a much different animal. These events are distinguished by significant elements of novelty. This novelty makes the problem much more difficult to diagnose and then deal with. This type of emergency often has one or more of the following characteristics:

1. The threats have never been encountered before, which means there are no existing plans to manage it.
2. The situation may be a familiar event, however, it is developing at unprecedented speed; therefore, developing and executing an appropriate response (including notifications and ongoing coordination) is severely challenging.
3. The incident may represent a confluence of forces, which, while not new individually, in combination, pose unique challenges to the response.

Excerpted from "From Routine to Crisis", Regina Phelps, CEM, RN, BSN, MPA and Kelly David Williams, http://go.everbridge.com/ITAlerting-ReginaPhelps-Sept292015EMEA.html

2 BUILD PARTNERSHIPS WITH LEADERSHIP

Critical events can impact different areas of the business, and often impact more than one. This is why more companies are changing their organizational structure to enable a consolidated approach toward handling major incidents. Sometimes it starts with an overlay team that deals with major incidents. The ideal is to build a fusion center – a collaborative effort of two or more functions that provide resources, expertise and/or information to a joint response center with the goal of maximizing the ability to detect, prevent, apprehend and respond to critical events, regardless of scope.

However, if that's not possible, the best practice is to build alliances across the chief security officer (CSO), chief information security officer (CISO), and chief information officer (CIO) at the very least. Combining the experience, insights and intelligence from across the organization makes it possible to quickly understand the root cause of an event and ensure a rapid response and operational continuity.

3 ASSESS YOUR RISKS AND SOURCES OF INFORMATION

With a plan and partnerships in place, it's time to assess how well the organization can navigate critical events. One of the biggest issues is not knowing when a threat develops and then not being able to confidently vet what happened.

