everbridge®

SURVEY RESULTS: CRITICAL EVENT MANAGEMENT IN FINANCIAL SERVICES

A Critical event is defined as when one or more incidents, for example, severe weather, crime, violence, critical equipment or technology failures, impact a business's assets – its employees, buildings, processes, operations, supply chains, or brand/reputation – resulting in revenue loss, cost increases, brand damage or concerns for health and safety. Several factors would suggest that critical events are occurring more frequently:

+ **Cyber: The number of cyber incidents jumps 1087%** reported by UK Financial Conduct Authority. Sharp increases were across several sectors including credit cards, banking, insurers, mutual funds, lending, pensions, and investment management.[1]
+ **Weather:** According to NOAA, over the last 5 years (2014-2018) there have been an average of 12.6 weather and climate disasters per year – more than double the average of 5.3 per year over the preceding 34 years from 1980-2013.[2]
+ **IT:** Money magazine reported that since April 2018, when banks were first required to report issues that may affect payment processing, banks reported 302 separate incidents, or more than one per day. The top two banks averaged one such incident per week.[3]

Because of these trends, companies invest significant resources into teams, technology and processes to protect their operations, brand and assets from critical events. However, despite this investment, companies struggle to optimize their Critical Event Management (CEM) operation, slowing down their ability to either avoid or mitigate the impacts of these events, increasing the losses to the business and the risks to human life and safety.

Everbridge commissioned Forrester Consulting to evaluate CEM Strategies. The results of the survey show that:

1. Critical events are a 'when', not an 'if'. 100% of the companies surveyed had suffered at least one critical event in the past 24 months, and on average, they suffered over four.
2. Critical events resulted in a "large" or "severe" impact in multiple areas, from people safety, to brand value and revenue, to operational efficiency and employee productivity.
3. While most companies had invested in tools and procedures to manage critical events, those that took a unified approach to CEM saw improved outcomes across the board from human safety to positive business outcomes.

The study consisted of 56 executive-level employees of a Financial Services Firm.

Report Demographics – Financial Services

LOCATION

All companies are based in the US or Canada.

OTHER OPERATIONS

Europe/Middle East: **48%**
Asia/Pacific: **45%**
LATAM: **38%**
Africa: **32%**

POSITION

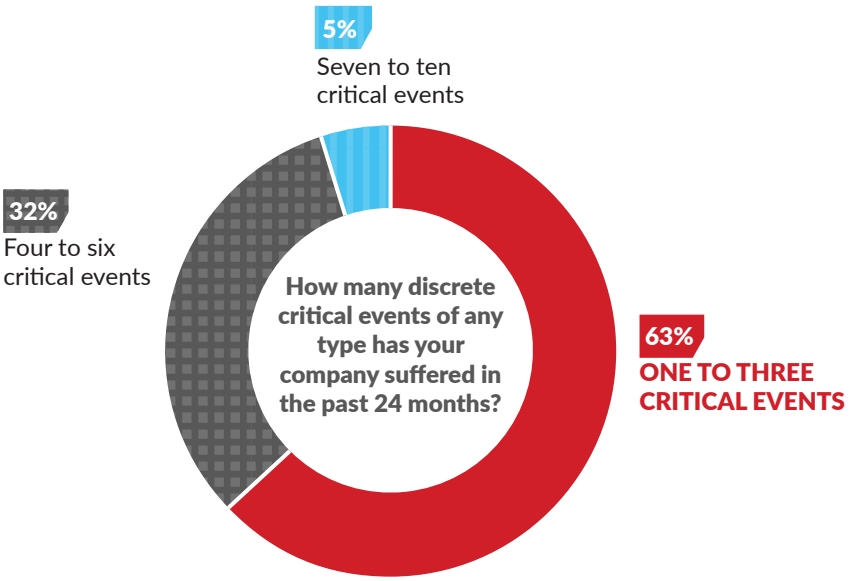
C-level: **12.5%**
VP: **12.5%**
Director: **75%**

REVENUE

$500M - $1B: **43%**
$1B - $5B: **41%**
$5B+: **16%**

CRITICAL EVENTS EXPERIENCED

Critical events are common, and they are basically inevitable. 100% of all respondents had suffered at least one critical event in the past 24 months, and the average number over that timeframe was four critical events. The types of critical events the companies experienced were widely varied and included events that impact business operations, business value, and life safety. Severe weather was the most common event, and while active shooter was the least common, it was still reported by 4 out of 56 companies to have occurred to them in the past 24 months. This highlights the need for companies to make sure that the firm covers a wide variety of potential events. It is not enough to have a 'weather' response and a 'cyber attack' response – business disruptions and threats come in many forms.



