The Resilient Organization

A Guide for Disaster Planning and Recovery

Table of Contents

Introduction 5

How to Use This Guide 5

Part I: Planning for Disaster 6

Chapter 1: How to Build Resiliency from the Ground Up 7

Basic IT Best Practices 7

Communications Redundancy 9

Your Internet Presence 10

Data in the Cloud 10

Chapter 2: Understand Backups 12

Types of Backup 12

Devices to Back Up 13

Chapter 3: Develop a Backup Plan 15

Best Practices for Backup 15

Locate Files for Backup 16

About On-Premise Backup Solutions 16

About Remote Backup Solutions 19

Chapter 4: Documentation and Your Master Key 21

Storage of Your Documentation 21

Chapter 5: Staff and Training 23

Part II: Recovering from Disaster 24

Chapter 6: Basic Equipment Recovery 25

Technology Triage 25

General Safety Tips 26

Hardware Recovery Tips 27

Reestablish Communications 28

Network Recovery 28

Data Recovery 29

If You Need to Move Your Website 30

Chapter 7: Guidelines for Non-Technical Disaster Planning and Recovery 34

Quick Disaster Checklist 34

People and Deliverables 34
Operations 36
Project Planning and Rollout 37
Communications 37
Business Impact Assessment Questionnaire 38
Legal and Regulatory Requirements 39
Work Flow Relationships 40
Data and File Recovery 40
About This Guide 42

Introduction

Part I of this guide is *Planning for Disaster*. It offers guidelines and strategies that would be useful for any charity, NGO, or public library in the world. However, some are more applicable for smaller organizations. If your organization is large, we encourage you to discuss our recommendations with an IT manager or consultant in order to develop an appropriate plan. We've also supplemented this guide with links to additional, useful information from around the Internet.

Unfortunately, disasters are the times when your constituents most need your services. Part of a recovery plan, therefore, is a triage phase. During this phase, you evaluate which programs must continue to receive full staff attention and which ones you can slow or pause while you rebuild. Part II of this guide, *Recovering from Disaster*, is intended to help you simultaneously continue key operations and rebuild your infrastructure.

This guide is not intended for charities whose continued efforts in a time of disaster may put their staff in danger. You might find more appropriate information from your local Red Cross or Red Crescent in some instances. An example is if your charity needs to recover during a civil war or other period of political upheaval. Another instance would be if your work requires your staff to stay in an area in which a disaster has occurred or is underway.

How to Use This Guide

This guide is divided into two sections, *Planning for Disaster* and *Recovering from Disaster*. For charities that need to recover from a disaster, the second section will be more relevant than the first. Regardless of your current situation, however, if you read the entire guide, you'll gain a deeper comprehension of the issues that surround disaster planning and response.

As you document the technologies and strategies that you implement in the disaster preparedness section, you'll simultaneously create your own instructions for a future recovery. Should a tech crisis arise in the future, your own documentation will be your primary aid in the recovery process. This guide and other resources can serve as supplements.

If you're in recovery mode, this guide is intended to help you through the triage process and development of your recovery plan. Chapter 7 of the guide lists the key areas where you should focus on and as you work through the recovery process.

Part I: Planning for Disaster

Disaster preparedness isn't just a state of readiness for a fire or earthquake; it's a nimble, flexible approach to your organization's day-to-day programs and operations. A natural disaster may never hit your office, but if you adopt certain technologies and strategies, you can deepen your charity's impact. And you can make your work faster and more efficient.

In this section, we'll discuss simple strategies to prepare your charity or public library for new challenges and opportunities. First, we'll talk about ways to protect your systems from preventable disasters. Next, we'll discuss everything you need to know to devise a sound backup plan. Lastly, we'll help you document essential processes to reduce downtime during an emergency.

Chapter 1: How to Build Resiliency from the Ground Up

Disaster planning addresses more than the need to be ready when a fire or flood damages your computers. It's a way to think about your charity's day-to-day operations just as much in times of health as in times of crisis. An organization that's ready for a disaster is an organization that is effective regardless of scale. Disaster preparedness is also part of how you fulfill your mission to your constituents.

Basic IT Best Practices

This guide is mainly about a catastrophic disaster that affects an entire office, area, or even region. However, there are some basic IT best practices that are very useful, even for minor disasters. Any disaster entails loss of some sort, and the root of disaster planning has to do with loss prevention. In contrast, disaster recovery is the expedient replacement of what was lost, in a manner that is appropriate to the disaster suffered.

There are many ways to lose assets, but the most important asset in any organization is its data. Protection of that data forms the basis of disaster planning. Large enterprises employ "data-loss prevention" (DLP) strategies and technologies to prevent any data, especially confidential data, from leaking outside the organization. There are simple things that small organizations that are in the charity sector and that lack the extensive budgets for a comprehensive technical solution can do too.