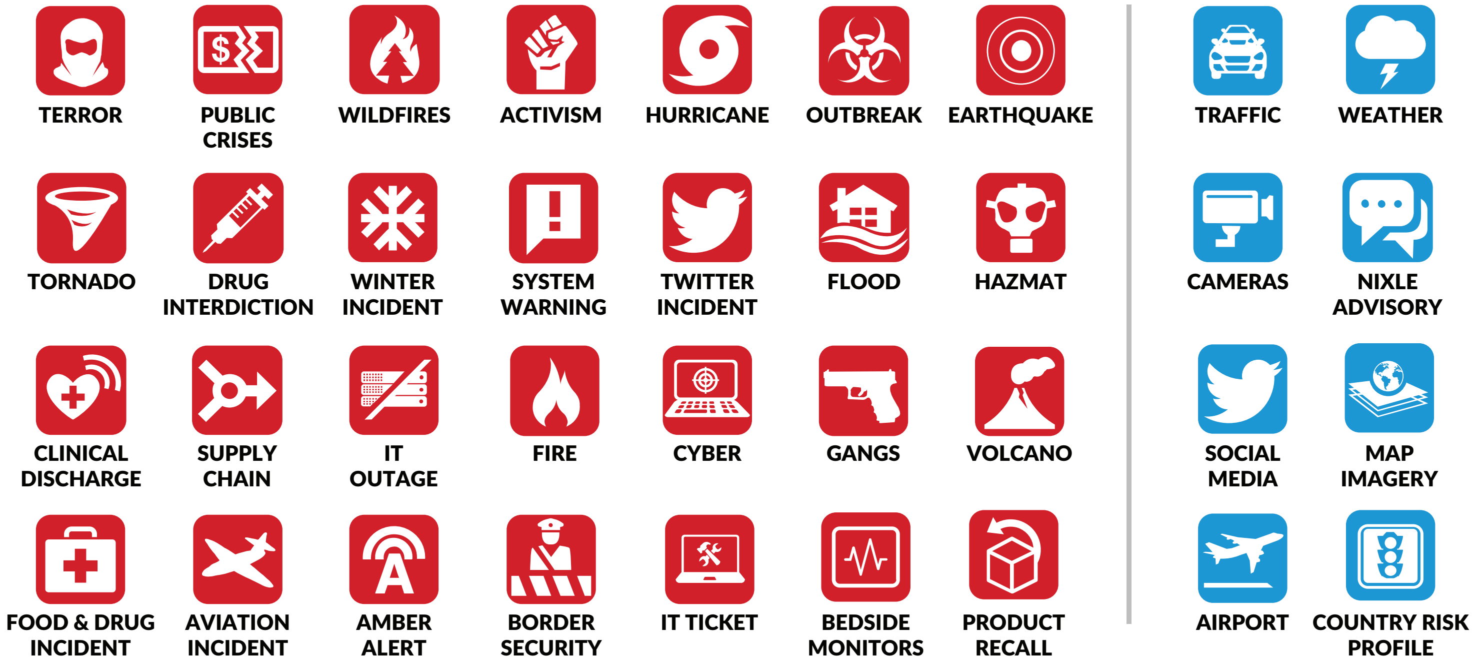


Figure 4. Types of critical events and information sources

As people are assessing events and risks, they typically call upon a range of information from a variety of sources that might be lacking details or even contradictory. The goal is to confirm the threat event and ensure the appropriate team has all needed input and contextual feeds in one place to make the appropriate decisions. That means lining up trusted information sources for all types of risks.

This undertaking can get complex, especially in larger organizations. Start by understanding the event in the context of the five key assets: people, buildings, IT systems, supply chain and brand/reputation. In some cases, organizations might even associate a particular value to these assets in order to better determine risk.

4 IDENTIFY CRITICAL ASSETS AND FUNCTIONS

During every event, it's essential to know where employees, travelers, visitors, offices, manufacturing facilities and other critical assets are located. It's also critical to know how they are interconnected and the dependencies between them. Ideally, organizations can visualize this at a glance.

Common examples of business assets include:

- Employees
- Buildings, branches and retail stores
- Product inventory
- Supply chain
- Machinery & specialty equipment
- Land
- IT assets
- Brand/reputation

Beyond knowing the location and interdependencies, organizations also need an idea of how much it will cost if these assets are impacted by an event. For instance, perhaps a critical business application goes down resulting in a thousands of dollars in losses every minute. It's important to calculate losses based on the overall use case, such as how many employees are going to be impacted.

Organizations must be careful not to overlook less tangible assets such as their brand and reputation. A firestorm of Tweets could cause far more damage than a physical attack on the company or its infrastructure.

5 QUANTIFY AND PRIORITIZE YOUR RISK

The next step is to figure out what is critical and what isn't. Answer the big question: What is the impact and exposure?

An effective approach is to differentiate between threats and risks across the board, and to then quantify risk based on:

- The threat
- The threat's nature
- The organization's overall vulnerability or exposure
- The overall impact, which may go beyond the immediate assets, people and elements that are in harm's way

Unfortunately, it's not a simple equation because organizations must factor in a few more variables. Consider the overall timeline, which is often dynamic. For instance, it's not sufficient to ask, "How many employees are in HQ right now?" since employees are constantly on the move. Or perhaps a geopolitical issue or event is going to cause a disruption to the supply chain, but the organization won't feel the impact for two months.

While it's critical to quantify risk, keep in mind that the impact from a single event can differ across the company and can impact different assets in different ways. For instance, a labor strike in Paris is not a critical event for local employees who know how to deal with it, but it is for ex-pats and traveling employees who aren't accustomed to this.

In other words, context matters, and can change the risk profile. The key is to understand risk based on all variables to determine the best response to any event.

6 IDENTIFY AND LOCATE ALL STAKEHOLDERS

Quickly locating, communicating with and assisting employees in a crisis is a priority. To that end, typically in any type of critical event, organizations will be dealing with three groups of stakeholders:

The people who can do something about the event. These people can put context around the situation and can help assess the threat to determine who's impacted. They might be called responders or resolvers. In larger organizations, this might be an incident response team. When creating a list of responders, organizations should take into consideration schedules, rotations and locations.

Those impacted. In addition to identifying impacted people, organizations must know where they are located so they can be quickly notified. Automating communication can save even more time.

Those needing to know about the event. Who needs to know about the event? Should the CEO be woken up at 2 am? Should the governor or other high-ranking officials be involved? Can the event be handled regionally? Determining this ahead of time is key to reducing the impact of the event.

To avoid alert fatigue or "the boy who cried wolf" syndrome, only inform those who need to know. At the same time, make sure people aren't bombarded with updates. If possible, let the appropriate people see all necessary information in one place. To that end, set up profiles indicating who can do what based on skill sets and experience, and who should be involved under different circumstances. Be sure to include a secondary profile, including 'identifiables' for people who may be limited in dealing with a crisis – such as those with disabilities.

7 VISUALIZE WITH A COMMON OPERATING PICTURE

To minimize confusion and accelerate an effective response, it's necessary for everyone to share and operate from the same set of information about the situation. If everyone knows how many people, supply routes, buildings, etc. are impacted by the situation it can dramatically speed the overall response and increase effectiveness.

