Contingency Planning in the Changing Face of Disaster

By Bill Munn

On September 11, we watched as New York, Washington, DC and Western Pennsylvania area public safety responders and emergency communications personnel tackled the savagery and devastation of the worst act of violence ever perpetrated against Americans. And we watched with awe and respect. Through the course of the attack on the World Trade Center, despite spikes in call volume, loss of switching facilities in southern parts of Manhattan, and wireless networks stretched to the limits, 9-1-1 service in New York City never went down.

Since the inception of Enhanced 9-1-1 service and its nationwide deployment over the past 25 years, the United States has experienced a number of catastrophic, high-profile disasters such as the Lomo Prieta earthquake, hurricanes Andrew and Hugo, Southern California brush fires, outbreaks of tornadoes and flash floods—not to mention hideous assaults on humans such as the bombings on the World Trade Center in 1993 and the Alfred P. Murrah Federal Building in Oklahoma City. Although public safety's ability to respond was sometimes complicated by call volume, loss of cellular towers, inability to respond due to street and roadway conditions, or overwhelming demand on resources, where telephone service remained 9-1-1 survived and did its job. The horrific events of September 11 were no exception. New York City Police Department officials confirm that the attacks on the World Trade Center did not compromise 9-1-1 service in New York City.

Examining 9-1-1

The potential for events before considered unthinkable cause us as managers of 9-1-1 networks and answering centers to rethink some issues regarding continuity and/or restoration of service.

Are our facilities secure, and safe from attack by individuals or groups? Every 9-1-1 center can't be hidden away in a secret concrete and steel bunker, but authorities should certainly be able to control access to the facility. This need for security extends beyond public safety facilities, however, since most of the 9-1-1 networks and system components are located in commercial facilities. In addition, most 9-1-1 PSAPs are located in public facilities occupied by other governmental agencies, and the security issues for the facility may be the responsibility of another agency.

Are 9-1-1 networks and data bases protected from cyber attack? The threat of intrusion into the cyber networks that route 9-1-1 calls and provide response data now goes beyond "hacking" by vicious pranksters. The possibility of a group or individual compromising national communications networks, which would affect 9-1-1, is a reality which has drawn the attention of government and military officials.

Are call-takers and dispatchers trained to recognize terrorist incidents? The possibility of chemical and/or biological attacks raise new concerns regarding protecting the first responders to possible incidents. Obviously, as in all violent incidents, responders need to have all the information available before they expose themselves and others to a chemical or biological hazard.

The nature of the response should be determined based on what is communicated in early reports from the scene, and what might have appeared, under normal circumstances, to be illness or carbon monoxide poisoning could be a nerve gas attack.

Are call handling arrangements adequate for significant, sustained spikes in call volume?
Every 9-1-1 network experiences periodic spikes in call volume, varying from one or two minutes to an hour, resulting from accidents on busy highways, highly visible fires, storms or the sounding of warning sirens. An attack or series of attacks of a terrorist nature could result in extremely high call volumes for days following the onset. Even the perceived threat of a hazard may result in large numbers of calls from citizens seeking information.

The Nature of the Threat
Experts in terrorism tell us that as we move into the 21st century, the face and focus of terrorism is changing. Political terrorism of the past required popular support in order to meet their objectives, and may have operated under certain constraints in order not to alienate those they were recruiting to their cause or to turn public opinion against them. As we enter into an age where terrorists are motivated by religious fervor and hatred, we not only see the violence reach the shores of the U.S., but we have entered into a new and dangerous time where few, if any, restraints remain. Attacks are planned to generate incredible numbers of casualties, and to cause crippling damage to the infrastructure and the economy. As the late leader of the group Hezbollah once stated, "We are not fighting so that the enemy recognizes us and offers us something. We are fighting to wipe out the enemy."

Considering the reality that this brand of fanaticism has already resulted in major loss of life within the U.S. itself, it is suggested that emergency communications administrators rethink their contingency plans with the following in mind:

When developing contingency plans and procedures, it is time to think of the unthinkable. Those familiar with concepts of emergency management and hazards analysis know that an emergency plan outlines those hazards which are most likely to occur. Although it is not statistically probable that any one emergency communications agency will have to deal with a catastrophic event, the definition of what is possible may have been redefined September 11. In our planning process, we should consider such conceivable scenarios as:

1. A terrorist strike similar to the events of September 11 with a large number of casualties
2. A biological or chemical attack, with a resulting spike in calls from citizens seeking information or instructions
3. A large-scale cyber attack which affects the 9-1-1 provider network and/or data base

Emergency contingency planning should be a joint function of public safety, law enforcement, and emergency management.

In many jurisdictions, the function of emergency management, and therefore the emergency planning process, is functionally located in a separate agency from 9-1-1 and emergency communications. Given the fact that 9-1-1 centers will likely field the first calls reporting incidents which may be terrorist-related, or calls from the public reporting incidents and/or seeking information, it is important that communications functions—including 9-1-1—be incorporated into

the emergency plan, and that 9-1-1 managers be included in discussions of emergency response scenarios.

For example, in the event of a chemical attack, many hospitals would close their doors to new patients in order to protect existing patients and staff. The plan for such a scenario would provide for a public area such as a gymnasium, warehouse, or park to be set aside for triage and decontamination. In such an event, the 9-1-1 center could expect to receive calls seeking information regarding where victims should go, where persons could locate loved ones, or even from public safety responders seeking the location of the temporary facility. The contingency plan should be written so that once the response begins, the 9-1-1 center would be notified and kept informed as the situation developed. If an agency maintains a back-up answering point, the emergency operating plan might include use of that facility for answering information calls or calls of a non-emergency nature during the course of the emergency.