Data loss might mean that you have lost data because a virus has rendered your computer unusable. Or it could mean that you have misplaced your notebook computer. Or, it might mean that an actual natural disaster that damages your office and equipment has occurred. For the first scenario, it's important to make sure that your computers are properly protected against viruses and malware. Spam prevention is also important because spam often either carries those dangers directly or leads unsuspecting users to malicious websites to install malware. Users should be properly educated to recognize suspicious emails and websites. Many of these suspicious emails and websites use "social engineering" to trick users to provide confidential information or to unintentionally install malware. Users also need to be coached to only open email from known senders. And they also need to know that even if the "From" field is familiar, if the subject or body seems odd, it's best to confirm with the sender to make sure it really is from them.

Another basic tip that many forget is just that you need to save your data frequently. Although applications are now more sophisticated and have auto-saving functionality, you should err on the side of caution. If your computer freezes and you need to restart it, a recently saved copy is better than an old backup. If you save a second copy to a shared drive or an online folder, that's a good way to ensure redundancy.

If your computer does have problems, it's good to have recovery discs available to restore it to a working state. If your computer is newly purchased, it's important to keep the recovery discs handy in case you need them. A more likely situation is that your computer was donated, or was upgraded several times, and a system recovery disc did not come with it. In Windows, recovery disc creation differs by version, so check online to find the solution applicable to you. In Mac OS, you can press

Command-R to initiate the OS X Recovery process. You can also download a separate "Recovery Disk Assistant" on a USB drive.

Data Encryption

In an ideal secure IT environment, if a device and its data are lost, the data on that device was backed up recently. Thus, the data can be easily recovered to another device. The lost device would be remotely wiped and made inaccessible. And even if someone were to gain access to the device, the data itself is encrypted and would require sophisticated decryption to be readable.

IT environments in the charity sector, however, are often less than ideal. The use of encryption is not a strategy that most organizations consider. But in some instances, state and federal laws may dictate a certain level of encryption for sensitive data. In all instances, your first priority should be to protect the people who trust you with their personal information. If your organization has compliance needs or staff who frequently travel, or if your mission may subject your systems to intrusion, you should definitely keep your data and systems as encrypted as possible. There are three levels that you can use:

- File encryption: Your files are individually encrypted. They can only be unlocked with a password. Microsoft Word, for example, allows you to password-protect and encrypt a file under the **Protect Document** settings. Keep in mind, however, that if you rely solely on a software program's password-protection, the file itself may not be encrypted.
- File system encryption: With this level of encryption, an entire directory of files or even the entire operating system is encrypted. This is available as a feature for certain operating systems. For Windows, BitLocker technology can encrypt the entire drive or a data folder. It is available for Windows 7 Enterprise and Ultimate, and Windows 8 Pro and Enterprise. For Mac OS, FileVault is available for Mac OS Panther and up, with levels of implementation that vary. You can also use a third-party program like Truecrypt (which is free) to perform the same function. This feature may also be available for mobile phones and tablets.
- Full-disk encryption: With this level of encryption, the entire drive is encrypted. Most often, full-disk encryption uses a combination of software and hardware. It can also be used in conjunction with file system encryption. This is the most secure level of protection against physical loss.

It is very important to protect the private information of your donors, constituents, and volunteers. Constituent relationship management (CRM) and donor database applications should always be password-protected to deter unauthorized access. And if possible, the data should be encrypted too. Regardless of whether they are cloud or on-premise systems, be sure to log out of these applications every time you are finished with them.

Many countries have individual laws and standards that address encryption of personal data, particularly health information; please consult the materials that are appropriate to your country for specific security recommendations. The Health Insurance Portability and Accountability Act (HIPAA) protects health data in the United States.

Communications Redundancy

To build resiliency, it's also important to ensure that your organization can communicate in the event of an outage. Email, social networking, and mobile technologies have enabled communications that are free from ties to a specific desk or even a physical location. However, if your organization relies on timely communications, it's important to consider whether it is equipped to handle an outage. A unified communications (UC) approach may be what it needs.

UC refers to a large family of technologies and organizational practices that simplify and integrate multiple forms of communications. These forms of communications include phone conversations, email, video and web conferencing, instant messaging (IM), voicemail, fax, and SMS messages. If you implement UC, your organization can be better prepared for disaster and can more quickly restore your communications.

The central idea behind UC is that an employee can access and reply to a message with the use of whatever device is convenient at the moment. This is regardless of what sort of device the message was generated on. If so, there will be less lag time between replies, and the organization will be able to communicate more effectively internally and externally. In a disaster scenario, it's essential that fast communication be free of the requirement that employees are physically present in the office.

UC also refers to business practices that encourage a smooth flow of communications among several media. Before you select a UC strategy, it's a good idea to take an inventory of how your organization currently communicates, both internally and externally, such as:

- Do employees communicate with each other more by phone or by email?
- Do employees use personal phones and email addresses for work?
- Do volunteers and other people outside of the staff use office telephones and email?
- In a disaster situation, what steps would be necessary to reestablish communication?

Most importantly, remember that staff adoption of UC is just as important as whether you choose the best technical approach. Train your staff to use new communications solutions and make sure that they have time to learn and ask questions.

