BlackBerry Intelligent Security. Everywhere.

CRITICAL EVENT MANAGEMENT

GUIDE TO EMERGENCY PLANNING

HOW TO

Organizations of all types and sizes face the risk of critical events such as a flood in an office building, a cyberattack that targets infrastructure, a hurricane, a pandemic and the like. Whether an event merely disrupts business or threatens life, the risk is always present. A critical event could occur at any moment.

Consequently, planning to help ensure a timely, well-informed response is essential because neither customers nor the public have patience for corporate stumbles and public safety finger-pointing. They expect accurate communications, a well-coordinated response and complete transparency.

Even if your organization has some preparation, you can improve the response by enhancing command and control systems and ensuring the organization can reach and communicate with all stakeholders, gather and act on real-time information and eliminate inefficient processes and outdated technology.

EIGHT ELEMENTS TO A BETTER EMERGENCY PLAN

As you engage in emergency planning, above all, ensure your plan prepares your organization to prepare, respond, recover and improve your response over time. Consider the following:

LIKELY THREATS

ACCOUNTING FOR EVERYONE

THREAT INTELLIGENCE & PUBLIC SAFETY ALERTS

COLLABORATION WITH EXTERNAL ORGANIZATIONS

ACTION PLANS

REAL-TIME INFORMATION

NOTIFICATION & RESPONSE

TRAINING & TESTING

STEP #1:

IDENTIFY POTENTIAL THREATS

Your first step is to identify the most likely types of threats your organization could face. A school or government agency faces threats that differ dramatically from those of an oil refinery or corporate campus. Threats such as extreme weather and fire, by contrast, are common across all types of organizations. You should also consider emerging threats, including ransomware and other types of cyberattacks.

Keep in mind that no two critical events are the same—every incident or emergency has unique elements. However, preparing clearly defined job roles and processes for notification and response can dramatically reduce your risk.

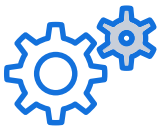
STEP #2:

ACCESS THIRD-PARTY THREAT INTELLIGENCE

Consider how to identify the presence or forecast of threats more quickly. Threat intelligence, public safety alerts and other sources of third-party data can identify many types of threats and hazards before you can. The integration of such external data sources with your enterprise systems enables a faster, more informed response.

Threats are dynamic.

Emergency plans and technology for notification and incident response must be flexible enough to implement modifications on the fly.



Automate when possible.

For example, integrate real-time cyberthreat intelligence with an enterprise IT ticketing system, such as ServiceNow®, to trigger a faster IT response.

STEP #3:

CREATE DETAILED ACTION PLANS

Draft response plans for the most likely threats such as the accidental activation of a fire sprinkler pipe overnight, which causes flooding. You can quickly activate a predefined action plan with notification and incident response technology.

1. Connected sensors notify the facility (or office) manager of the incident.
2. After verifying the incident, the facility manager sends an alert to targeted senior leaders via email, text and phone to inform them of the situation and the actions taken to resolve it. The facility manager requests approval to activate the organization's business continuity plan (BCP) and receives a response in minutes.
3. The facility manager swiftly sends another alert with two-way capability—this one by email and text to explain the situation to all staff and in-house vendors. The alert also requests that all recipients confirm their status by responding.
4. The incident response team escalates the incident and collaborates in real time with the local fire department and sprinkler system service vendor.
5. The facility manager periodically sends alerts by email and text to the leadership team and all employees and partners with updates on the situation and expected time of resolution.
6. Once the situation is resolved, the facility manager sends a final alert to notify individuals that it is safe to re-enter the building.

STEP #4:

STREAMLINE NOTIFICATIONS

How will you reach everyone quickly? It's a big challenge. Keep in mind that contact details change, and people use and respond to different devices. Integrations with Workday® and Microsoft® Active Directory® help ensure you have access to up-to-date contact information for those you target.

With contact details ready, you can alert everyone or targeted groups on any device with one click. Static and dynamic groups—based on organization structure, role, location, geography and many more defined criteria—enable you to send alerts en masse or to specific individuals. Predefined message templates for a multitude of critical events speed communications and overall response times.

INTEGRATE ALERT SYSTEMS.

Notifications must go out fast and often broadly. Integrate an alert system incorporating external sensors and data sources, such as fire alarms and the National Weather Service, to trigger notifications automatically for specific conditions on personal devices, social media and broadcast devices such as display boards.

