Why Your Business Needs A Holistic Approach To Managing Critical Events

Published on 4 Aug 2017

In today’s world, businesses face a growing threat landscape. Looking back on just the past few months, there have been increased incidents of workplace violence (e.g. the recent New York city hospital shooting), terrorist activities (e.g. London Bridge attack, Manchester attack), and cyberattacks (e.g. Petya and WannaCry). While critical events have become more frequent, more complex, and costly to businesses, organizations’ emergency communications systems, plans and processes have remained surprisingly siloed and constrained by an inability to holistically manage the lifecycle of a critical event—from assessment, to communication, to analysis.

The reality is that organizations today find themselves tasked with maintaining multiple, separate
emergency, security, and IT command centers that each require 24x7 availability and utilize a different set of siloed tools and processes to monitor and triage threats.

**Situational Awareness For The Modern Workplace**

Siloed processes aren’t desirable because they result in individual departments conducting their own threat assessment, which can lead to inconsistent responses to critical events. Without situational awareness, response to operational risks is delayed, leaving an organization’s employees, facilities, travelers, and other critical assets vulnerable.

The fluidity of the modern workplace is also a challenge for businesses. With 72 percent of workers projected to be mobile by 2020, and spending significant time away from a traditional office facility, locating and protecting workers, sharing critical information and directives, and activating the right responders becomes an even more complicated task. For example, it can take hours – and even days – for companies to determine if all their people, including traveling and remote employees, are safe after a terrorist event.

The bottom line is that the way current event management processes are set up is inefficient, ineffective, and – most importantly – can severely impact employee safety while also harming business operations.

**Centralized Incident Management**

To better communicate with their people and protect them from harm, organizations must adopt a holistic approach to critical event management inclusive of crisis communications and incident management. This includes consolidating physical and digital tools that are traditionally siloed under multiple disciplines and operations centers. Combining these functions enables organizations to develop a common operating picture of a situation and implement an effective resolution plan complete with predefined communication paths to senior management, on-site and remote workers, customers and any other effected parties.
Having a single platform that combines employee safety capabilities with threat assessment and visualization capabilities allows organizations to better manage the full array of intelligence, coordination, collaboration, and execution required to speed response times, reduce risk, and, above all, keep their employees safe in any critical event.

How Security Teams Can Manage Critical Events

With a consolidated Critical Event Management platform, security teams within an organization can dynamically do the following to keep their people safe and the business running effectively:

1. Assess critical events

Leveraging a more integrated operational approach in lieu of the disparate systems used today allows organizations to better assess what is happening in their offices, on their campuses, or near their traveling and remote employees. By integrating physical and digital tools, such as front line, social, trusted threat, and weather intelligence, organizations have an end-to-end view integrating threats, operational impact, and response status information on a “single pane of glass.” When all information is housed in a centralized location, it is far more effective and efficient for an organization to determine the likelihood, severity, and impact of a specific event on its people.
Linking access control and badging systems, biometric systems, and Wi-Fi access points provide information on an employee’s static, last known, or expected location.

2. Locate employees in harm’s way and communicate in a timely manner

The increasing regularity of critical events worldwide necessitates the need to locate and alert employees of any nearby risks at a moment’s notice. Organizations need to first identify who is in harm’s way, and then notify those affected on what action to take. Aggregating data across multiple systems 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.

For example, linking access control and badging systems, biometric systems, and Wi-Fi access points provide information on an employee’s static, last known, or expected location to a master database that an organization’s security personnel can use for triggering automated incident communication. This information allows security teams to provide critical information – including site evacuation directions – while an event is occurring to ensure the safety of employees based on their
targeted geographic region (e.g. a specific building, floor, neighborhood or zip code) and coordinate the efforts of responders.

If an active shooter is seen approaching from the western half of an organization’s campus, for example, the targeted alert may tell all employees on east campus to get off the property and go across the street, while all employees on west campus may be told to barricade themselves behind locked doors, as they might not have time to run. Visitors who are expected to arrive on campus later that day would be warned to stay away until police secure the premises.

With a centralized system that houses all location information and communication processes, the right messages will be sent to the right people in a matter of seconds.

3. Identify decision makers and automate action

A huge part in managing a crisis is not only identifying who is in danger, but who can help, and how. This process needs to be as streamlined as possible so there’s no question about who should be contacted and who is responsible for doing what. Leveraging an integrated critical event management system in which all information is centrally located allows organizations to initiate instant communications that share all relevant information and status updates with key stakeholders – there’s no confusion as to who should send out the communications, and no one is waiting on important information that is essential to convey.

Each critical event can be analyzed to identify which tasks took too long or what resources were missing

In addition to identifying team members who need to act, an integrated system distributes targeted alerts based on specific scenarios. Taking the same active shooter scenario, an organization’s security team can share incident details, collaborate with, and activate separate response teams, such as the police, SWAT team, and emergency responders, in a single platform – all while following standard operating procedures, escalation policies, and best practices for responding to
that particular event.

4. Analyze the aftermath

Once a critical event is over, benchmarks related to an organization’s notification responses and incident time-to-resolution can be recorded, measured and assessed. Each critical event can be analyzed to identify which tasks took too long or what resources were missing in order to learn from and improve response rates for the next major incident.

**Critical events should be managed as any major business function**—through a single process with clear lines of responsibility, common situational understanding, accountability, and visibility of performance. Currently, processes are focused on the use of too many overlapping tools which only create noise and impedes an organization from following a prescribed procedure for assessing and resolving threats. It’s time for all organizations to take a careful look at how they approach critical event management and opt instead for a centralized system that offers a holistic view – siloed processes are simply no longer effective in today’s threat landscape.

Author Profile
Cloud Video, Predictive Maintenance & Emergency Preparedness Top Secur...

Three key trends will continue dominating the security industry looking ahead to 2017 – cloud video, predictive maintenance and emerge...

Building Advanced Connected Solutions For Modern Security Threats

Did you hear the one about the bear that nearly caused a nuclear catastrophe? It was around midnight on October 25 1962, in the mi...

2020 Vision: Guide To Protecting Schools From The Threat Of Terrorism

It seems schools still need to be alert when it comes to the risk of terrorism. Following a recent security threat, Bury College has set an...