Hosted Voice over IP Services

Adoption of a hosted Voice over IP (VoIP) service can improve your organization's ability to communicate if disaster strikes. You are also more likely to restore services sooner. A hosted VoIP service in the office is functionally similar to regular telephone lines. However, it allows employees to work in different physical locations if that's needed. During a disaster, an employee can bring VoIP equipment home and use it with her home Internet connection. Or she can have the VoIP service forward her calls to a mobile phone. There are numerous VoIP services that are available on the market. A web search for "Hosted VoIP" with your local search engine will provide you with some relevant results.

An obvious advantage of hosted VoIP services is their simple, fast installation. If a disaster requires staff members to work from home, they can easily use VoIP routers or phones with their own Internet

connections. Generally, VoIP providers let businesses set up their group phones at multiple locations and even move them from place to place for travel or field work.

Voicemail-to-Email Online Services

A voicemail-to-email service might really help to prepare you for a disaster. Such a service would let you receive voicemail messages quickly from anywhere with an Internet connection. If phone communication becomes unavailable, you'll still be able to receive and respond to urgent communications.

In the past few years, numerous free or inexpensive voicemail-to-email services have gained popularity. These services serve as virtual voicemail boxes for one or more phone lines and generally allow the user to access messages either by phone, online, or by email attachment. If you need to give a message to a colleague, you can forward it as an email from the online user interface. Or you can simply forward the email message. Popular services in the U.S. include Google Voice, YouMail, and RingCentral. Many of these services also let you have a single telephone number that will forward to multiple numbers at once.

Your Internet Presence

Your charity's website is the most visible part of your organization's operations. It's natural that in a time of disaster, people who care about your work will turn to your website for updates. If your organization is involved in disaster-relief work, your updates will become even more pertinent. Unfortunately, to maintain your website during a disaster — let alone add needed updates — may be too difficult, especially if your computers are damaged. Unless you host your website on premise, your web hosting provider will have their disaster recovery in place to hopefully minimize the downtime.

You should assess whether it might be a good idea for your organization to set up an emergency website. An emergency website can keep followers aware of the developments that surround a disaster more quickly than your regular website. For example, you can send updates to your Twitter feed from mobile phones and other devices. In this way, you can communicate with friends of your organization through Twitter even without a computer or regular Internet access. Perhaps the main way you communicate with your constituents online is through a blog or Facebook page. These can be updated via any device regardless of platform, if you have any sort of Internet access. Even if there is a region-wide disaster, these large Internet companies will have recovery plans in place. This is especially true if they have large enterprise customers who are affected too.

Data in the Cloud

As cloud adoption in the NGO sector increases, the cloud's often-mentioned benefit is its resiliency to disaster and data loss. If the data is in the cloud, it is perceived that users no longer have the responsibility to back up that data. This is only partly true. Cloud services providers do all that they can to ensure that their service is uninterrupted and that their data is available to their users at all times. However, their downtime is outside your control, so as a user, you also have some responsibility to ensure that the data is available. If it's crucial that your organization must have all its data available at all times, then your backup strategy probably needs to specify how you will safeguard that online data.

More importantly, your organization should not rely upon a service that is designed mainly for online sharing and collaboration. An exception is if the service is specifically designated "online backup" or "remote backup."

For example, your organization may routinely use a file-sharing service like Google Docs, SkyDrive, or Dropbox as a shared location for your reports or spreadsheets. If so, it is better to think of these as another location that you need to back up, either locally or to another online location. An inability to access that data, due to service interruption or inability to get online, is just like any other data-loss scenario.

If you use an online CRM or database application, it is also advised that you periodically download that data. Generally, you can use an **Export as CSV** function to download the data to a server or backup location that you can access. This would better prepare your organization if you were unable to access the online service at a critical time. CSV stands for "comma-separated values." CSV files can be easily read by many programs.

Chapter 2: Understand Backups

Regular backups are vital insurance against a data-loss catastrophe. In this chapter, we'll present some basic backup concepts.

There are two broadly defined approaches to backup: on-premise backup and remote backup. The approach you choose will depend on the resources you have, such as staff expertise, IT budget, and the reliability and speed of the Internet. In addition, it will depend on the amount of data that you generate as an organization and how soon you need to restore data after a disaster occurs.

	Description	**Pros**	**Cons**
On-premise	Data is backed up to media located on premise, such as CDs or DVDs, an external hard drive, or a shared drive on the network.	All the data is within your reach and is available for immediate retrieval.	Backed-up data is vulnerable to loss, whether through theft (someone breaks in and steals equipment) or damage (such as a leaky water pipe or a natural disaster).
Remote	Data is backed up to a remote location.	You pay for storage and traffic, not for the equipment. In the event of a localized disaster, your data is still viable.	Internet access is required to back up your data. Data recovery takes time if done via the Internet. Your provider may be able to mail you your data, but you may incur extra costs. You also have to entrust critical data to a third party.

With both methods, you use a piece of software that schedules the backup at regular intervals. In the case of remote backups, that software is included with your subscription. For an on-premise setup, although all operating systems include rudimentary backup applications, you must also separately acquire specialized backup software.

Types of Backup

With most backup solutions, you can choose to back up all of your data or just data that was added or changed.