CRITICAL EVENT MANAGEMENT

Comprehensive emergency planning supported by critical event management (CEM) technology can mitigate negative impacts on your people, your organization's assets and your operations:

- *Reduces response times and costs with more centralized plan management*
- *Increases user adoption with improved plan awareness*
- *Empowers teams to collaborate with secure instant messaging*
- *Improves situational awareness with a centralized view of the response operation*

STEP #5:

ESTABLISH A SYSTEM TO ACCOUNT FOR ALL PERSONNEL

Create a system that enables you to know everyone's location and access their safety status when a critical event occurs. This include all employees and contractors, whether working on-site, in the field or remotely. By automating this task to immediately assess the status of individuals, groups or the entire workforce, you can save valuable time.

STEP #6:

PREPARE TO COLLABORATE WITH EXTERNAL ORGANIZATIONS

Make sure you can collaborate with partners. Critical events frequently cross organizational boundaries, so a seamless incident response requires secure collaboration between multiple entities, including facility management, governmental agencies, regulators, first responders, staff and affected customers.

Collaborate securely by ensuring your incident response technology enables you to "invite" external groups to join a secure communications network to manage the critical event cooperatively. Multiple delivery channels broaden participation and provide flexibility. Once the emergency is resolved, an archive of the securely communicated chat maintains transparency.

ACCOUNT FOR EVERYONE.

When the status of all personnel is collected in a centralized dashboard, you know who is accounted for and who is missing. Managers can quickly identify who may be available to take on an emergency assignment, and if a given individual fails to respond to a request, the next available person is contacted automatically. Individuals can check in and check out or turn on tracking so their status stays current.

SECURITY REQUIREMENTS.

Security requirements and compliance mandates to protect personally identifiable information (PII) apply even during a critical event. Encrypted real-time chat via a mobile app maintains privacy and confidentiality.

STEP #7:

ARRANGE TO COLLECT REAL-TIME INFORMATION

Take advantage of all the information available to your response team. Real-time information from eyewitnesses and primary sources helps lead to faster resolution of a critical event. Employees in the field become the eyes and ears of the organization by providing firsthand information that helps resolve the situation more quickly.

STEP #8:

TRAIN AND TEST

Find ways to raise awareness of emergency management plans through training and testing. The more your organization practices, the better the response will be when a critical event occurs because everyone will be familiar with the plan and technology. Use tabletop exercises, drills and simulations. Always collect and analyze data in reports after the test and use them to improve your response.

GPS LOCATION TRACKING.

GPS-enabled location tracking, known as geo-tracking, enhances situational awareness in several ways. With source, type and location data appended to incoming information, responders can visualize the scene and make better decisions. Any individual who feels endangered can use a “track me” feature to alert responders, and a one-click duress button signals responders the location of an individual in distress.

BUILD A TRUSTED SOURCE.

A critical event management platform provides a single source of truth for your entire organization. Training and testing help create an enterprise-wide partnership in which people see the platform as a trusted source of information and recognize the alerts as top priority, requiring their immediate attention.

WHY YOU NEED A CRITICAL EVENT MANAGEMENT PLATFORM

Emergency notification and incident response technology helps private enterprises and governments prepare for critical events. With such technology, the organization and its collaborative partners are ready with the tools and information they need to make the best decisions and execute a seamless response the moment a critical event strikes.

A critical event management platform combines both emergency notification and incident response tools to help organizations manage critical events with real-time communications and intelligence. Ideal for private and public entities alike, this type of integrated, centralized technology enables you to plan, manage, remediate and continuously improve emergency responses.

ENSURE YOUR ORGANIZATION IS READY FOR EVERY CRITICAL EVENT

BlackBerry® solutions for Critical Event Management—BlackBerry® Alert and BlackBerry® AtHoc®—provide secure, real-time notification and incident response capabilities specifically tailored to the needs of diverse

Learn more at www.blackberry.com/cem

COMMERCIAL AND INDUSTRIAL

BlackBerry Alert protects commercial and industrial facilities across the globe, enabling them to keep people safe and reduce downtime.

Read the case study ⇢

GOVERNMENT

BlackBerry AtHoc protects millions of people from earthquakes, chemicals and more.

Read the case study ⇢

HEALTHCARE ORGANIZATIONS

BlackBerry Alert streamlines hospital daily staffing operations for effective resourcing so medical professionals are always where they're most needed.

Read the case study ⇢

REGIONAL AND LOCAL AGENCIES

BlackBerry AtHoc connects regional, state and local agencies with the communities they serve, meeting critical interoperable communication needs.

Read the case study ⇢

BlackBerry

Intelligent Security. Everywhere.

About BlackBerry: BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including over 195M vehicles. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security, endpoint management, encryption, and embedded systems. BlackBerry's vision is clear - to secure a connected future you can trust.

*For more information, visit **BlackBerry.com** and follow **@BlackBerry**.*