The Business Evolution: From Incident Management to Critical Event Management

Managing Critical Events as an Integrated Process to Mitigate Cost and Risk

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper

October 2017

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

The Business Evolution: From Incident Management to Critical Event Management

Table of Contents

©2017 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

The Business Evolution: From Incident Management to Critical Event Management

Executive Summary

In the modern era of specialization, the creation of organizational and technological silos is a natural outcome for large organizations. Such silos serve an important function in enabling faster problem resolution by quickly and easily applying the right set of skills, processes, and technologies to the specific problem at hand. Within IT, incident management and incident response evolved out of such silos, and for the most part remain somewhat narrowly focused on tools and processes used to resolve a single IT incident at a time–most often centered around a trouble ticketing-type system.

As enterprises face an increase in the number and variety of risks (both physical- and technology-focused), a more integrated and holistic response is becoming paramount. Overlapping and unconnected tools, data streams, interfaces, and teams can slow an organization's response to a critical event when minutes count.

An increase in the number and variety of risks (both physical- and technology-focused) requires a more integrated response.

The increasing maturity of Critical Event Management (CEM) systems that centralize a range of data feeds and enable fast communication among key participants can help bring about a more integrated response to emergencies such as severe weather, workplace violence, terrorism, and IT incidents. Such systems should be architected to support a variety of activities, including the ability to assess, locate, act, analyze, visualize, and orchestrate, communicate, and collaborate. Common use cases span incident management, IT alerting, safety, and managing supply chain disruptions.

Incident Management, Incident Response, and Critical Event Management: Reimagining Operational Risk Management

Information security incidents such as a ransomware or other cybersecurity attacks can cause significant disruption and business losses, and such incidents are receiving an increasing amount of press coverage. However, they are just one type of incident that can have a major negative impact on an organization. In today's modern business environment, global organizations face increased incidents of supply chain disruption due to severe weather, brand reputation attacks in social media, product quality issues, workplace violence, and terrorist activities. These unplanned, critical events require organizations to expand their view beyond the IT-centric definition of incident management. Negative events that impact the organization's operations, executive management, legal standing, the safety of employees, and customers' perception of the company can ultimately reduce productivity, efficiency, employee morale, and revenue, and damage the company's reputation in the market.

Today, most organizations treat the management of IT incidents as a process. Incident management follows protocols such as ITIL to restore a normal service operation as quickly as possible following an unplanned interruption to an IT service or a reduction in the quality of an IT service.[1] Incident response is an organized process to manage the consequences of a data breach, cyber attack, or other incident in a way that limits damage and reduces recovery time and costs. It is based on a response plan that defines what constitutes an incident and provides step-by-step procedures for each incident defined. Tools such as Information Technology Service Management (ITSM) software (e.g., ServiceNow and BMC Remedy) have been widely adopted and integrated with other systems to manage problem resolution. This same discipline needs to be applied to managing the broader array of critical events.

[1] International Organization for Standardization, "Part 1: Service Management System Requirements." ISO/IEC 20000-1:2011

©2017 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Most enterprises are at a relatively immature state in managing critical events. EMA research found that the majority of organizations still take a more reactive, ad hoc approach toward applying incident management and response beyond IT. Response activities tend to be highly compartmentalized, with few organizations having overarching programs designed to efficiently marshal the resources necessary to address defined incidents. This deficiency means organizations lack adequate visibility on the scope and status of resolution, or the ability to apply appropriate feedback for improved performance management. However, the growing number of organizations already able to coordinate response efforts broadly leverage it as a means to improve business performance, the safety of employees, and even identify sources of revenue enhancement.

Resolution of critical events is also a fairly immature function for most enterprises today. The use of separate and potentially overlapping tools, data kept in separate silos, and uncoordinated groups responsible for different tasks can take a toll on an organization's ability to effectively manage emergencies. Such factors increase response time and event handling costs, which can ultimately lead to greater financial losses due to missed business opportunities and increased operational costs.

While critical events have become more frequent, complex, and costly for enterprises, companies still find themselves with separate emergency, security, and IT command centers that each require 24x7 availability and use a different set of siloed tools and processes for incident management and response. Decentralized organizations face an additional challenge in responding to critical events because of a lack of understanding across the organization of the actual risks to their people, assets, and operations. They also lack visibility into what actions have been taken and their status. Gaining a common operating view across departments and through executive ranks is key to implementing a coordinated response supported by appropriate decision making.