- A full backup is the most complete type of backup. It is the most time-consuming and requires more storage space than other backup options.

- An incremental backup only backs up files that have been changed or newly created since the last incremental backup. This is faster than a full backup and requires less storage space. However, in order to completely restore all your files, you'll need to have all incremental backups available. And in order to find a specific file, you may need to search through several incremental backups.
- A differential backup also backs up a subset of your data, like an incremental backup. But a differential backup only backs up the files that have been changed or newly created since the last full backup.

Devices to Back Up

The simple answer may be that you plan to back up all of your organization's computers, but there are additional factors to consider too.

Workstations

You'll need to know the location of the data that you plan to back up. For example, while most Windows users store data in their Documents folder, they also may keep files and folders on the Desktop. So you'll need to back that up also. Special database- or financial-software packages may store files in their program directories, so be sure to back these up, too. Some programs will allow you to back up configuration or settings — find out if your programs support this functionality. Finally, be sure to understand how your email is set up. You'll need to know where your messages (sent and received), calendar (if your email application has one), and contact information are stored.

If you have an extensive bookmark collection in your browser, be sure to back that up as well. You may choose to periodically export your bookmark file from within the program, or point to the bookmark file itself in your backup software. Alternately, browsers like Chrome and Mozilla allow you to sync your bookmarks online.

Servers

You should have regularly scheduled backups for your servers. In addition, it's good practice to conduct a full backup of your server before every major update. Then you will have a way to restore your server's entire hard drive if anything goes wrong during the update. A proper file server should also have a server-class operating system, with hot-swappable hardware RAID. (RAID stands for "redundant array of independent disks." A RAID system divides and replicates data among multiple physical drives, which protects the data from loss in the event of a disk error.)

- If your organization uses an in-house email server, the email server must be a part of your backup plan. Email servers include their own backup utilities; check the user manual for more information.
- If your organization does not use an in-house email server, then mail is stored locally on users' computers. The mail folder on each computer must be backed up.
- If you use a webmail service, check with your email service provider on its backup and restore policies. If the webmail service is offered through your Internet service provider (ISP), find out whether the ISP backs up your email.

- If you only use cloud services like Google Apps for Nonprofits, these services are generally considered safe from hardware failure. However, you might want to download important messages if you need to ensure accessibility. You can also use a mail client to access these services, and then back up the mail folder files as if the services were non-cloud applications.

Personal Computers

If your employees, contractors, or volunteers work with their personal computers, their data should be part of a regular backup strategy. For all remote backup services, you can install a backup program on any computer, even for one that is not on the work network. As a simpler alternative, require that work that is performed at home is saved to a work computer or shared storage solution every day.

Mobile Devices

If you store critical data on your mobile devices, such as contact lists or other documents, this data needs to be backed up as well. It's generally not recommended that you store sensitive data on a mobile device. However, if you do have sensitive data that's on your mobile devices, those files must be encrypted. For instructions on how to encrypt your files, see the device's manual.

Cloud and Other Hosted Solutions

A disaster that strikes your office or even your city or region likely will have minimal or nonexistent impact on cloud solutions. However, it's good practice to periodically download data from your cloud services, in case you need to access it if there is an outage.

Website

If you host your website on-premise on a server, then it should be backed up like any other server. If it's hosted off-site, your web hosting provider should back up the data according to their data backup policy. Be sure to check with your provider to determine if their backup and restore policy is sufficient for your organization's needs. As with other services that are managed by a third party, there are many reasons to keep a copy of your website on an office computer. Most content management systems allow you to back up your own content on a local computer, which you should include in your regular backups.

Networking Equipment

The setup and configuration that the networking equipment has is important information that takes time to reconstruct. Information such as ISP details, reserved IP addresses, special routes, and wireless settings should be backed up as well. Both retail- and enterprise-level networking equipment allows you to back up configuration information if you access the device via a workstation.

Chapter 3: Develop a Backup Plan

Best Practices for Backup

All backup routines must balance expense and effort against risk. Few backup methods are 100-percent perfect. Here are some guidelines that you can use to develop a solid backup strategy, regardless of whether it's on-premise or remote. Have a backup plan that outlines:

1. What's being backed up
2. To what location it's being backed up
3. How often backups will occur
4. Whose responsibility it is to perform and validate backups

In addition, think about:

- Data that is created by everyone you work with (and that includes people who are in addition to staff and contractors) and everywhere (instead of just in the office).
- Data that is only in hard copy. This is especially important because hard-copy data can be difficult to reproduce. This type of information should be stored in a waterproof safe or file cabinet as well as backed up electronically (either scanned or computer-generated). It includes:
    - Government forms, such as paperwork that qualifies your organization to be a charity or tax-exempt
    - Finance and personnel information
    - Contracts, like equipment and office leases
- Data that is crucial to your day-to-day operations.
    - Charities that do a lot of data entry should consider whether it makes sense to back up their databases after each major data-entry session. Core files like documents (such as your Documents and Desktop folders) and email files should be backed up at least once a week, or even once a day.
    - It's unnecessary to back up the complete contents of each individual computer's hard drive, since most of that space is used by the operating system and programs.

