
Picture credit: Getty

# CRISIS MANAGEMENT

**Imad Mouline** *reports on the benefits of a consolidated view in an emergency for ports around the world*

**Businesses are under attack both literally and figuratively – whether it's man made events, natural disasters, supply chain disruptions, IT incidents or any other form of critical event. Today, many companies address both concerns within different departments and hope for the best. However, this type of siloed planning has proven to be largely reactionary and unable to keep pace with a fluid environment that requires both a physical and digital response. Any delay in response could result in millions lost to hackers or even fatalities. A centralised approach is necessary to properly plan, manage and remediate the modern crises that enterprises face every day.**

Likewise, on the employee safety side, the historic market for corporate security and safety solutions has been focused on establishing perimeters – locks, alarms and guards – to keep threats to employees outside of the physical premises. In reality, today's workforce is mobile—frequently remote, travelling and on the go. This article will highlight emerging trends and technologies that offer global organisations the ability to establish a common operating picture of the risk events, which can impact operations, and employee safety, at all times and in all locations.

Between rising security risks, civil unrest, natural disasters, supply chain disruptions, climate change, business application slowdowns, IT outages and unpredictable man-made threats, it's not a question of whether, but when, a serious security or performance issue with digital or physical infrastructure will endanger a port or the communities it serves. The results can be immediate and devastating.

Outcomes may include lost revenue, reduced employee productivity, regulatory fines, compensation pay outs and reduced customer satisfaction. In public safety terms, the stakes can literally mean life or death if the public and relevant supply chain partners aren't notified of an emergency evacuation.

**Ports have remote workers and contractors so need to be able to locate them quickly if a crisis occurs**

## RAPID RESPONSE

Many transportation hubs are being asked to respond more quickly and more decisively to critical events, with fewer resources. Yet, without an end-to-end process for dealing with critical events, it's nearly impossible to satisfy this mandate. They are often using manual processes and disjointed systems. As a result, they are unable to efficiently and effectively manage a crisis.

Security, operations and risk professionals are lacking the time needed to react or even avoid the negative consequences of these events. Simply put, the traditional method of managing critical events is outdated. What is needed is a holistic approach to critical event management that enables a more unified, efficient, distributed, automated and collaborative process.

The software tools used to manage operational risk, employee life safety and crisis management (continuity, IT operations, etc.) have started to move from reactive and compliance-driven technology solutions to more proactive, intelligence-based automation toolsets. These tools are designed to anticipate threats predictively to allow security, operations and risk professionals more time to respond to critical events, assess their aftermath or even head them off at the pass.

> **EACH CRITICAL EVENT CAN BE ANALYSED TO IMPROVE RESPONSE RATES TO DEVELOP BEST PRACTICES**

However, with the proliferation of these new technologies and new sources of information, such as social media, ports have struggled to support a unified, efficient, distributed, automated and collaborative process for managing critical events. Confounding matters, many organisations find themselves tasked with maintaining multiple, separate emergency, security and IT command centres that each require 24/7 availability and utilise a different set of siloed tools and processes to monitor and triage threats.

What makes more sense is to empower organisations like port authorities with a holistic approach to crisis management – or, the emerging industry term, critical event management (CEM). The term speaks to the reality that everyone faces today; employees and other stakeholders need to be kept safe and the business needs to keep running in the face of global or local crisis events.

Organisations that build and execute a CEM strategy can dynamically assess, respond to and manage the resolution of the wide range of threats and disruptions, which impact daily operations. CEM helps to improve response time, minimise disruption and attain better management control in handling critical events.

There are several specific functions where CEM helps those with responsibility for IT, business continuity and physical security to gather information and make the right decisions during a crisis:

- **Assess the impact of the event quickly**

The key to executing an appropriate response to a crisis is knowing what is going on. Critical events are confusing and chaotic. Organisations can't begin to remediate a situation until they know precisely what is happening and where the event is taking place. For instance, a cyber attack carried out online versus a person in the port operations server room downloading information on site.

