Is Your 9-1-1 System Protected?

By Bill Munn, Ph.D., ENP

As 9-1-1 professionals, do you wonder if terrorists, international or domestic, would ever strike against the 9-1-1 system? Do you wonder if we've done all we can to protect the service and to restore it, if necessary?

After Oklahoma City, I had the opportunity to pose this question to an expert on terrorism, an individual who is frequently called upon by the national news services for his knowledge of terrorism and how terrorists operate. His answer was this: 9-1-1 is generally seen in a positive role. Therefore, it is unlikely that any terrorist group trying to win sympathy for a cause would want to be known as the group that struck down the public's ability to call for life-saving services.

OK, I'll buy that. But as federal officials warn us of an anticipated increase in terrorism in the U.S., I remain concerned that we are doing all we can to protect 9-1-1 and to see that restoration occurs quickly if there is an interruption in service.

What if the event is not aimed at 9-1-1 but at an agency or entity in close proximity to a PSAP or critical switching office? Will the PSAP be capable of handling or re-routing calls during the aftermath when literally thousands of 9-1-1 calls are made, not only to report the emergency but to obtain information. If calls must be re-routed, how will emergency units be dispatched?

Are we ready for violence against the PSAP or persons within the PSAP? Public safety employees are not exempt from personal problems, emotional difficulties, stress, anger, or domestic situations that may result in violence.

How safe is the data so critical to 9-1-1 call-delivery and the provision of location information? Who can access it? Could a hacker manipulate the data as a prank? Could a well-financed terrorist group use the data against public safety or even destroy it? Could a disgruntled employee enter a virus into the system?

Consider the following imaginary scenarios:

> Police indicate the person responsible for the bombing of a County Courthouse that resulted in the deaths of twelve persons yesterday likely died in the blast. Although they have not released the name of the individual, authorities indicate the suspect was recently involved in a court battle in which custody of his three children was awarded to his parents. The sister had sought custody on the basis of his alleged unwillingness and inability to properly care for the children following the death of his wife two years ago.
>
> The incident, in which the defendant detonated a quantity of explosives apparently packed in the trunk of his car, killed eleven other persons in or near the County Courthouse and caused a portion of the building to collapse. In addition to the destruction of the county building, 9-1-1 service was interrupted for several hours, since the primary 9-1-1 call-taking center, which serves fifteen cities as well as the County, was located in the basement of the building.

With the loss of the county facility, authorities and phone company officials worked feverishly over several hours to re-route calls to the adjacent county. Although the re-routing was accomplished within a half hour, telecommunicators were unable to dispatch most calls due to the lack of common communications channel with the county affected. Calls are now being routed to a special communications center established by State Police until service to the Sheriff's Office can be restored.

* * *

Wide spread service interruptions resulting from what were originally reported as "software glitches" may have been the work of hackers, terrorists, or a disgruntled employee, according to law enforcement officials. The loss of data affected the delivery of 9-1-1calls from a population of over 2 million persons for over four hours Friday, possibly resulting in at least five deaths due to inability of the 9-1-1 network to deliver the call along with critical location information.

Although law enforcement and FCC officials have yet to issue a formal statement, sources indicate what was originally thought to be an accidental loss of 9-1-1 data may have been intentional. According to one source, the FBI is investigation the possibility of a computer "virus" as the cause of the service interruption.

* * *

A domestic dispute between a 9-1-1 call center supervisor and a former boyfriend turned deadly yesterday, as the suspect was shot to death by police tactical squad members moments after he shot his former live-in girlfriend, wounding her critically. The shooting took place after a two-hour stand-off during which the 9-1-1 center was evacuated.

The suspect, a familiar and frequent visitor to the center, was admitted with out question around 3pm, and almost immediately drew what was identified as a 9mm automatic handgun. The gunman was apparently seeking a fellow worker he suspected of talking his girlfriend into breaking off what was described as an abusive relationship. Although the person was not in the center, the suspect allowed other employees to leave before firing random shots into the ceiling of the center. Tactical squad and hostage negotiators arrived shortly afterward, and began a two-hour process that failed when the suspect turned the gun on his hostage.

In addition to the loss of 9-1-1 telephone and dispatch service, critical switching equipment was damaged by gunfire during the exchange. Following the evacuation, emergency calls were rerouted to the County Sheriff's Office.