If you have the expertise and storage space, you may choose to perform a full-system image or "bare-metal backup." This would minimize the time to reinstall and reconfigure your operating system in the event of a disaster.

- Consider what data would be most essential to have at your disposal in an unexpected scenario. If Internet connectivity is lost, online services may take time to recover. Keep the information that would be essential to service restoration regardless of Internet connectivity.

It's also really important to test the backups before you need them. Make sure your backup software has full read-back verification. Simulate a disaster scenario at the organization, and try to restore a few files to a different computer at a different location.

Locate Files for Backup

While most Windows users store data in their Documents folder, they also tend to keep files and folders on the Desktop. So make sure you also back up those. Special database or financial-software packages may store files in their program directories, so be sure to make copies of these, too. Understand how your email is set up. You need to know where your messages (sent and received), calendar (if your email application has one), and contact information are stored. It's important to back up the settings in addition to the data.

Check with your email service provider — which may offer backup services — on its backup and restore policies. Email messages may also contain copies of sent attachments. If you do not have a backup of a file and your original was lost, it may be attached in an email somewhere. Locally, mail data files should be backed up, and their locations vary by program. In Microsoft Outlook, mail data files are commonly located in:

```
C:\Documents and Settings\<username>\Local Settings\Application
Data\Microsoft\Outlook\*.pst
```

About On-Premise Backup Solutions

If you use on-premise backups, remember that it's still essential to store copies of backup data off-site. Any disaster that affects more than one computer is likely to affect the backup device in the same physical location. We recommend that you rotate a set of backups off-site once a week. Ideally, you should store your backups in a safe deposit box. Another method is to follow the 2x2x2 rule: two sets of backups that are held by two people in two different locations. You may lack the resources to ensure this level of redundancy. However, keep in mind that in general, the more copies of backups you have, the safer your data is.

Backup Hardware

Here are some guidelines to choose backup hardware that would be appropriate for your organization:

- Determine how much data you need to back up. Survey the machines on your network or at least a representative sample. How large is each user's documents folder? How large is the email file? How much data is in your organization's primary shared folder? Add up the totals for all your machines, or multiply the average by the number of machines in your organization. Be sure to leave room to add a few new staffers and to plan for growth — it's very possible to add five GB of data per person per year.
- Double that number. Choose a backup solution that allows you to store at least double the amount that you think you will need to back up every three months. This will give you room for growth and will also allow you to store incremental backups on the same media as full backups.
- Consider the device's speed and how it interfaces with your computer. When you have a large amount of data to back up, a big storage device is less useful if it writes data slowly. Make sure your hardware can support reasonably fast data transfer rates.

Magnetic tape was previously the standard for storage of large amounts of backup data. However, disk-based technology such as backup and file-storage servers, as well as external hard drives, has slowly replaced tape as the backup media of choice. For example, network attached storage (NAS) is a type of device that offers disk-based storage like a dedicated file server or backup server would. However, it's in a small and efficient chassis. NAS may offer specific features such as scheduled backup or FTP access; it depends on the model. NAS is a great solution for charities that want to easily back up a lot of data. You can also back up data from a NAS via an external drive to store offsite.

For larger networks and disk space requirements, a storage area network (SAN) is a network of storage devices that is accessed and shared via standard network communications. If you want to use NAS or SAN, you must have a robust network that can properly support fast data transfers within the network.

CDs, DVDs, and portable flash drives are convenient and cost-effective, but they are inappropriate as your organization's primary local backup solution. They are less secure than other backup solutions, and they discourage best backup practices, such as completion of incremental backups. However, they can be great if you need to:

- Create quick copies of critical files. If you store critical files on a CD, DVD, or flash drive, you'll be able to easily access your files without specialized backup hardware or software, and without an Internet connection.
- Transfer files from one computer to another.
- Archive old data. CDs and DVDs are appropriate for the storage of data that you won't need to modify, such as photos and finished printed materials. Plus, disks make your archives portable, which makes it easy to store a copy off-site.

Backup Software

For individual users, Windows and Mac OS operating systems both have built-in backup tools.

In Windows 7, the backup functionality can be accessed from **Control Panel > System and Maintenance > Backup and Restore**. In both Windows 7 and Windows 8, different versions of the same file are kept for easy restore. This, however, requires that the computer be available and accessible in order for you to be able to access those previous versions.

For Mac OS, Time Machine is the backup feature that comes with the operating system. You can set up the location and schedule as well as the files you wish to back up. Older backups are deleted based on the space that is available in your backup location.

These built-in tools for backup are adequate for individual computers. However, a dedicated program such as Symantec's Backup Exec or System Recovery is preferable if you have the resources to pursue an organization-wide strategy. A dedicated backup program allows for more detailed refinement of the backup options, as well as more sophisticated management of multiple computers. It allows for a wider view of all the data that is backed up, for example, and less intervention on the actual computer itself.

Backup for Mobile Devices

As mentioned previously, it's important to consider whether you should back up the mobile devices that you use regularly for work. Here are some instructions for the major mobile operating systems.