Leveraging a more integrated operational approach in lieu of the disparate systems used today allows ports to better assess what is happening in their operational offices, or near their staff working on the ground. By integrating physical and digital tools, such as front line, social, trusted threat and weather intelligence, ports have an end-to-end view of a situation including operational impact, safety risks and response status information.

- **Locate employees in harm's way**

The fluidity of the modern workplace is a major challenge for businesses, but this is even more of an issue for port operators. Not only are people moving between different locations, many ports also have remote workers and contractors so they need to be able to locate workers quickly if a crisis occurs, particularly if they are a part of the response team. Aggregating data across multiple location-based systems – including building Wi-fi and access controls, travel management systems and mobile phones – allows for dynamic location tracking and alerting of impacted personnel, response team members and key stakeholders. This includes employees, executives, emergency responders, boards of directors and others who require detailed information of the response effort.

- **Being able to access the right information at the right time**

It's not enough just to know where people are, however. CEM systems enable IT and security teams to be able to communicate with them. Linking access control and badging systems, biometric systems and Wi-fi access points provide information on an employee's whereabouts and empower security personnel to communicate specific directives – including site evacuation directions – to people directly. This benefit can serve as the difference between life and death in some situations.

Active shooter responses are heavily influenced by location. If an assailant is on the third floor of a specific building, for example, CEM enables security teams to alert everyone in the surrounding area to evacuate. People located on nearby floors may even be directed to hide or prepare to fight (following the 'run, hide, fight' emergency response standard). CEM allows law enforcement to effectively manage the situation to keep people safe and out of the way until the threat has been remediated.

### • Analyse the aftermath

Once a critical event is over, benchmarks related to a port's notification responses and incident time to resolution can be recorded, measured and assessed. Each critical event can be analysed to identify which tasks took too long or what resources were missing to improve response rates and develop best practices for the next major incident.

## REDUCING THE IMPACT

Continuously looking for ways to better prepare and respond to critical events will not only improve performance when similar events occur again, but will also improve response effectiveness when unforeseen events strike. With the right historical data, ports can start to predict the right response resources, protocols and activities to reduce the impact.

When a crisis occurs, it's much better to be in the driver's seat executing pre-planned strategies to quickly reach a positive resolution. CEM's ability to combine physical and cyber security policies and technologies enables ports to develop a common operating picture of a situation and implement an effective resolution plan complete with pre-defined communication paths to senior management, on-site and remote workers, customers and any other affected parties. Current processes favour redundant tools over results. It's time for ports to integrate physical and cyber security functions to deliver better outcomes when a critical event takes place ●

**THE TRADITIONAL METHOD OF MANAGING CRITICAL EVENTS HAS QUICKLY BECOME OUTDATED**

**CHANGING ENVIRONMENT**

**The role and expectations of security operations are undergoing a dramatic change in today's increasingly unpredictable world. There is a greater sensitivity to the potential of a violent incident happening at work or in a public space, and most organisations are looking for ways to continue with business as usual, but still feel secure. Security operations are a strategic asset that provides organisational resilience for not only the people and the infrastructure, but also the overall business objectives.**

**Incidents we once thought unlikely in the UK are now increasingly commonplace. Our response to this, the way that we communicate and the speed with which we can locate and make safe anyone involved will make the difference between success or failure, and in some cases life or death. This requires a nimble, agile approach and a willingness to take a fresh and analytical look at how we have handled critical events in the past.**

**Forrester research reports that organisations with a unified approach to critical event management have been able to minimise the impact of critical events, to a moderate or high degree, in the areas of revenue protection, customer safety, brand and reputation and employee safety.**

**Imad Mouline** is the chief technology officer for Everbridge and is responsible for market strategy, product roadmap, innovation, and research and development. Mouline is a graduate of the Massachusetts Institute of Technology, and has been awarded five US patents.

**The key to executing an appropriate response to a crisis is knowing precisely what is going on**


Picture credit: Getty