In order to be effective, any contingency plan should be distributed to every individual expected to act on it, including elected officials and those responsible for working with the media.

Contingency plans for 9-1-1 service disaster recovery should consider loss of service for wide areas over extended periods of time. The most likely scenario for loss of service in the past has involved accidental interruption of the network, including digging accidents and loss of switching facilities due to power failure, problems with the building, or failure in the switch itself. Most jurisdictions have plans in place for emergency response in the event of the loss of dial tone, central offices, or the PSAP facility itself. Consideration of a "terror" scenario should address the need to carry out emergency call-taking and dispatch duties for an extended time.

It is the responsibility of those administering 9-1-1 emergency services to protect 9-1-1 from interruption and to put in place plans and procedures designed to restore it quickly if an interruption occurs. Each and every 9-1-1 manager should review security practices and capabilities to see that access to all sensitive areas is limited to personnel absolutely essential to the operation of that particular facility, whether it is a PSAP, a telephone company switching office, or a data base management facility. Given the possibility of cyber attacks in the future, public safety and commercial personnel dealing with administering and delivering critical 9-1-1 related data should be particularly vigilant in protecting these assets and to providing secure backups.

Do We Change How We Deliver 9-1-1 Service?

In an effort to put the Anthrax situation in proper perspective, public health officials have reminded the public that they are statistically more likely to die in an automobile accident or from the flu than from this disease. In a similar vein, any given 9-1-1 PSAP is more likely to be taken out of service by a backhoe than a terrorist attack. The reality of the attacks of September 11, and the potential for further attacks to "retaliate" for the War on Terrorism, compel us to at least address the possibility for contingencies which could go much further in severity and duration than what we as 9-1-1 administrators have faced to date. Most jurisdictions have plans for dealing with the loss of a central office, dial tone, ANI-ALI services, or the actual PSAP itself. Worst case scenarios could involve interruptions of sufficient duration to require changes in plans for default or alternate routing, relocation of PSAP personnel, or use of back-up facilities in the event of prolonged loss of service.

It is suggested, then, that every 9-1-1 manager and staff continue with the contingency plan based on providing a reliable, robust 9-1-1 service, based upon a service interruption/disaster recovery plan which:

1. Is based upon a thorough inventory of all components of the 9-1-1 call path. A thorough audit of the entire 9-1-1 call network, including landline and wireless company facilities, and completed by public safety and telephone service providers jointly, may provide opportunities to eliminate single points of failure, eliminate vulnerabilities, and provide for use of alternate capacity in the event of service interruption.

2. Is dedicated to making 9-1-1 a "hard target." All components of the 9-1-1 call path should be protected from tampering or destruction by any individual or group seeking to compromise public safety communications, whatever the motivation.

3. Provides a thorough and realistic assessment of hazards most likely to cause an interruption of 9-1-1 service. Our definition of what is likely or possible may have changed as of September 11, but the need for a thoughtful assessment of hazards likely to take communications down, whether natural disaster, construction, or accident, is the foundation of the disaster recovery plan. It helps to plan for the resources necessary to accomplish service restoration if the most likely hazards are known and addressed.

4. Provides for flexibility in the face of the interruption. No large-scale disaster, whether it is an incident of criminal violence or a tornado, follows a rule book. Although the plan should incorporate as much detail as can be realistically predicted, it should not be written in such a way that it discourages innovation or modification in the face of a real event.

5. Is distributed and understood. All agencies, departments, commercial entities, or leaders expected to be involved at any level during a possible event should possess and understand the plan in advance. Hopefully, all agencies participated in the drafting of the plan.

6. Includes provisions for working with the media. Although it may seem difficult to get the attention of local media during normal times, the importance of 9-1-1 is understood and appreciated, and in the event of a major service interruption the media will want to know the impact on the 9-1-1 system and the people who take and dispatch calls. The media can be a valuable ally when it is necessary to deliver a message to the public in general, such as a new hotline for locating loved ones or for obtaining non-emergency information regarding a perceived threat.

7. Practiced... Emergency management agencies routinely conduct exercises in response to disasters, from table-top exercises to full functional exercises. It is to be expected that new scenarios are being developed to rehearse response to chemical or biological attacks, or to WTC-type incidents. If 9-1-1 is not already included in the exercise procedures, the time has come.

September 11 did not bring down 9-1-1 service in the Northeast. It did not change the manner in which 9-1-1 calls are handled. It demonstrated to the public the importance of the service, and the dedication of those who provide public safety communications to the people of New York, New

Jersey, Washington DC and the communities of Northern Virginia and Western Pennsylvania. It also perhaps reminded us of the importance of protecting 9-1-1 assets and of maintaining emergency operating plans, activities that we as 9-1-1 managers already perform.

Dr. Bill Munn, ENP, is past president of NENA and is currently the executive director of the Tarrant County 9-1-1 District, which is headquartered in Fort Worth, Texas. His district serves a population in excess of 1.7 million through 46 PSAPs. He is also a member of the International Association of Emergency Managers, and is an online instructor for NENA's course in contingency planning for 9-1-1 centers.