Android

With Google's mobile operating system, Android, you can link your phone or tablet data with your personal Google account. Google's backup program includes your Android settings (such as your WiFi networks and passwords) and your Google application settings (such as your browser bookmarks). It also includes the apps you install from Google Play.

Backup of your phone or tablet information to your Google account is a simple process on phones that have Android 4.1 (Jelly Bean) as their operating system. Go to **Settings > Personal > Backup & Reset**.

However, your phone may have the Android 4.0 (Ice Cream Sandwich) operating system. If so, go to **Settings > Privacy** on your phone and check the boxes that are labeled **Back up my settings** and **Automatic restore**. Be sure to specify to which Google account you want to back up your data.

For documents, you can download the Google Drive app and store your files in the cloud. This way, the documents themselves are not stored on the device, and you merely access them from it.

You can upload your phone or tablet's photos to Google Picasa directly from the Gallery app in Android.

Lastly, if you use Google Chrome on your desktop, your bookmarks will be automatically synced with your Google Chrome browser in devices that have the Android 4.1 operating system and up.

Windows Phone

Similar to Android, you can now easily back up your data on a Windows Phone if you link it to a personal Microsoft account. This includes your SMS conversations, apps and app settings, call history, photos, theme, and Internet Explorer Favorites (bookmarks). You can change your backup settings if you navigate to **Settings > System > Backup**.

Microsoft's cloud storage service, SkyDrive, is built into the phone's operating system. Your photos and Microsoft Office documents are saved automatically to your SkyDrive account.

You can also download the free SkyDrive app, which lets you easily share and view your files or photos with others. The free SkyDrive account comes with seven GB of storage, but some phones come with more; it depends on what type of phone and which carrier you have.

Windows 8 and Windows RT Tablets

Like Windows Phone, Windows 8 and Windows RT tablets can use SkyDrive to back up files to the cloud.

Windows 8 and Windows RT tablets also have a feature called File History. This is a backup application that continuously protects your personal files that are stored in Libraries, Desktop, Favorites, and Contacts folders.

File History periodically scans your file system. Then, it backs up any changes to an external hard drive, a network share (such as a NAS), or a Storage Space (Window 8's new RAID tool).

Apple Devices

If you own an iPhone or iPad, you can avoid a lot of extra work to back it up. This is because iCloud does much of it for you automatically. iCloud is Apple's device syncing service. It backs up your device settings (such as your wallpaper, contacts, and calendar data from your various apps), messages (SMS, MMS, and iMessage), and much more. It also backs up photos and videos from your camera roll. You get five GB of storage for free; if you need more storage, you'll have to purchase an upgrade. You get unlimited storage, however, for purchased music, movies, apps, and books from iTunes.

iCloud is available to iPhone, iPad, or iPod Touch running iOS 5 or later. Backup will run on a daily basis as long as your device is connected to the Internet via WiFi and connected to a power source with the screen locked. For more on iCloud pricing and backup, see Apple's dedicated iCloud site.

You can also use iTunes to create backups of your iOS device either manually or automatically. When you plug in your iDevice, you'll see a button that is labeled **Devices** in the upper right-hand corner. Click that and it will open up a summary of your device. You should see the **Backups** section, which gives you the choice to either automatically back up to iCloud or do a full backup of your iPhone or iPad to your computer (locally). If your iOS device crashes, you can then restore from that locally saved backup.

A good strategy might be to automatically back up your iDevice to iCloud and then back it up manually once or twice a week to your computer. If you have a Mac that runs Mac OS X 10.5 or higher, you can use Time Machine to handle incremental backups of your iTunes library.

About Remote Backup Solutions

Online backup programs that are automated require an Internet connection and the appropriate software to back up the data to a remote location. You must first install the software on every computer that contains data that you want to back up, identify the files and folders to be copied, and set up a backup schedule. The software then sends copies of the files to a remote repository via the Internet.

Keep in mind that online backup differs from online file storage sharing. Online file storage services such as Dropbox, Google Drive, or SkyDrive do mitigate some of the data-loss issues with data stored on premise. This is because your data is stored in the cloud and is not tied to a physical location. But, these services are not designed as a repository for backups.

Online remote backup moves the data out of your office and to a third-party facility, usually a large, shared datacenter. This means that you can avoid the initial capital expense of the purchase of backup equipment. And in the event of a disaster, you can still recover critical data, if the facility was unaffected by the same disaster. This is ideal for small organizations with more than three workstations. These small organizations probably need to store critical information such as donor lists, fundraising campaign documents, and financial data. However, they also probably lack the equipment or expertise to set up dedicated on-site storage. For organizations with many more workstations and data, it is worthwhile to compare the costs of on-premise and remote solutions. This is because it may become

more cost-effective to keep the backups in-house (and periodically move them off-site, as recommended previously).

