

An aerial photograph of a large crowd of people walking on a floor with a glowing orange and yellow geometric grid pattern. The scene is viewed from above, showing the tops of heads and the intricate layout of the floor design.

FOR CIOs

# Why Standardize Orchestration and Automation of the Incident Response Process?

How CIOs can prepare for  
critical events management  
while streamlining IT operations







**RISK IS GROWING**

---

## **Crisis Management, IT Alerting and Business Continuity: The Big Picture**

There's a real cost to lost opportunities resulting from unplanned technology disruptions, outages, or breaches. Gartner advises those charged with maintaining business continuity to understand the impact of unexpected downtime on a range of indicators, including user experience, revenue, sales and safety<sup>1</sup>, rather than only chasing the elusive dollar figure associated with a given interruption.

In order minimize downtime and protect people, facilities and business operations, Chief Information Officers (CIOs) need timely information on the nature of every critical event and context to understand how it is affecting the business overall.

---

<sup>1</sup> Gartner

**The shift in emphasis on remote work in the worldwide response to the COVID-19 pandemic exposed countless enterprises to phishing scams, malware attacks and other cyber crimes.**

## **RISK IS GROWING**

Cybercrime skyrocketed in early 2020 as businesses were reacting to COVID-19.<sup>2</sup> The pandemic forced enterprises around the world to grant millions of workers remote access to corporate resources, often via untrusted devices. This pivot opened companies to increased risks of phishing, malware, intrusion and data exfiltration. The U.S. Department of Health and Human Services noted that more than 10,000 COVID-related domains were registered in the first quarter of 2020, many of which were hosting malware.<sup>3</sup>

Beyond pandemic-inspired cybercrime, enterprises today are already at daily risk for unplanned disruptions. Some will result directly from infrastructure failures. Other potentially more damaging events, like extreme weather, natural disasters, or workplace violence may also impact IT. These disruptions place the broader enterprise in peril too. In either scenario, IT operations and company financial performance can be severely affected.

Large enterprises need to monitor their global operations and be ready to react immediately and appropriately as soon as a threat is detected. Consequences of failing to act with the proper urgency and remediation steps can not only have an impact on business operations and profits, they can put assets and even personal safety at grave risk.

---

<sup>2</sup> Federal Bureau of Investigation

<sup>3</sup> HHS

**The IT environment is getting more convoluted each year as new solutions gain traction in the enterprise marketplace.**

**1,935** different cloud services  
are used by enterprises

**750** custom applications have been  
deployed by global enterprises

Due to the increasing reliance on technology to facilitate business-critical activities, operational efficiency is clawing its way up the CIO priority list.

## THE RISK IS GROWING

Business continuity and resilience are perennially at the top of the CIO agenda. Due to the increasing reliance on digital strategies to facilitate business imperatives, however, operational efficiency is now gaining visibility with CIOs and corporate boards. According to recent reports from McAfee, the typical enterprise uses 1,935 different cloud services,<sup>4</sup> and global enterprises have deployed an average over 750 custom applications.<sup>5</sup> This complexity only increases each year as new solutions gain traction in the marketplace. As large enterprises extend their global presence and expand their digital footprint, pressure mounts on CIOs to streamline these complex operations.

Operational efficiency is no longer solely the responsibility of the chief operations officer (COO). All executives, CIOs among them, must identify opportunities to bring greater efficiency to the enterprise. The CIO can contribute by recommending strategic consolidation of enterprise technology solutions.

---

<sup>4</sup> McAfee

<sup>5</sup> McAfee

**With Critical Event Management (CEM) from Everbridge, enterprises can engage a SaaS solution built on a unified architecture that integrates all emergency response communications to protect company assets and people and preserve business continuity.**

## THE PILLARS OF RESPONSE

Three pillars comprise effective response to critical events requiring urgent and immediate action:

- 1) Ability to communicate quickly and meaningfully across the organization
- 2) Collaboration hubs in which people can work together to effectively restore normal operations
- 3) Consolidated digitalization of business processes and orchestrated workflows which efficiently move information upstream and downstream in support of rapid resolution

When it comes to leveraging these pillars to protect people and assets and ensure business continuity, CIOs have Everbridge as a strategic partner to bring all systems for crisis management and IT alerting into a purpose-built, end-to-end, workflow-driven, emergency incident response platform. With Critical Event Management (CEM) from Everbridge, enterprises can engage a fully cloud-based SaaS solution featuring a unified architecture that aggregates and integrates all emergency response communications to protect company assets and people and preserve business continuity.



