Assess, Analyze, Plan: How to Prepare for Emergencies

By Mark Clarke, senior consultant, business continuity services, Sollievo

It was just on the news. A hurricane is heading your way, and it's on target to collide with your organization. What do you do? How do you handle a situation like this? Three words: assess, analyze and plan.

Assess

First, you should do a complete *risk assessment*, or a rundown of the risks your business faces with an impending storm on the way. By performing a risk assessment, you'll be able to identify any and all potential problems as a result of the emergency, from the smallest hang-up to the largest snafu.

Look at every angle of the hurricane scenario. Consider all of the following risks:

- Environmental
- Staff
- Cyber
- Natural hazards
- Utility
- Transportation
- Terrorism
- Pandemic
- Fire

In this case, many of your organization's assets - from your property and your operating systems to your staff - are at risk. In the interest of business continuity, your risk assessment should focus on EVERYTHING that could possibly go wrong.

While you're identifying the risks, also consider known vulnerabilities. Does your building have an infrastructure weakness? Do you have back-up servers to preserve your information if an

outage occurs? Knowing of these vulnerabilities is an important part of the risk assessment process because it can help you better prepare for the planning process ahead.

Analyze

But before you plan, you need to analyze all aspects of your business and how they relate to one another so you can understand how the risks you just identified will impact your business. The best way to do that is to conduct a *business impact analysis (BIA)*.

A BIA is designed to look at all of your processes, one by one, to determine your recovery time objectives (RTO); your recovery point objectives (RPO); your maximum allowable downtime; when your process/business will be impacted by a disruption; when your membership will be impacted by a disruption; regulations that affect the process; potential financial impact; dependencies; legal fines or penalties; IT recovery time frames; and data classifications. These are only a few of the items identified by a BIA.

This identification will help you determine the criticality of each of your processes, from which you can prioritize your preparations. Apply your resources to your critical processes first, and place yourself in a better position to recover or continue your operations should something occur. Once all of your critical processes have been addressed, you can then move down the line to less critical ones.

Plan

At this point, you've assessed and analyzed the situation ahead. Now is when the planning should begin. Take everything you've learned from your risk assessment and your BIA and figure out how to best mitigate the issues that lie ahead.

Place your resources where they are the most useful in your plan. Designate staff for specific jobs and budget money for critical operational contingencies, such as data back-ups or building infrastructure reinforcements.

Also make sure that your plan includes detailed procedures for communication. This includes communication with staff, with your clients, with the media, etc. Communication is absolutely key in any sort of emergency, so make sure your organization is ready to disseminate information to key groups via an efficient communication process.

Including the items listed above, your plan should cover all of the following elements:

- Emergency response
- Resource management
- Crisis communications
- IT disaster recovery
- Employee assistance and support
- Incident management
- Training

The best thing you can do with this or any kind of emergency is be prepared. Have a process in place to deal with dire circumstances. And be sure to employ the fundamentals - assess, analyze and plan.

About Mark Clarke

Mark Clarke is senior consultant, business continuity services for Sollievo. Mr. Clarke's experience consists of directing, facilitating, and coordinating business continuity programs, and ensuring that the program is maintained and tested in consideration of business needs, and in compliance with internal policies, standards, and regulatory guidelines. Mr. Clarke is also experienced in conducting operational risk assessments.