Because you will need to entrust critical data to a third party, make sure you do your due diligence. You need to ensure that the backup provider that you choose is reliable and financially secure. Otherwise, you might end up with a company that has poor data-protection habits or goes out of business. Here are some tips to select a remote backup provider:

- Support — Verify that the level of support is appropriate for your organization's needs and budget.
- Redundancy — Your data should reside on multiple servers, even multiple physical locations if necessary. Ask for specifics about each provider's storage facility and whether it is redundant and accessible in case of an area-wide disaster.
- Security — Your charity's sector may have special regulations that pertain to it, such as regulations that address health information. If so, confirm with the facility about whether it will be compliant with the regulations.

Here are some other important questions to ask:

- Are there additional charges to the base price? Will the company notify you if you are near your allotted storage capacity, and how much do they charge if you exceed that capacity?
- Has the provider built its own datacenter, or do they co-locate with a third-party provider?
- How do they secure physical access to the equipment where data is stored?
- What credentials are needed to physically access the datacenter?
- Who has network access to the machines that store your data?
- Does the backup provider automatically encrypt your data? Or do you need to do so yourself beforehand?
- Does the provider offer a guarantee or insurance of a successful recovery?

These questions will help you avoid unpleasant surprises and ensure that copies of your critical information are secure and available.

Chapter 4: Documentation and Your Master Key

It's important to have the following information available in a form that's easily accessible. It needs to be available for anyone who might be asked to repair, restore, or change your organization's tech infrastructure.

- Warranties and receipts for computers and peripherals
- Information about where, how, and how frequently your data is stored and backed up
- Instructions for how to restore your data
- Passwords for encrypted data
- Contact information for any employees, volunteers, or consultants who maintain your organization's tech infrastructure
- A phone tree that includes home and cell phone numbers for all staff. The phone tree should follow your normal chain of management, which means that each manager will contact her direct reports in case of an emergency.
- Login information for administrative accounts on all computers
- Login information for web hosting and backup services
- Contact information for web hosting and backup services (if there's an account representative devoted to your account, include their name and contact information)
- Software registration information, and that includes keys

You may have pieces of this information that are scattered in various binders and email accounts. However, it's worthwhile to take the time to compile it safely and accessibly in one place. If you lose your web hosting information or communication with the one volunteer who knows all of your passwords, a disaster can be exacerbated.

Storage of Your Documentation

We recommend a three-tiered approach to the storage of your documentation: hard copies, personal storage devices, and online. It's essential that you keep the hard copies of your documentation somewhere that is sheltered from both natural disasters and theft. Examples include a waterproof safe or a safe deposit box.

You should encrypt electronic information, unless encryption will hamper recovery. In both cases, keep copies in two different places that are unlikely to be hit by a single disaster.

In addition, it is crucial that the information is updated and consistent with the changes in your office. Inaccurate information at a time of disaster recovery is worse than no information at all. You can schedule a time every three months to ensure the data is current.

The Master Key

Your master key is a portable USB flash drive. Here, you'll keep all information that you'll need to restore your technology infrastructure after a disaster or to respond to any other unforeseen incidents. It's a place where you can compile all of your important documentation and other crucial information

safely and conveniently. Flash drives range in prices, but you may want to invest in a "ruggedized" USB drive that will better withstand physical damage.

It's easy to store the documentation that is listed above and any other essential data on a flash drive. But, you should encrypt that data to make it less readable if it becomes misplaced. There are numerous secure flash drives on the market that automatically encrypt and password-protect any data that's saved on the drive. Some of these drives include additional features such as fingerprint scanners or automatic deletion of files after a certain number of incorrect password attempts.

A less-expensive alternative is to use a standard flash drive with a special encryption application. FreeOTFE and TrueCrypt are two free applications that you can use to secure the drive. Both applications give you the option either to encrypt an entire disk or create an encrypted, virtual disk. A virtual disk can then be stored on either an internal or external drive. You can also copy either application onto your flash drive and execute it directly from there, which makes it easy to access your encrypted files from any computer without the need to download new software.

Who Should Have a Master Key?

How many people at your organization should have a master key? That depends on a number of factors. How many people in your organization have the authority to make time-sensitive decisions about your tech infrastructure? At the very least, the executive director and one other person should have a key.

When you consider who should have a master key, think about the problems that could befall your charity. For example, perhaps your charity is located in a flood-prone area. If so, ideally the person with the master key should be a trustworthy staff member who lives in an area that's safe from floods.

Back Up Your Documentation

There are various approaches to storage of your documentation online. What's most important is that it's easily accessible for you and your fellow decision-makers, but impervious to accidental or malicious security breaches. In this case, it makes sense to use online file storage. A company such as Google, Microsoft, or Dropbox has the resources to devote to security and ensure global redundancy.

For a greater level of security, you can encrypt the files before you upload them, and ensure that their access privileges cannot be changed except by an administrator. These files are not designed to be edited online, but only downloaded if you are unable to access the originals or the ones that are on your master key.