## The Business Case for Critical Event Management

Critical events cause disruptions to the operations, safety, and security of businesses every day.

From extreme weather and natural disasters to cybercrime to pandemics, the threats businesses face are increasing in scope and frequency. With each critical event, businesses are losing an average of \$350,000.<sup>6</sup>

---

<sup>6</sup> Risk & Insurance

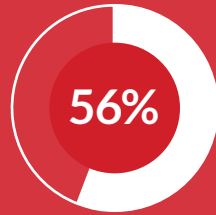
## The broad impacts of poor critical event response

⚠ In 2018, economic losses caused by natural disasters amounted to more than \$220 billion,<sup>9</sup> and the FBI reported that businesses suffered another \$2.7 billion in losses from cybercrimes.<sup>10</sup>

⚠ In addition to revenue losses:



Of the critical events resulted in severe impacts on customer and employee safety.



Caused significant damage to the brand reputation.

⚠ Erie County Medical Center in Buffalo, N.Y., recently suffered a ransomware attack that cost it \$10 million, infected 6,000 machines and required more than six weeks to recover.<sup>11</sup>

## THE NEED FOR A UNIFIED APPROACH

IT systems are another common point of disruption for businesses. According to the LogicMonitor 2019 report IT Outage Impact Study, nearly half (47%) of study participants have experienced five or more unplanned IT outages over the last three years.<sup>7</sup> Outages can result from multiple, concurrent events which makes resolving them even more difficult. A natural disaster, for example, may cause a power outage that in turn creates an IT outage threatening both business operations and personal safety.<sup>8</sup>

Frontline defense against critical events has become an enterprise-wide imperative which calls for a unified and technology-forward approach. This entails preparing for, and responding to, critical event threats. While critical events may not be avoidable, being impacted without a comprehensive emergency response plan in place ahead of time is. CEM helps enterprises get the right message to the right people at the right time to minimize disruption, preserve business continuity, keep people safe and orchestrate enterprise remediation efforts.

<sup>7</sup> LogicMonitor

<sup>8</sup> Inc.

<sup>9</sup> Climate.gov

<sup>10</sup> Federal Bureau of Investigation

<sup>11</sup> Becker's Health IT





## YOUR ROLE IN CEM

# Orchestrated Incident Response: A CIO Essential and a Key Capability of CEM

CIOs need full visibility and control of the enterprise IT environment to ensure an effective and comprehensive incident response. But when a critical event occurs, CIOs, like all executive leaders, need a broader awareness to understand the potential effects of a critical event on all company assets and personnel. Leaders cannot make the right call on the right remediation steps without a comprehensive understanding of the threats and response options.



## Imagine harnessing the power of a singular, comprehensive solution that allows you to:

- ✓ Create, execute and monitor true end-to-end cross-tool workflows to mitigate the impact of IT incidents on businesses and teams;
- ✓ Proactively orchestrate the response to a wide variety of critical IT service disruptions and interruptions to accelerate resolution;
- ✓ Seamlessly integrate with IT management tool actions and teams' activities to improve efficiency, effectiveness, accountability and predictability.

## YOUR ROLE IN CEM

The Everbridge CEM platform's IT Alerting module allows information and technology leaders to triage and resolve IT incidents faster with workflow automation and on-call schedule management. IT Alerting provides critical risk management and peace of mind for the CIO through an end-to-end emergency response mechanism designed to initiate appropriate remediation actions as quickly as possible:

- Automate communication channels, collaboration tools, and orchestration response to minimize downtime
- Alert the right personnel and engage teams automatically without manual calls or emails
- Notify key stakeholders and impacted users and keep them updated with targeted notifications
- Maintain a full audit trail of the incident resolution.
- Maintain visibility to improve IT response performance and accountability over time
- Streamline incident response to accelerate resolution across all IT functional areas:

IT Ops

Service Ops

Sec Ops

Dev Ops

IT BC/DR

## YOUR ROLE IN CEM

Deploying an orchestrated, end-to-end enterprise incident response solution, inclusive of comprehensive IT alerting, allows executive leaders to understand more quickly the severity and context of each critical event.

For the CIO, this means the ability to assess the incident's likely impact on the organization and initiate the actions that will minimize downtime, operational disruption and revenue impact. Orchestrated incident management enables enterprises to utilize workflow templates to automate incident response for faster, better coordinated remediation.

