Improving Post-Incident Communication and Coordination

Welcome back to our continuing discussion of the National Incident Management System (NIMS). We first introduced you to NIMS in the fourth quarter of 2011 newsletter. As a recap, NIMS addresses five basic response components:

- Preparedness (discussed in our previous article)
- Communications and Information Management
- Resource Management
- Command
- Ongoing Management and Maintenance

In this article, we will discuss the second response component, Communications and Information Management.

An effective response to almost any incident requires accurate information. But evaluating the information, making effective decisions and communicating the common objectives to all personnel involved in the process is also essential. This concept is especially true when your organization is coordinating responses with outside emergency responders, the public and the families of those involved in any disaster.

You may recall the Sago mine disaster in 2006. Miscommunication about the status of the West Virginia miners was passed on to the families, raising false hope that 12 miners survived. But, in fact, all the miners perished. During Hurricane Katrina, the communications infrastructure was rendered virtually inoperable. Further complicating the response, agencies used nonstandard vocabulary and 10 sets of emergency codes.

As a result of these and other lessons learned, NIMS identifies key features of a communications and information management process. The NIMS approach is designed primarily for the public responder community, but every organization should consider mirroring these key concepts.
Communication systems should be:

**Interoperable** - able to communicate within all divisions in your company and with supporting agencies. Part of interoperability is the ability to understand each other. Utilizing plain language instead of codes reduces confusion.

- As a private/public organization, you will not have the same radio hardware and frequencies as your first responders. However, should your company be directly involved in an accident, a company liaison may be embedded in the response organization as a source of information sharing. If a liaison is not requested by the responders, ask. After all, you know where and what kinds of hazards are located in your facility. You know what kind of aircraft is involved and what cargo was onboard. You know how many personnel are unaccounted for and who they are.
- Ensure your Emergency Response Plan clearly identifies how information is passed both internally and externally during crisis situations.

**Reliable** - able to function in the context of any kind of emergency. Do you lose power or phone lines during high winds? Would a flood disable your communications system? If the sprinkler system went off, will your hard drives and routers remain safe?

**Portable** - built on standard radio technologies, protocols, and frequencies. The Department of Homeland Security is continuously evaluating communication equipment with advanced technology and reliability for emergency responders to take to the field. But, think about the portability of your communications system. In the event of a natural disaster that destroys your headquarters, can you relocate your communications system to the temporary facility you identified in your [Continuity of Operations Plan](#)?

**Scalable** - suitable for use in small and large incidents. Can your existing communication system handle your daily traffic as well as a significant increase in volume? During a disaster, communications both internally and externally will increase dramatically. How many telephone lines do you have coming in and going out? Can you easily increase the number of lines with trained operators who know how to route the calls to the appropriate offices?

**Resiliency** - able to perform despite damage or lost infrastructure. For emergency responders, having a resilient system may involve establishing satellite communications. For your company, using smart phones or text messaging may be an option.

**Redundant** - able to use alternate communications when the primary systems go out. In your own emergency plans, have you built in back-up systems for communications? How will you
communicate to your staff if a storm destroys the power grid and the telephone lines? Do you have the cell phone contact information and email addresses for all of your employees and their families? What other back-up communication methods do you have and do they work?

In NIMS, the objective of Communication and Information Management is to ensure accurate information is shared with all who need to know in order to carry out the incident response. Completing a Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis will help you identify ways to improve your communication crisis plans. Plan and conduct communication drills to evaluate and improve your own capabilities. You could learn how information is confirmed and shared throughout your organization as well as how that information is shared with responders, the public, and the press. Once your plans become part of your corporate policies, it is possible to get everyone on the same frequency and to operate in the most effective possible manner.

Fireside Partners, LLC
An international leader in Corporate Emergency Response Plan (ERP) development, Crisis mitigation and organizational training and assessment for appropriate response.
http://www.firesideteam.com/