

Emergency Communications and Disaster Response

By **David Page**

Recent events such as terrorist acts, hurricanes and power outages have shown us that interruptions to our businesses, not to mention our daily lives, are never far away. Even the best-thought-out disaster-response plans are inadequate if they don't include effective means of communicating to first responders, citizens and emergency operations centers.

Hopefully, in 2006, we will experience fewer disasters than we did in 2005. However, managers must operate with the assumption that they may face unexpected events at any moment. By following the best practices below, learned through responses to recent disasters, business leaders can make adjustments that will help them manage and effectively communicate through any threat to the continuity of their operations.

Make Sure Your Business Continuity Plan is Modern and Complete

Even with an emergency plan in place, many companies overlook simple, yet crucial, details that will impact them in the case of an unplanned event. Managers should make sure that their plans are adaptable and up-to-date to minimize downtime and ensure business recovery when an unplanned event occurs.

A modern business continuity plan takes a holistic view of the needs those impacted by the plan, including employees, customers and partners. Additionally, it proactively defines which procedures to deploy and who may execute those procedures during an unplanned event, and aligns the communications messaging with the plan and the company's values. The plan, while focusing on business continuity, should also cover compliance issues and address specific ways in which the organization will protect its employees, assets and reputation. Always keep in mind that developing a strong business continuity plan takes time and discipline.

Practice Your Plan

It is not enough to develop a plan. It is crucial also to practice and test the plan to expose any weaknesses, overlooked aspects or problems. Since continuity of operations is critical during a disaster, testing the plan regularly improves an organization's ability to maintain continuity by working out the kinks in advance.

Kinks in plans can lead to communication failures. For example, in May 2005, federal buildings in Washington, DC—including the Capitol, the White House, and Supreme Court—were evacuated after a small plane, flown by a student and his teacher, accidentally entered airspace three miles from the White House. Grave concerns regarding the government's emergency notification system came to light after the incident, when it was revealed that President George W. Bush, who was in nearby Maryland, was not taken to a secure location, and that the White House's emergency notification system had failed (CNN.com, May 2005). Exercising a plan can reveal such vulnerabilities before a business (or government) has to rely on it in a real emergency.

Business needs live, grow and change, and continuity plans must live, grow and change with those needs. Practicing your plan lets you see if it's in sync with your needs. Pay attention to what went wrong, what went right and what needs to be updated or amended in the plan.

Make Sure Your Employees Are Well Trained

If employees are unfamiliar with the plan, it will fail. They need to know how to initiate action, how to operate the appropriate technology, what to do in case any element of the plan doesn't work, and where to go for additional information.

San Francisco experienced a breakdown in their warning system during the tsunami in December of 2004. As a result, the alert was nearly an hour old before San Francisco officials were informed. According to the city's emergency operations chief, the nighttime alert from the state Office of Emergency Services was unheeded for critical minutes because the emergency communications dispatchers did not receive a teletype from state regarding the tsunami danger. In the chaos, county officials had to rely on the Internet and other tsunami warning centers for information (SF Chronicle, June 2005).

Make Emergency Communications a Priority

After Hurricane Katrina, New Orleans faced an emergency communications disaster. Residents were unable to tell rescuers their location and rescue workers were unable to contact headquarters or each other. Police and repair crews were unable to enter New Orleans because they could reach no one who could authorize their entrance.

Communication is critical during an emergency and needs to be addressed thoroughly within the disaster-response plan. No matter what the industry, business continuity demands that organizations inform and mobilize response teams, provide guidance and instructions to employees, and communicate with appropriate authorities and external stakeholders. Challenges include reaching people in different locations with different devices quickly and simultaneously; providing the right message (in terms of content, length, and format); monitoring delivery and response; and ensuring that the process is initiated and suspended at the right times.

One way to address communication challenges is with automated-notification technology, which can rapidly distribute information to large numbers of people. Be sure to provide extensive training and conduct regular testing so that human-driven errors, such as sending incorrect messages or failing to notify the right parties, are reduced to a minimum.

Companies also need a way for external stakeholders to call *in* to provide information, as well as receive it. For instance, in a situation like Hurricane Katrina where cities are evacuating, many companies set up 1-800 numbers where employees would call to report on their safety, while receiving pertinent information. This enables management to account for its employees, determine where employees evacuate and identify potentially missing employees. When employees call in, management can include valuable information for the employees concerning payroll, health care, satellite-office locations, and so on. With this method, employees are able to receive information when the time is convenient, not only within the short window of time possible with automated outbound calls.

Lastly, understand that during disasters, communication obstacles are all but inevitable. A successful disaster-response plan should anticipate communication failures and account for inaccessible communication channels, such as downed phone lines. Obtaining multiple modes of contact from stakeholders, including home numbers, cell numbers and email addresses, in advance of disasters increases the odds that businesses will be able to reach everyone necessary. See the appendix at the end of this article for strengths and weaknesses in various modes of communication.

Remember Communications in Business Continuity

Unplanned events that pose potential threat and disruption will continue to confront businesses. Because businesses have intellectual, business and human assets to protect, it simply does not make business sense to be unprepared. And, as we've discussed here, being prepared does not mean simply creating a plan.

It's easy to overlook the role of communications because we live in an age when it works virtually all the time. However, because a real disaster can bring down communications systems and because effective response to a disaster requires communicating with many stakeholders, it is imperative to consider communications disruptions as you update, test, and practice your business continuity plans.

APPENDIX: STRENGTHS AND WEAKNESSES IN COMMUNICATION DEVICES

Key to your communications strategy is the ability to send and receive messages over a variety of devices—landline and cell phone, satellite phone, mobile device and pager. To be effective, a crisis-communication plan must anticipate and overcome potential obstacles such as power outages and downed phone lines. Be sure to consider the following limitations associated with each mode of communication:

Cell phones and landline phones: These are most efficient for less-severe events and are most accessible for reaching employees, family, first responders or citizens. These devices also offer the ability to bridge into a conference call or command center for full incident management with the touch of a button. However, phone lines may be compromised or tied up during a more-severe incident.

SMS: While it takes longer to type a message than to speak it, SMS has proven to be a reliable method of communication, even in more-severe incidents. Most cell phones now accept SMS messages, and because they require less bandwidth, the ability to send SMS messages is often available when a voice call is not. These channels continue to be overlooked and underutilized in emergencies.

BlackBerrys, PDAs, and Emails: BlackBerrys prove valuable because they can receive email, voice or SMS messages. However, they often rely on a corporate server or backup server that would need to be in a safe location distant from the incident. Email without a BlackBerry is effective only in less-severe incidents when someone is near a computer.

Satellite phones: These are most effective for critical incidents as they will work when a cell phone or landline is unavailable. However, they are expensive and harder to manage and may be best for decision makers and first responders only.

About the Author

David Page is senior vice president and general manager for EnvoyWorldWide, a PAR3 company. For more information, please visit www.envoyworldwide.com.



Crisis Simulations International, LLC
1673A SW Montgomery Drive
Portland, OR 97201 USA

West Coast Phone: (503) 248-2233
East Coast Phone: (305) 205-5042

email: info@crisissimulations.com
web: www.crisissimulations.com