Survey Results: Critical Event Management in Financial Services

FROM WHICH OF THE FOLLOWING TYPES OF CRITICAL EVENTS HAS YOUR COMPANY SUFFERED IN THE PAST 24 MONTHS?

Natural disaster/ extreme weather
32%

Brand/reputational crises
29%

Executive protection threat
29%

Cyber Attack
27%

Supply Chain Disruption
27%

Ransom/Extortion
25%

Theft of physical/ intellectual property
25%

IT failure of a business critical system
23%

Terrorism or acts of terror
20%

Utility Outage
18%

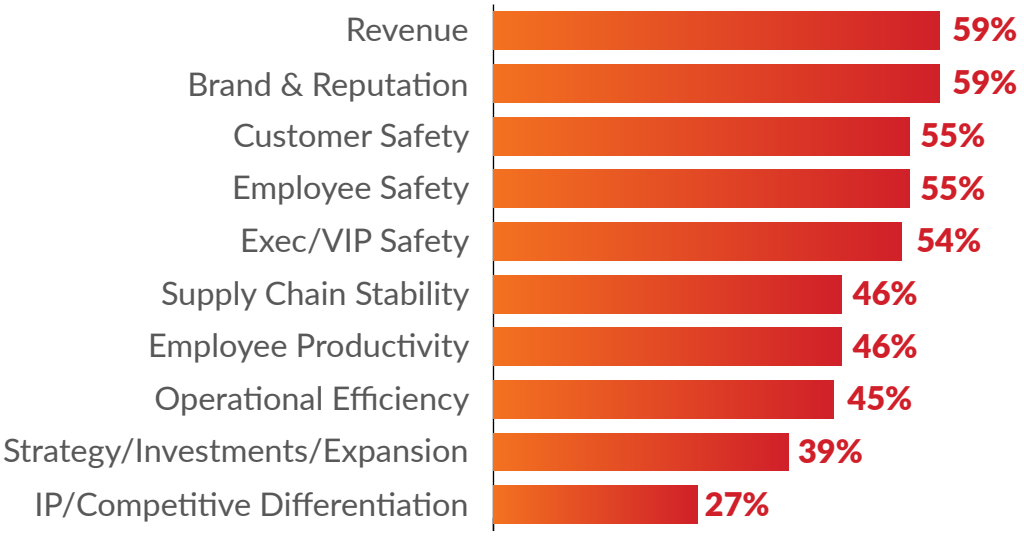
Geopolitical events/ social unrest
18%

Active shooter
7%

IMPACTS

Critical events result in significant impacts to both business operations and industry continuity. As companies design and implement their CEM teams and processes, they must consider customers, counterparties and investors. In addition, a single event will often have impacts across multiple areas of the business. Therefore, critical event management must account for all impacts – the response cannot be siloed into 'security', 'cyber response' or 'business continuity' only.

THINKING BACK TO THE CRITICAL EVENTS YOUR ORGANIZATION HAS FACED IN THE PAST 24 MONTHS, HOW SEVERE WAS THE IMPACT OVERALL IN EACH OF THE FOLLOWING CATEGORIES?



APPROACH

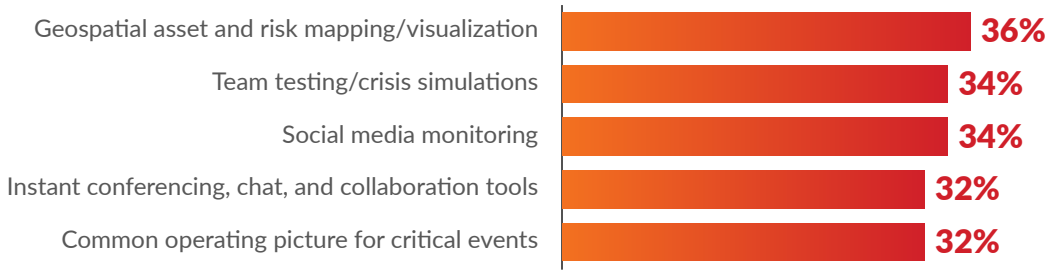
To try to mitigate against these impacts, companies have invested in teams, technologies and processes to address them. Companies reported being further along in some respects and lagging in others, overall, the industry is evolving capabilities at an even and consistent pace.