As critical events escalate and impact a larger number of organizations, breaking down such silos and integrating overlapping tools and separate data streams is becoming an important requirement for successfully responding to all threats, whether physical or technological.

A New Operational Approach to Managing Incidents and Risks

Critical Event Management takes a broader view of potential risks and delivers a framework to help prepare for a variety of scenarios.

Critical Event Management takes a broader view of potential risks to the organization and delivers a framework to help those organizations prepare for a range of different scenarios. EMA defines CEM as a preplanned, organized method of rapidly and effectively responding to any type of crisis, whether it involves a terrorist attack, natural disaster, cyber-attack, or major IT outage, industrial accident, or other type of emergency. CEM aligns all the resources necessary to manage the organization's response to the event and enables alerts if threats intersect with the location of a company's employees, assets, facilities, and supply routes. It also manages interactions among participants with different roles, unifies processes, automates communication with various stakeholders, and facilitates post-event analysis to identify bottlenecks and improve future performance. Such stakeholders can include executive management teams, legal, facilities, IT, environmental health and safety professionals, customer support, and security groups, as well as external partners such as supply chain partners or emergency responders.

©2017 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

In order to understand the difference in scope between incident response (IR), incident management (IM), and Critical Event Management (CEM), it helps to think of the three as a stacked pyramid, with IR at the narrow top, IM in the middle, and CEM making up the larger base portion of the pyramid. Incident response, more often than not, is more technically focused on tools and processes used to resolve a single IT incident at a time. IR is typically centered on a trouble ticketing-type system. Depending on the perceived source of the incident, whether it is a system outage or cyber attack, the incident identification and resolution are carried out by separate teams within IT and with little coordination with other groups. Incident management brings more programmatic discipline to the task, but is still fairly limited in its scope and application. For the most part, both IR and IM remain within the confines of the IT department. The silo may be bigger, but it is still just the IT silo.

Figure 1

Against this backdrop, the modern business environment is characterized by a need for speed in order to respond to rapidly-evolving market requirements. However, for organizations that expanded through merger and acquisition activities, there exists a tremendous amount of overlap in tools, technology, and business processes that can act as a speedbump. Enterprises of all stripes are responding by consolidating their operations in order to increase efficiencies. To do this effectively, the business as a whole must consolidate tools and processes in order to meet the need to accelerate and reduce costs.

Developing a common operating view across different groups responsible for replying to a range of different threats is essential for CEM. It is paramount for organizations with decentralized operations. Such a view allows the people and processes directly responsible for evaluating the threats to rapidly execute a plan to contain or eliminate the threat's potential impact on the company and its supply chain partners, customers, and other key stakeholders.

©2017 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Within a large enterprise, determining which group owns overall responsibility for coordinating a Critical Event Management program could be a matter of debate. A corporate security executive at one large oil and gas industry system provider using CEM software from Everbridge found that its security operations center was the best fit for overall crisis management. At the same time, it's important that different business units have the ability to manage their own process in an emergency. That ability to segment a crisis response helps to ensure continuity of operations in other parts of the company.

Creating a Critical Event Management Architecture

Any architectural design for a CEM system that addresses more than just critical IT events must take into account the need to create processes that operate across the organization, and enable communications and management across different departments and business units. To be truly effective across a range of incident types, it must not only encompass IT and line of business participants, but also executive management, legal, law enforcement, and other first responders, suppliers, vendors, partners, and customers.

A Critical Event Management architecture must encompass IT, line of business, and other participants.

The operational components of such a system include a range of activities, including the ability to assess, locate, act, analyze, visualize, and orchestrate, communicate, and collaborate.

Assess: What is actually taking place in the incident and what is its impact? This includes gathering threat data and contextual information needed to assess the magnitude of a risk from a range of sources including threat intelligence feeds, IT system intelligence, public safety information, weather status and forecast, social media information, and in the case of a physical threat, data from the location of the threat.

Locate: This includes not only those who could be in harm's way, but also preassigned employees who can help resolve the particular event at hand and any key stakeholders affected by that event.

Act: This component automates the appropriate incident response, including standard operating procedures, escalation policies, best practices, and response team and device activations.

Analyze: This provides key performance indicators of the operational response to an incident, including benchmarks, team performance, post-action reports, and notification analysis. It answers questions about which resources were missing and which tasks took too long. Those answers can then be used to identify bottlenecks and improve future assessments of the impact of threats.