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



Natural disaster / extreme weather (33%)



Executive protection threat (23%)



Theft of physical / intellectual property (28%)



Brand / reputational crises (23%)



IT failure of a business-critical system (25%)



Supply chain disruption (22%)



Cyberattack (24%)



Terrorism or acts of terror (14%)



Utility outage (24%)



Active shooter (11%)

IT systems failure is the third-most common critical event type faced by large enterprises.

Source: A commissioned study conducted by Forrester Consulting on behalf of Everbridge, September 2018





## CEM ADVANTAGES

# Benefits of a Unified Architecture for Emergency Response

Everbridge CEM offers enterprises the rare opportunity to improve operational efficiency while also strengthening their risk management posture. Consolidating business continuity, disaster recovery, active assailant, emergency response, natural disaster, IT incident risk management, and mass notification systems in one unified platform offers distinct advantages.

**Deploying an orchestrated, end-to-end enterprise incident response solution allows executive leaders to engage the right emergency response teams sooner, preserving business continuity, accelerating incident resolution and saving hundreds of thousands of dollars in cost avoidance.**

## CEM ADVANTAGES

### Tight integration of messaging solutions:

Rather than reacting to an emergent threat with siloed, fragmented actions based on partial information, emergency response teams base decisions on aggregated intelligence and respond within the structure of an easy-to-execute strategic plan that taps into Everbridge's integrated suite of emergency notification solutions:



#### Mass Notification

Keep everyone informed before, during and after critical events with targeted communications and workflow automation



#### Crisis Management

Orchestrate all crisis response activities, teams and resources while providing real-time visibility



#### Public Warning

Communicate with a region or area during critical events and threats without the need for user opt-in



#### IT Alerting

Assess and address incidents faster with workflow automation and on-call schedule management



## The Everbridge CEM Advantage

### Financial Services Provider

- ✓ 15x faster incident response
- ✓ Response Team mobilization time improved by 93 percent
- ✓ Hundreds of thousands of dollars saved per incident in cost avoidance

### Payments Processing Company

- ✓ 12x faster incident response
- ✓ Response Team mobilization time improved by 92 percent
- ✓ \$382,000 saved on average per incident in cost avoidance

## CEM ADVANTAGES

### Operational efficiency:

Consolidating emergency notification systems in a single unified architecture allows the enterprise to reduce its digital footprint. Embracing a unified architecture also eliminates the need for IT administrators to train on disparate messaging systems. These improvements add up to streamlined operations, freeing valuable resources for other purposes including strategic business initiatives.

### Single vendor relationship:

Consolidation reduces reliance on multiple vendors which eliminates the need to manage multiple contracts and varying service level agreements (SLAs) and reduces the points of failure inherent in integrations.

### Better business continuity and disaster recovery capabilities:

A faster, more comprehensive response to emergency situations is more likely to preserve business continuity and accelerate disaster recovery. In the case of the need for either, faster and better-coordinated action may protect the company from considerable financial harm.



## GETTING AN EDGE

# Critical Event Management as a Competitive Advantage

Enterprises today will likely suffer multiple critical events every year, resulting in consequential, unexpected costs to business, disruptions to operations, and real threats to their workforce, customers or suppliers. If you know you have the most comprehensive emergency response management platform supporting your business operations, you are in a stronger position to expand your enterprise's risk appetite, which can help you compete in your marketplace. Confidence in your emergency incident response platform gives you the peace of mind to focus on growing your business while Everbridge protects your base.



# How prepared is your organization for critical events?

## Get Your Personalized Organizational Resilience Maturity Report.

How effectively would your organization respond to critical events that threaten worker safety and business operations?

Get a detailed, personalized report on how your organizational resilience maturity scores against industry averages, complete with next steps on how you can improve your company's organizational resilience across multiple attributes.

Click [here](#) to run your own Organizational Resilience Self Assessment.



## 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 pandemics, 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, more than 5,000 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 2.8 billion messages in 2018 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 Australia, Sweden, the Netherlands, Singapore, Greece, 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®, Public Warning, Crisis Management, 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, 46 of the 50 busiest North American airports, 6 of the 10 largest global consulting firms, 6 of the 10 largest global auto makers, all 4 of the largest global accounting firms, 9 of the 10 largest U.S.-based health care providers, and 5 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, Bangalore, Kolkata, London, Munich, Oslo, Singapore, Stockholm and Tilburg. For more information, visit [www.everbridge.com](http://www.everbridge.com), read the company [blog](#), and follow on [LinkedIn](#), [Twitter](#), and [Facebook](#).