It's also important that people are viewing the right information to make informed decisions and not wasting time trying to correct the dissemination of bad intelligence. Along those lines, here are three best practices:

- Know when to engage the appropriate levels of people as well as the appropriate functions.
- Launch the appropriate protocols.
- Be prepared to deal with more groups and workflows for more complex situations.

8 AUTOMATE WORKFLOWS

Once organizations mature their processes, the opportunity exists to automate many of the previous steps to prevent human errors and respond more quickly. As a result, they are able to execute their CEM plans by feeding a minimal amount of relevant information into a CEM system. Some take it a step further by adding elements like checklists. Even checklists should be dynamic in nature, but they help ensure nothing is overlooked as events are occurring.

A good place to start with workflow automation are with the most frequent activities a team addresses. Consider the list below as a starting point:

- Emergency operations center (EOC) activation notices
- Employee accountability checks
- Executive sitrep reports
- Executive conference bridge activation
- Response team callouts

9 ANALYZE PERFORMANCE

The final step is to close the loop by analyzing how well the organization responded. By classifying and tracking all assets in a centralized, visual and correlative way, it's possible to assess each event's impact and response effectiveness.

Data tells us organizations that perform after-action reviews improve their future response by understanding the following:

- Has this happened before?
- What was the impact?
- What did we do well?
- What could we have done better?
- What slowed us down?
- Who was involved?
- Who responded fastest?

The ideal is to be able to readily access all this information to analyze it in different ways, such as by determining the incident response commander for the three times the organization responded fastest. Just remember: the key is to not only perform these reviews but to close the loop by learning from experience and continually improving the plan and response.