Two of the top five areas that companies reported being 'optimized' in: social media monitoring and having a common operating picture for managing critical events, also are in the top five areas companies 'needed improvement' in.

WHICH OF THE FOLLOWING STATEMENTS BEST REFLECTS THE CURRENT STATE OF YOUR COMPANY'S MATURITY OF CRITICAL EVENT RESPONSE/ REMEDIATION (REGARDING RELATED TOOLS AND PROCEDURES)?

Percent of companies that have *optimized* tools/procedures (top 5 shown)

Percent of companies *needing improvement* in tools/procedures (top 5 shown)

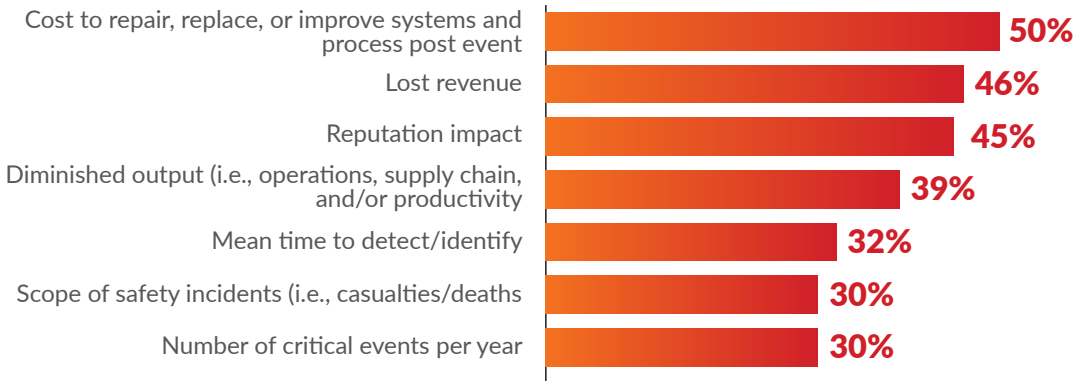


Interestingly, while a large percentage of respondents believed their current tools and procedures to be effective in reducing the time it takes to detect and respond to a critical event (between 82-89% across the different phases of managing the event), the majority of respondents do not actually track the metrics that would quantify this effectiveness. In fact, 88% of respondents believed themselves effective in reducing the time it takes to identify a critical event, yet only 32% actually measured that as a KPI.

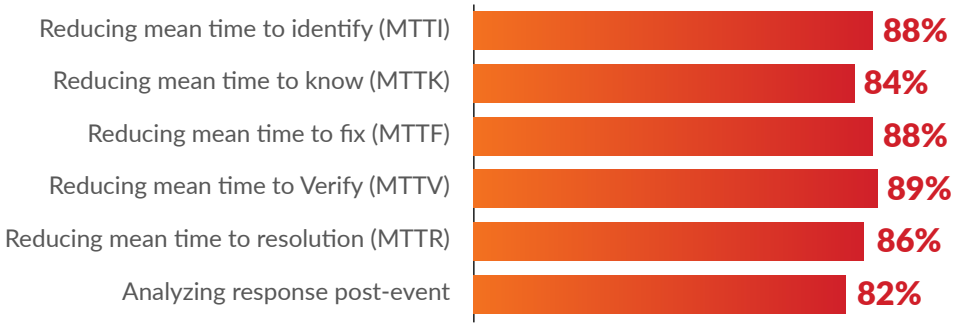
Companies know they need to effectively manage critical events, and they invest in people and technology to solve the problem. That investment leads them to believe they have addressed the issue effectively.

But many have not matured to the point where they are measuring the impact those investments are making on the operations – in other words, they feel like they are doing well, but they don't know. And of course, without knowing how they are doing at various aspects of managing critical events, they also don't know what they can do to improve.

WHICH, IF ANY, OF THE FOLLOWING METRICS DO YOU USE AS KEY PERFORMANCE/RISK INDICATORS TO TRACK YOUR CRITICAL EVENT RESPONSE EFFORTS?



