If there is one thing that we have learned in the past 15 years, it’s that the unexpected happens. From terrorist acts such as 9/11 or the Boston Marathon Bombing in 2013; to random events such as the Blackout of 2003 and this year’s never-ending Polar Vortices and subsequent flooding, it is safe to say that we may not know what will happen, but we know that something will.

As each major disaster passes, organizations have responded by creating, implementing and updating Disaster Recovery Plans in order to better prepare for the future. These plans are reactive to the event and are designed to limit the disruption to an organization in the wake of a disaster. Typically associated with Information Technology (IT) processes, Disaster Recovery Plans are scaled based on the severity of the event and in getting an organization’s technology up and running as soon as possible.

Of course, Disaster Recovery means something very different for public safety and first responders. As the front line of defense in the midst of a disaster, it’s even more important to maintain access to your systems. While typical Disaster Recovery Plans account for failing over radio systems, phone systems and communication systems, software failover is often not accounted for and can inhibit the speed and efficiency of response at a time when access to information is valued most.

In the midst of Hurricane Sandy, 9-1-1 received over 20,000 calls an hour during the peak of the storm.

While this statistic shows the importance of informing the public of the use of 9-1-1 for an emergency only, it also shows the public’s likeliness of calling 9-1-1 during an actual event. If your department is directly on the front line of the emergency, how will it continue to operate?

Creating a Disaster Recovery Plan

It is recommended to consult with an IT company to effectively implement the best plan for your department, but below are just a few steps to consider before then.

1. What needs to be recovered first in order to continue operations?
2. What does the public need in order to be assured of our stability as a department?

3. How will we communicate that message if normal communication streams are compromised?

4. What do we require in order to conduct normal operations?

And last, but not least, how will you conduct these steps if the department’s location is compromised? In the case of a chemical spill, fire or bomb threat, access to your department may not be possible. How will you continue operations in this case?

Continuing Department Operations with Business Continuity

Business Continuity is often interchanged with Disaster Recovery, though the two are rather different. Simply said, Disaster Recovery is data and systems-focused (how quickly systems can be back online from a technology standpoint) and Business Continuity is operations-focused (how can we maintain normal operations following a disaster). As you can see, Disaster Recovery is simply a part of the overall Business Continuity structure.

Business Continuity as a Service

In areas hardest hit by planned emergencies, such as hurricanes, a department will need to evacuate its current location and switch to a remote location in order to continue operations. For cases like this, CAPERS software, a fully integrated CAD/RMS software provider based in Mokena, Ill., has implemented its Business Continuity as a Service for planned emergencies.

“In the event that a department needs to switch to a remote location, the department can contact us and initiate Business Continuity as a service,” said Reed Konnerth, Operations Manager of CAPERS. “This will switch all services and software to a new location, but everything runs the same as if it were in the department.

“We created Business Continuity as a service for our planned emergency customers, those located in hurricane-prone areas such as the southeast U.S.,” Konnerth continued. “However, we consistently work with our parent company, Intelligent Solutions, in determining the best Business Continuity/Disaster Recovery scenarios for our public safety customers; solutions that will allow a city/village as a whole, to setup multi-site failover locations. In the event of a building loss; due to an event like a fire or tornado, the systems can automatically start up in a new location, allowing the entire city or village the ability to access everything from that site.”

In the end, Disaster Recovery and Business Continuity should be thought of as an ongoing process. Working with an experienced software vendor that understands your department, your system and has a strong partnership with a technology company is imperative in preparing for the inevitable planned and unplanned emergencies that will arise in the future.

“At the turn of the last century, technology served to function as a desirable supplement to an organization’s infrastructure, much like the telephone at the turn of the previous century,” said Sebastian Abbinanti, Chief Technology Officer of Intelligent Solutions, a full-service IT Solutions Provider located in Mokena, Ill. “Today, however, both are the infrastructure of an organization and have become a requirement to its survival. Protecting technological infrastructure equates to protecting the survival of that organization.”

CHOOSING THE RIGHT SOFTWARE JUST GOT EASIER

For over 10 years, CAPERS® software has been serving the public safety sector with a single, focused mission: To Simplify the Process.

How We Make It Easier

1) All-In-One Solution: No need to pick and choose modules, you get them all: CAD, RMS, Mobile, Fire, Crime Analysis, Jail, Adjudication, Mapping, Reporting, Data Conversion and Cloud-Based Solutions;

2) Faster Implementation: Our browser-based software can have you up and running in a few months, not years;

3) All-Inclusive Pricing: CAPERS is site-licensed. So no matter how many workstations you have now, or in the future, the price of the software is the same.

To find out more or to schedule a Free Demo, please call 877.618.4911, or visit www.caperssoftware.com.