

**Title: How To Build The Ark**

**Subtitle: Web Technologies**

**Second Subtitle: #0 Disaster Preparation is Good Stewardship**

**Author: Steve**

**Date: 2011/11/3**

**URL: <https://www.christianwebresources.net/modules/article/view/article.>**

**Keywords:** preparation, planning, strategy, documentation, backups

**Summary:** When technology works - it's great. When it doesn't, life can be a challenge. Noah had to build the ark. He also had Joseph store up grain for the famine. What preparation for the ups and downs you'll experience?

Many days go by unplanned - heads down, noses to the grindstone, just trying to get through. Then it happens - some unexpected glitch throws your entire world on its backside. It could be trivial, like knocking over your coffee cup. Or, it could be 2 feet of snow, a power outage, an earthquake. Or, it could just be someone calling in sick. In any event, you need a way of coping with those changes.

With just a little bit of planning and only a few minutes out of your day, you can prepare and reduce your chaos when faced with an unplanned event.

**Communication - People First**

As mentioned above, human assets are above all others. Communicating during a disaster is essential to any and all plans. Disaster preparation and recovery plans have three stages - the first part of your plan must address communication.

**How will you communicate?** In the event of a loss of power, you could also lose your primary communication channels - very few phones work without power, even if they are still intact.. Will you use cell phones, text messages, emails, website updates, social media? Identify the channels of communication you will use before, during and after an event.

**Who will you communicate with?** Identify your contacts, families, neighbors, media outlets, etc. Make a list of the many people connected to you.

**When will you communicate and how often?** Different groups may have different communication needs - be sure to lay out a schedule of updates once you are able to communicate.

### **Communication Tips:**

In your preparations, be sure you have a list of people in different forms - you may not be able to retrieve them from your contact list on your computer.

Establish a calling tree to spread news and updates outside the potential disaster area. This can be your communications hub. Sometimes making a long distance call is easier than trying to call within the affected area.

### **Documentation - Putting the Pieces Back Together**

What I find is the most critical piece of equipment or information is usually not documented. You only discover how critical it is when it breaks, gets turned off, or you don't know what it does isn't around. Then there is a mad scramble to figure out what component is. Things you think you'll never need again will become the most important.

when disaster strikes - software licenses, technical support phone numbers, account numbers, installation disks and configuration information are all written down and stored safely in more than 1 place.

What's missing? Who's missing?  
Where does this go?  
Whose is this?  
Where do we get another one of these?

Documentation also needs a backup and backups need documentation

Where are the backups?  
Who did the backups?  
When were backups last done?  
What didn't get backed up?  
How do we restore the backups?

### Documentation Tips:

If your documentation is on paper, consider scanning it and having it in electronic form. If it is only electronic, consider printing copies and storing them in watertight containers outside the disaster zone.

Create a **video inventory** of your facility - show the items and describe them as you see them. Identifying items after they've been burned or covered in muck isn't as easy as identifying them before. Include in the inventory the network cabinet, the phone system and smaller items that are easy to wash away or destroyed.

Don't forget to protect your investments - place installation CD/DVDs and license keys in watertight containers and take offsite.

Backups - Filling in the Details  
What, How, Where, Do they work?

**It's as easy as 1-2-3** - 3 copies, on at least 2 different media and store a copy offsite. **Know what to keep and what to delete** - Maintaining multiple versions of a backup can create even more chaos. Having a document in 5 different folders doesn't make it easier to determine which one you actually need.

**Will it work on new hardware or with the new version of software?** - Test your backups on computers that come with a 3.5" floppy disk drive. Make sure you upgrade your systems. Also, stay current on your software! Even if you have the source files, you may not be able to get it to work on a newer computer.

### Backup Tips:

If you have backup software already installed, make sure it is running and working. Use several different backup media. Internal harddrive or even a network storage device is just as much at risk as your computer. Portable USB storage drives are also at risk. With backup software, too. Burn copies of backups to a CD or DVD and store them offsite.

There are several different backup solutions. Consider backup your critical systems on a daily basis. These solutions will provide you with a very remote backup, but they are not perfect.

access to that data from anywhere.

People - First and Last

Often, our disaster preparation only covers loss of a physical asset, like People are the most vital part of your organization and you should have of transition in staffing or people.

**Who can do what ~~four~~?** Everyone has their unique talents and responsibilities definitely burn out if no one else can chip in and lend you a hand from time may not be the same as yours, but they should be able to get the job done sick.

**Who knows what ~~you do~~?** When it happens more than once - someone leaves countless little things they didn't get done anymore. Eventually, they addressed, but sometimes those little things can be big headaches.

**Who has the computer?** People are working from home, or bring their personal to work. It can save on your expenses, but this also poses a risk. Is sensitive Do you have access to their work in progress when they are not on site?

This is the area that requires the most prayer and probably some of the most Please don't let this prevent you from having the necessary discussions assets. Remember **be a resource**

Continuity

Some disasters are very short-lived and the recovery is fairly quick. Some ever end so you can start the process of recovery. Use these questions to extended periods of adversity.

How long can you go unplugged? Do you have backup power supplies? Will generator be appropriate? How long will your phone or laptop stay charged?

How long can you go without Internet access?

How long can you go without fresh water, heat, or food?

What would it take for you to relocate and continue?

How many people would it take just to keep things running?

Other resources for disaster preparation

[Ready.gov - Business](#) Prepare. Plan. Stay Informed

[FEMA](#) Plan and Prepare