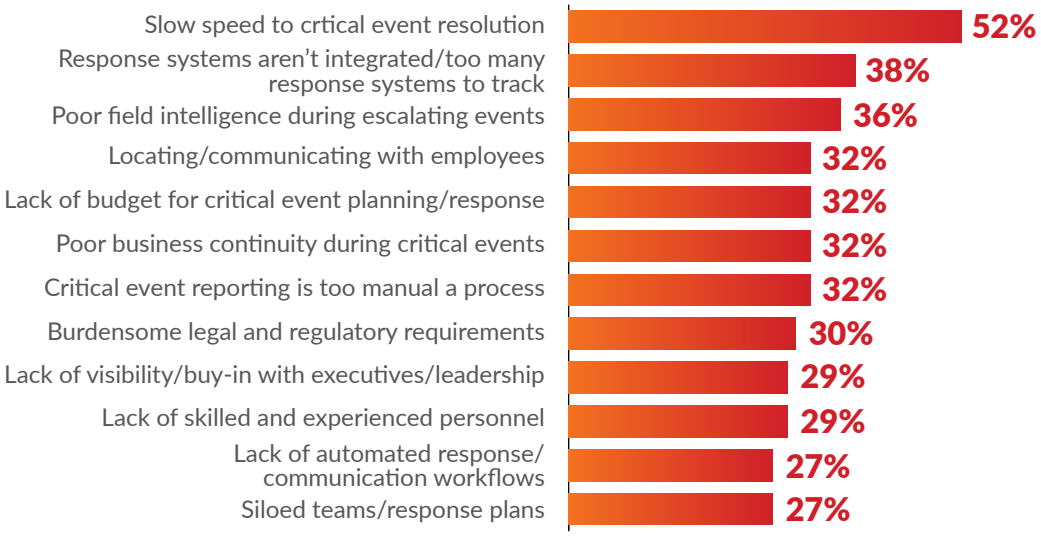
HOW EFFECTIVE ARE THE CRITICAL EVENT RESPONSE/REMEDIATION TOOLS AND PROCEDURES YOU CURRENTLY HAVE IMPLEMENTED IN THE FOLLOWING AREAS?



CHALLENGES

Unfortunately, even despite their investment, and in spite of their opinion on how effective those investments are, the companies in the study still suffer from challenges trying to manage critical events effectively. Over half believe their company suffers from the speed by which they manage critical events, with many citing issues like too many different response systems, lack of field intelligence during events, and challenges locating and communicating with employees as key reasons. And of course, as highlighted earlier, even with their investments, they are still suffering from an average of over four critical events every two years that are having large/severe impacts.

WHAT CHALLENGES DOES YOUR COMPANY EXPERIENCE IN PLANNING FOR OR RESPONDING TO CRITICAL EVENTS?



UNIFIED APPROACH

100% of respondents said they had either implemented, were in the process of implementing, or were planning to implement (in the next 12 months) a unified approach to critical event management.

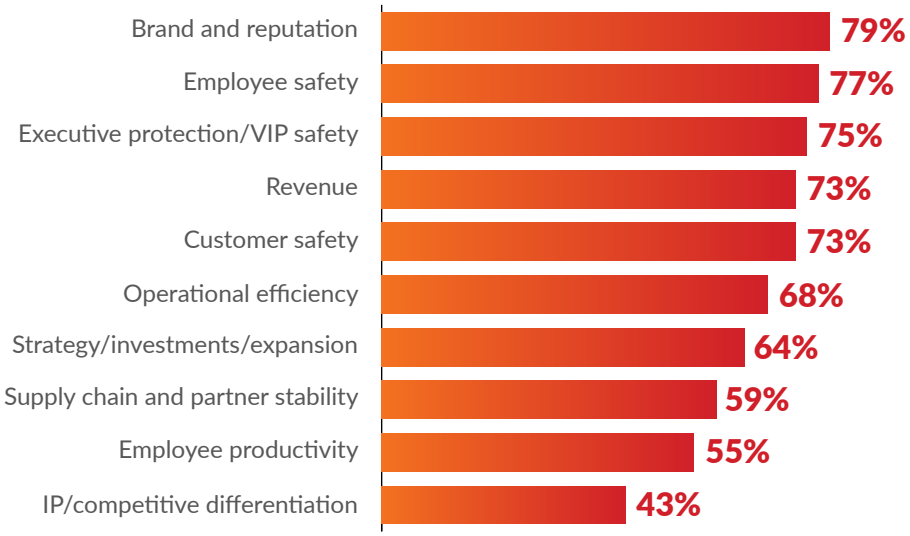
These companies either believe or have observed that a unified approach to managing critical events will improve many of the areas they currently struggle with. In fact, the challenge most commonly faced by the respondents, the overall slow speed to critical event resolution, was the factor expected to improve by the most companies when the new approach is implemented. That is why, in addition to investing in different areas of capabilities, companies are also implementing a unified approach to critical event management – merging the teams, processes and technologies responsible for managing a critical event together into a more cohesive unit with a common operating view and mission. This approach is sometimes implemented in the form of a 'fusion center', which typically refers to joining the teams responsible for cyber and physical security response. However, it need not be limited to those two categories. Operational Risk groups are quickly uniting the teams focused on business continuity, physical security, IT operations, cybersecurity, under one framework and risk methodology.