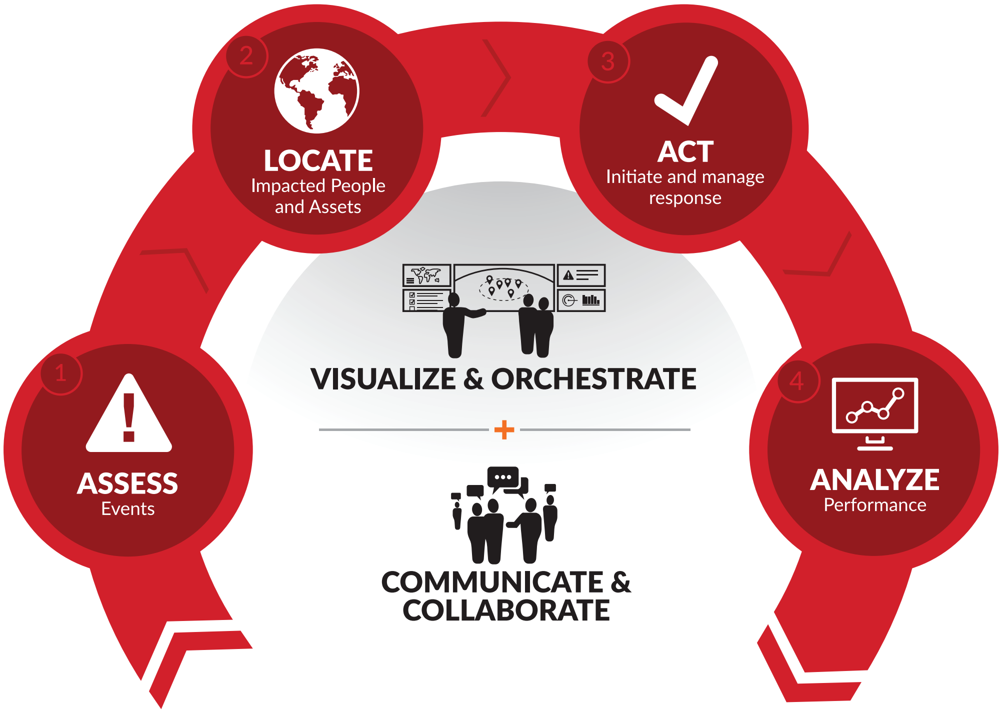
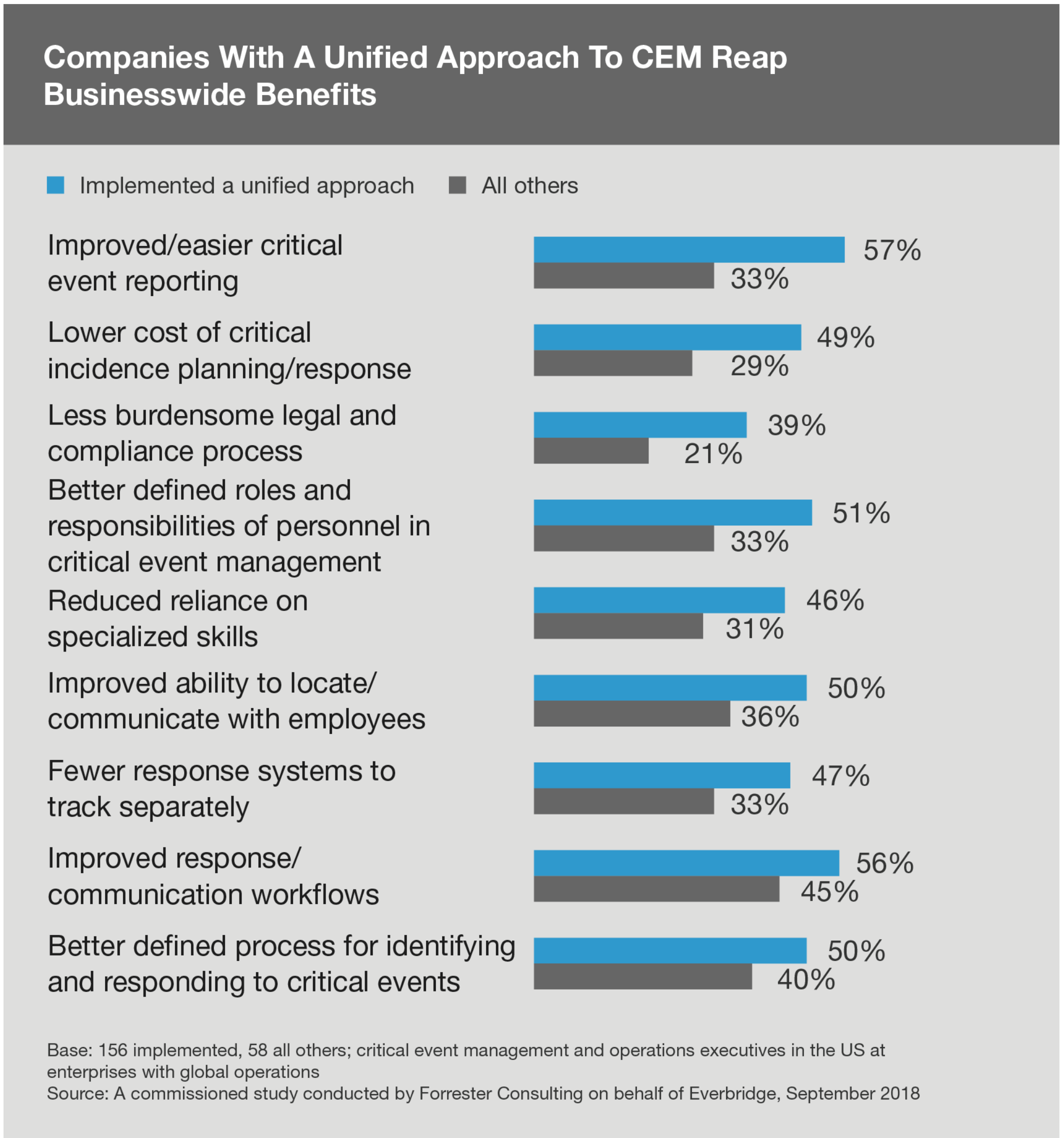


Figure 5. Unified Critical Event Management

As organizations reach higher levels of crisis event management maturity, they are likely to realize the following benefits:

1. Immediately know where all employees are when a disaster strikes and have a failsafe way to communicate with them.
2. Improve the operational efficiency and effectiveness of crisis management systems.
3. Avoid business disruptions and recover faster from events that impact assets.
4. Gain resilience by reducing enterprise and employee risk exposure.



Companies With A Unified Approach To CEM Reap Businesswide Benefits

Base: 156 implemented, 58 all others; 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

Figure 6.

CONCLUSION

As organizations face the prospect of dealing with a growing range of threats, they are smart to formalize and consolidate their operational response. Businesses are expected to not only know where their employees are at all times, but to quickly and easily gather information about critical events in order to anticipate the business and life safety impact.