As 9-1-1 professionals, we are not trained, equipped or given the responsibility for combating terrorism at any level. However, we are given the responsibility of operation at maximum effectiveness the 9-1-1 service for our citizens. Included in this charge would be maintaining a contingency plan for operational outages.

I suggest that if we prepare, maintain, and practice the appropriate contingency/data, including provisions to assure the adequate security of 9-1-1 data, networks and facilities, we are protecting the 9-1-1 emergency telephone service within the bounds of our responsibility.

We've learned in the past that the most common threats to continuous reliable 9-1-1 service do not always come in the form of the most visible, destructive events, such as hurricanes and tornadoes. Instead, the most common cause of all telecommunications service interruptions is accidental cutting or digging up the telecommunications cable. As the made-up events above try to demonstrate, the hazard to our 9-1-1 networks and facilities are less likely to come from well-known international terrorist groups than from local lapses in security or failure to protect data resources.

1. Recognize that 9-1-1 networks, data, and call centers are potential targets for violence. Notice the use of the word "violence" as opposed to terrorism. This is done to include individual acts of violence which are considerably more likely than an act of terrorism. However, in the event of an Oklahoma City type strike, the traditional location of public safety headquarters building near other government centers may place the 9-1-1 communications center in harm's way. Imagine the impact on 9-1-1 services in Oklahoma City had the 9-1-1 center been across the street from the blast at the federal building.

   The increase on call volume during and after an incident is also likely to overburden a call center. If the strike is sizable, and there is no publicized alternate number to call, 9-1-1 centers may receive calls seeking information on relatives and friends for days after the incident.

2. Adopt a contingency plan that will accommodate all types of service interruptions.
   Whether we're discussing acts of terrorism/violence, or Bubba and his backhoe, we're talking about service disruption, how to avoid it, and how to restore service after it occurs.

   If your organization has done a comprehensive emergency contingency/disaster recovery plan, chances are the plan addresses most types of interruptions which could be caused by a violent act. Whereas the most likely cause of loss of 9-1-1 service is typically a break in the interoffice facilities, the effect may be the same. These events may be summarized under the following categories:

   Isolation of PSAP – typically due to loss of communication link between PSAP and end office.

   Loss of PSAP Facility – due to storm damage to the building, evacuation, fire, etc. Would include the possibility that loss of the PSAP would be the result from evacuation as well. The more likely event would be a haz-mat emergency in the area, or loss of power, but could also include a violent incident.

   Isolation of Central Office (end office) – calls may be completed within service area of CO, but not beyond, other than wireless.

   Loss of Central Office –End office switching facility may be lost, which means loss of all landline phone service within the area served by the end office.

   Loss of Data Capabilities – Loss of ability of network to route calls and/or deliver call-delivery mechanism.

3. Make 9-1-1 a hard target.

   Security of the PSAP should be a primary concern of 9-1-1 administration, and access by unauthorized persons should be tightly controlled. Although the public safety 9-1-1 administrator does not have control over private sector facilities, such as telco buildings, a partnership should exist

to jointly assure control over access to switching facilities and other key points of potential failure to minimize exposure, not only to existing employees.

I would also encourage a review of procedures to protect all data resources, from the submission of MSAG corrections by the public safety agency to the administration of routing and location data. The objective of creating a hard target is to not only foil any efforts to intrude into data resources or facilities but also to discourage any misguided or politically motivated group or individual.

In summation, as 9-1-1 has been extended, contingency planning has been accomplished to varying levels. The threat of violence is a contingency which public safety must recognize and deal with. However, the overall objective is protection of the 9-1-1 network and facilities. A well-written, comprehensive contingency plan should be capable of addressing the potential for violence, especially when coupled with and aggressive security problem.

Cr. William Munn is the executive director of the Tarrant County 9-1-1 District in Fort Worth, Texas, and NENA's immediate past president. He is a recipient of the Emergency Number Professional (ENP) designation and the National Coordination Council on Emergency management's (NCCEM) highest honor of professional achievement, the Certified emergency Manager (CEM) credential. Dr. Munn received his doctorate from the University of Texas at Arlington, with Administration as his major field.