There are benefits to applying a consistent framework and process to the response for any unplanned disruptive event that has negative impacts on business operations. For example, while the response to a power outage at a bank, a large protest in front of a bank's headquarters, and a breach of the systems containing a bank's customer data will of course require different information sources to detect and different resources and steps to remediate – they all require a process of rapid detection and the ability to investigate and understand the issue. This includes identifying and communicating with the people that can address the issue, that need to be protected from the issue, and that need to be aware of the situation and possibly make decisions. They all might have indirect impacts in other parts of the business such as legal, finance and PR, and they can all be tracked and measured in terms of the timing and effectiveness of the response and the impact of the event. By combining the teams and tools used to manage these events, there are several benefits. The team sees more events as a group and can learn and improve through experience. A smaller number of tools can be used to manage the events, enabling more efficient and effective use of them. A consistent process can be applied to post-event analysis to enable more rigorous and better learning.

In many cases, one event may have impacts across several teams in an otherwise siloed environment and by managing the event through a single team and process, information can be better shared across the response.

WHAT ARE/WOULD BE THE BENEFITS OF A UNIFIED APPROACH TO CRITICAL EVENT MANAGEMENT? (TOP 10 SHOWN)

A UNIFIED APPROACH IS EXPECTED TO PROVIDE A POSITIVE IMPACT TO THE FOLLOWING CATEGORIES



CONCLUSION

Companies are on a journey away from a reactive and siloed response toward a unified approach, creating efficiency and expertise in their handling of incidents. Adopting a unified approach will not be enough, however. Companies must also quantify the success of their critical event management with KPIs measuring their abilities and the event's affect to their counterparties. Understanding near misses, tracking the impact of events and their frequency all contribute to a predictive organization. Seeking out best practices and establishing metrics and transparency to enable continuous improvement are the call to action.

[1] RPC, "Data breaches reported by financial services firms rise 480% in a year to 145" (26 Feb 2019). https://www.rpc.co.uk/press-and-media/data-breaches-reported-by-financial-services-firms-rise-480-percent-in-a-year-to-145/

[2] NOAA National Centers for Environmental Information (NCEI) U.S. Billion-Dollar Weather and Climate Disasters (2019). https://www.ncdc.noaa.gov/billions/

[3] Which? Money, Revealed: UK banks hit by major IT glitches every day (4 Mar 2019). https://www.which.co.uk/news/2019/03/revealed-uk-banks-hit-by-major-it-glitches-every-day/?wgu=5665_54264_15568899388918_8fde4974e2&wgexpiry=1564665938&utm_source=webgains&utm_medium=affiliates&utm_content=22278&source_code=314AGJ

ABOUT EVERBRIDGE

Everbridge (NASDAQ: EVBG)

We keep people safe, businesses running faster, and industries connected with sophisticated incident response and crisis management systems.

Over 4,600 global organizations, governments, corporations and regulators rely on the Everbridge Critical Event Management Platform to track relevant threats, visualize the impact to assets, and to deliver emergency notifications and crisis instructions as part of the operational resiliency plans of banks, clearing houses, regulators, capital market firms and insurance compaies.

The platform delivers on an unprecedented scale sending over 2.8 billion messages annually, with the ability to reach over 500 million people in more than 200 countries and territories, including entire mobile populations on a country-wide basis. The company's SaaS based service includes Mass Notification, Incident Management, Safety Connection™, IT Alerting, Visual Command Center®, Public Warning, Crisis Management, Community Engagement™ NC4 Risk Intelligence Feeds and Secure Messaging. With the acquisition of NC4, we now provide hyper-local and historical event risk intelligence.

Everbridge serves 8 of the 10 largest Investment Banks, 4 of the 5 largest Retail Banks as well as many Systematically Important Financial Firms, regulators and government agencies. The company is based in Boston and Los Angeles with additional offices in San Francisco, Lansing, Orlando, Beijing, London and Stockholm.

everbridge®

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