In turn, organizations understand the need to simultaneously protect their people, buildings, IT systems, supply chain and brand/reputation. Harnessing the right CEM technology, they can ensure the latest intelligence is at their fingertips and visualize the threats to their assets. They can then coordinate the appropriate resources based on reliable information, and quickly mitigate critical events of any kind to reduce the impact to safety and business resiliency. Just as important, the right CEM system makes it possible to audit response rates for continual improvement.

Just as companies grasp the need for CEM, employees are starting to see the importance of this process and how it can keep them safe in a crisis. In a tight job market where companies are competing for talent, organizations that can point to employee protection will stand apart.

[1] Active Shooter Incidents in the United States in 2016 and 2017 FBI, May 7, 2018, https://www.fbi.gov/file-repository/active-shooter-incidents-us-2016-2017.pdf/view

[2] The Economist, Weather-related disasters are increasing, August 29, 2017, https://www.economist.com/graphic-detail/2017/08/29/weather-related-disasters-are-increasing

[3] Business Continuity Institute: Horizon Scan Report 2018, February 9,2018, https://www.thebci.org/resource/horizon-scan-report-2018.html

[4] Ponemon Institute – Cost of IT Downtime, 2016

[5] Institute for Economics and Peace, Global-Terrorism-Index-2015; Swiss Re, Preliminary sigma estimates for 2015: global catastrophes cause economic losses of USD 85 billion; Lloyd's, Cyber attacks cost companies $400 billion every year

[6] *BCI Emergency Communications Report 2017* Business Continuity Institute, https://www.thebci.org/news/bci-emergency-communications-report-2017.html

[7] Managing Crisis: Responses to Large-Scale Emergencies, Arnold Howitt and Herman Leonard, CQ Press, page 5

[8] Ibid.

ABOUT THE AUTHOR

Imad Mouline is the chief technology officer for Everbridge. In this role, Mouline is responsible for Everbridge's market strategy, product roadmap, innovation, and research and development.

Mouline joined Everbridge in 2011, when the company acquired CloudFloor, an enterprise cloud management company where he was co-founder and CTO. Prior to CloudFloor, Mouline served as CTO of Compuware's Application Performance Management Solutions division, which was formed when the company acquired Gomez, a provider of web performance management solutions, where Mouline was CTO. Before this, he served as CTO of S1 Corporation, a provider of financial services solutions.

Mouline is a regular presenter at industry, technology, and academic conferences, including APCO, NEDRIX, the World Conference on Disaster Management, Cloud Connect, Interop, Internet World, and the MIT CIO Symposium. He is frequently quoted in leading publications including The New York Times, USA Today, BBC News, BusinessWeek, CNN Money, Fortune, Forbes, Investor's Business Daily, Network World, CIO Zone, and InformationWeek.

Mouline is a graduate of the Massachusetts Institute of Technology, and has been awarded five US patents.

ABOUT EVERBRIDGE

Everbridge, Inc. (NASDAQ: EVBG) is a global software company that provides enterprise software applications that automate and accelerate organizations' operational response to critical events in order to keep people safe and businesses running. During public safety threats such as active shooter situations, terrorist attacks or severe weather conditions, as well as critical business events including IT outages, cyber-attacks or other incidents such as product recalls or supply-chain interruptions, over 4,000 global customers rely on the company's Critical Event Management Platform to quickly and reliably aggregate and assess threat data, locate people at risk and responders able to assist, automate the execution of pre-defined communications processes through the secure delivery to over 100 different communication devices, and track progress on executing response plans. The company's platform sent over 2 billion messages in 2017 and offers the ability to reach over 500 million people in more than 200 countries and territories, including the entire mobile populations on a country-wide scale in Sweden, the Netherlands, the Bahamas, Singapore, Greece, Cambodia, and a number of the largest states in India. The company's critical communications and enterprise safety applications include Mass Notification, Incident Management, Safety Connection™, IT Alerting, Visual Command Center®, Crisis Commander®, Community Engagement™ and Secure Messaging. Everbridge serves 9 of the 10 largest U.S. cities, 8 of the 10 largest U.S.-based investment banks, all 25 of the 25 busiest North American airports, six of the 10 largest global consulting firms, six of the 10 largest global auto makers, all four of the largest global accounting firms, four of the 10 largest U.S.-based health care providers and four of the 10 largest U.S.-based health insurers. Everbridge is based in Boston and Los Angeles with additional offices in Lansing, San Francisco, Beijing, Kolkata, London, Oslo and Stockholm. For more information, visit www.everbridge.com, read the company blog, and follow on Twitter and Facebook.

everbridge®

VISIT WWW.EVERBRIDGE.COM
CALL +1-818-230-9700