Can Your Business Survive a Disaster?

Posted At : October 30, 2012 4:38 PM | Posted By : Admin
Related Categories: Workplace, Your Business, Business Continuity

We heard it this past week: "Nothing will happen to my business!" "The weather here is not that bad!" "All my company's important information is in my head!"

Our community was just incredibly fortunate. We escaped Hurricane "Sandy"! Nothing much happened here. However, just a hundred miles to our southeast, people and businesses were not so lucky. People lost their lives. Billions of dollars of business and infrastructure have been damaged and destroyed. It will take weeks, months, and in some cases years to assess all the damage and to rebuild.

The reality is that too many of our clients are not prepared to deal with a hurricane, fire, flood, or blizzard; all of which have happened right here in Central New York in the very recent past. A few businesses have failed because of those disasters. On the one hand, we don't want people to go around being scared, but without any planning or forethought, you are just rolling the dice.

Below are excerpts of an article from Cisco Small Business talking about the fundamentals of business continuity, what's involved, and how to plan. Yes, a lot of it is about protecting data and systems. The article is written from a technology company's perspective. However, it's surprising how much of the planning process also involves people, family, communication within your organization and with your clients.

People, processes, training, and planning are a signficant part of effective disaster preparedness. Here are five key steps to consider when implementing a program to help your company or organization survive a disaster.

1. Understand what data and systems are critical to your business
Some of your data is more important than other data. You need to figure out which is your critical data and make sure you don't lose it. Many governments have mandated the remote replication and storage of financial, medical, and certain other kinds of data. Other businesses have realized that their data and applications are their life blood. We have businesses that require no more than fifteen minutes of downtime for some of their systems while other data can be "down" for much longer. We can help you assess what data is important, make sure you know where all of your company's critical data and applications are located and how best to manage it all.

2. Identify and fix single points of failure in your network, business processes, and people
In network design, redundancy eliminates single points of failure. Make sure that network elements — including switches, routers, and other components — are redundant and enabled with software failover features. Understand your business processes and job responsibilities to ensure that there are similar "failovers," should a process or employee become adversely affected in a disaster.

3. Create a workforce continuity plan
This is probably the most important item here. First and foremost, figure out how to communicate with all your employees. Have a plan to determine whether they are safe in the event of a disaster. Have a central method for everyone to check-in. If employees can't get to their offices for days, weeks, or longer, it is important to understand what kinds of remote access solutions they need to continue being productive, based on their individual job

requirements. For example:
Back office workers need access to applications and data and can probably use e-mail or instant messaging to communicate.
Other categories of employees whose jobs require a lot of collaboration may need high-availability voice-over-IP (VoIP) services along with access to corporate data and applications. The benefit of IP and Ethernet in a disaster is that they are so pervasive compared to other technologies that devices are truly plug and play. Every business is different. There is no cookie-cutter solution.

4. Create a disaster recovery plan
I know -- most of us hate this kind of planning process. I do. However, some kind of formal plan should be initiated and endorsed by senior management. It needs to involve all levels of personnel in your company or organization. An inclusive process of gathering information and drafting the plan will create the necessary sense of everyone's ownership in and responsibility for disaster recovery. Here are some of the common elements of most plans:

- Risk and threat analysis
- Leadership and succession plan
- Emergency response plan
- Internal and external communications requirements
- Human resources responsibilities
- Facilities management
- Availability of information and communications technology
- Cooperation with first responders, public officials, vendors, partners, and customers

5. Train your staff on disaster response
Training and practicing emergency responsibilities for certain types of disasters relevant to your business could have dramatic consequences related to personnel safety, business continuity, data confidentiality, and asset security in the event of a real disaster.

We do have a few clients with sophisticated and comprehensive plans. Others have basic plans that just manage their most critical information and have a way to communicate with their staff. What you decide to do is up-to-you. The goal is for your business or organization to survive should disaster strike. We'll be glad to help.