Visualize and Orchestrate: This component includes the creation of a critical event collaboration center that provides multiple views of the event through a common interface and mechanism to coordinate response teams.

Communicate and Collaborate: This element lets employees know what they should do and keeps key stakeholders informed.

The technology foundation for a CEM platform requires the integration of multiple functions, including a rules and policy engine, external event ingestion, location awareness, a notification engine, a contacts database, and open API for integration with other control, notification, and alerting systems. In addition, the critical nature of the system requires that redundancy be built into the system to ensure high availability. Redundancy should span data centers, communications providers, network operations centers, and access points. Redundancy also applies to people.

©2017 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

Common Use Cases

Incident Management

Incident management can help organizations achieve the most mature stage of development for use cases. That stage, defined by EMA as the dynamic incident response capability, is characterized by a high degree of automation that draws on multiple integrated systems, workflows, and communications functions. As more devices become connected to the Internet, incident management can also be expanded to incorporate IoT devices. For example, IM can be used to enable a connected sensor to communicate about a server room becoming too hot and trigger an automated response to that condition before it causes an outage. Dynamic incident response enables the alignment of cultures and goals between IT and the business, and the use of contextually-driven analytics resources allows IT to be a business enabler to the enterprise. As such, incident management and response can be delivered by IT as a service to any line of business or other groups within the organization.

IT Alerting

All IT organizations face the prospect of an unplanned outage that has the potential to disrupt the business, especially as attacks such as Distributed Denial of Service or ransomware campaigns affect more organizations. Time to response and resolution is critical. The ability to automate the process of notifying the right people and teams responsible for responding to any given outage can greatly reduce resolution time and help ensure service-level agreements are met. An automated response process can involve not only IT operations, network operations, and the security team, but also DevOps and storage. To be effective, alerting must be able to target notifications–sometimes across different time zones–to identify and contact the right response team members using multiple communications methods. Integration with trouble ticketing systems, such as BMC's Remedy, can streamline the incident management workflow.

Safety

Ensuring the physical safety and protection of employees, especially field service personnel and traveling executives, is another common use case for CEM systems, especially among highly distributed, global enterprises. By combining the ability to track dynamic employee locations with a mass notification system, enterprises can contact employees on their device of choice and give them information to help ensure their safety during location-based emergencies. Organizations can also send messages to employees in specific locations that are tailored to the specific incident (e.g., a terrorist attack) and provide traveling employees with mobile SOS applications. The ability to quickly communicate with the right employees, whether they are home or traveling, is crucial in this use case. It is one of the most important benefits that the Everbridge oil and gas industry customer achieved with the CEM tool.

Supply Chain

Severe weather, refrigeration, outages, unplanned IT system outages, and other events can disrupt supply chains and challenge the ability of retailers to keep store shelves stocked or keep work-in-process goods from reaching factories to maintain production. CEM systems can integrate weather, threat, and sensor data feeds to help enterprises understand risks to their supply chain routes and assets, and to know when shipments need to be rerouted to assure supply. By graphically depicting risks and their proximity to partners and assets, and by incorporating data such as the wind direction of storms, CEM systems give enterprises more time to plan their response and take proactive steps to mitigate risks.

©2017 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

EMA Perspective

Enterprise CSOs and COOs understand that their organization is constantly under attack, but they can never predict when or if an attack will deal a business-disrupting blow to their defenses. At the same time, executives never know if or when a physical emergency–whether it is a terrorist attack, natural disaster, industrial accident, or supply chain disruption–will put information resources, employees, and other key stakeholders in harm's way. As enterprises face the prospect of dealing with a growing range of threats, they should prepare to formalize and consolidate their operational response to a wider variety of threats.

Executives never know when or if a physical emergency will put information resources, employees or other key stakeholders at risk.

A CEM system like Everbridge's enables customers to integrate and consolidate disparate tools to deliver the right information at the right time to the right individuals, so the incident response team can make the best possible decisions to manage a crisis. It is designed to help visualize threats, coordinate the appropriate resources, and manage the crisis management process for any size or type of event. It also enables incident response teams to operate more efficiently and communicate more effectively to reduce the impact duration of a critical event, limit business disruption, and ultimately protect employee safety and company brand reputation.

Having a single tool with a consolidated view and a streamlined interface can reduce errors and potentially save lives, according to one Everbridge customer. At the same time, being able to audit response rates enables greater fine tuning of the system to improve event handling in the future.

©2017 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2017 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3633.102417