Chapter 5: Staff and Training

It is useless to have a disaster plan if your staff is unaware of it or if they forget about its existence. For many charities, even those who regularly work in disaster zones or work with the needy on a daily basis, staff training on disaster preparedness is inadequate. Here are some guidelines to raise awareness within the organization:

- The moment a new member joins your organization, your backup plan will need to be updated. The new staff will create more data. They may need to travel or work from home part of the time. They may use their own mobile device in the office, or be assigned one. All of the above factors are reasons to review your backup plan and revise it if necessary.
- All new staff should be required to read your backup plan, especially any organization-specific information. This ensures that they are informed of your organization's setup. They may also make suggestions to improve the plan that are based on their experience in their previous jobs.
- Staff should meet regularly, at least once a quarter, to review the disaster plan, and to verify documentation. It is advised that you meet more frequently during the season in which there's a greater likelihood for a disaster in your region.
- Just like a fire drill, you should simulate disasters that affect the regular operations of the organization. It can be as minor as an Internet outage. How will your staff respond? Did the backup last run properly? Did the restore work as expected? You can then do a post-simulation analysis to fill in any gaps in the plan, or with staff who needs additional training.

Likewise, when staff leaves the organization, your plan and documentation needs to be updated as well. Additional tasks include:

- Archive the former employee's email (don't delete it). Forward the emails that are sent to that address to the former employee's manager.
- Change any passwords that the employee had access to, and that includes passwords for the organization's presence on any social networking sites. If applicable, have the employee make a list of any accounts and passwords that he set up on behalf of the organization.
- If the employee had a master key, or passwords that decrypted files, be sure to change those as well. If his fingerprint was used for access, be sure that you are able to access the data before his departure.
- Back up the former employee's computer. Reformat it before you give it to another employee.
- Keep a list of up-to-date email addresses for former employees. This is useful for two reasons. First, it allows you to forward any personal messages that an employee might receive at her old email address. Second, you might discover in a disaster that the employee forgot to document a crucial piece of information.

Part II: Recovering from Disaster

Part II is intended for organizations that need to recover their IT systems after or during a disaster. We'll explain the process of triage. During triage, you choose priorities and determine which programs you must continue through the recovery process and which ones can be slowed or paused. Next we'll discuss how to recover or replace hardware, your network, Internet access, and your website.

Chapter 6: Basic Equipment Recovery

In this chapter, we will discuss recovery steps for a disaster that affects more than a single workstation — one that affects your entire office.

To recover from a disaster is difficult even in the best of circumstances. The fear and panic, and the need to decide things quickly, make it difficult to complete a thorough, in-depth assessment and planning process. Technology is unlikely to be your top priority after an earthquake, fire, flood, or other catastrophe. However, if you can set aside a few minutes to address some key issues, it will help your organization to recover. And you can then return quickly from crisis management to normal day-to-day operations.

A sequence of safety > communications > priorities > full recovery is ideal. Circumstances might prevent you from a full assessment of your situation and prioritization among competing options.

Technology Triage

So first, your organization will identify what needs to be done and in what order. Then, you can focus and work to obtain the resources, funds, advice, and technology that you will need to begin the recovery process.

Every organization will have different technology priorities after a disaster. However, there are some general guidelines that can help you to develop a good technology triage list:

1. Communication is very important. In most cases, the first priority during and immediately after a disaster is to reestablish communication with the outside world. If the disaster is widespread, communication systems are likely to be overwhelmed, so prioritize who needs to be reached first.
2. Consider your constituents. Focus on services, functions, programs, and audiences first, before you consider machines, networks, and applications. Some questions that you may want to ask are:
    - Who supports you?
    - Whom do you support?
    - Who relies on you the most?
    - Who might suffer as a result of the disaster and be in need?
    - Which programs must continue through the time when you will rebuild?
    - Which ones can be postponed?

The demand for your services may increase after a disaster. So you need to be realistic about how many constituents you can serve if your organization suffered damages.

3. Identify essential data and information. Determine what data and information your organization needs to operate effectively in the short- and medium-term. Use this information to decide which equipment to repair first. Restoration and repair of systems can take a significant amount

of time. In order to succeed at triage, you will need to focus your efforts where they will have the most impact.

4. Consider backup systems. If you planned properly for disaster, you should have stored backup media in a safe place that you can access. In the event that the backup media and hardware are unreachable or unusable, you'll need outside help to recover the data. If you have data that is stored in a remote system, you may lack the consistent power and bandwidth to sufficiently restore your system. Focus on the data and systems that will have an immediate impact post-disaster.
5. Think about your server(s). The server is the core of many networks. To recover it may be a high priority, since it is essential in order to recover your data and to restore your network. Only attempt to recover the server if the power and network are in good enough condition to warrant its revival.

You may need to recover very important data from a machine that is physically damaged (and for which you lack a backup). In this instance, we strongly recommend that you hire a data recovery professional.

General Safety Tips

Ensure that you have a safe environment before you begin the recovery process. For your own safety, observe these precautions:

1. If the floor, any electrical wiring, or computer equipment is wet, make sure the power is off before you enter the room or touch any metal, wet surfaces, or equipment. If you're certain that the power is off and that it is safe to move the equipment, move it to a safe, dry environment with reliable electric power.
2. If you need to use temporary extension cords and cables, make sure that you follow safe procedures. Cords and cables should either be placed where they won't be walked on or taped to the floor to provide protection in high-traffic areas. Be sure that the cables are rated for the device and appliance that they are connected to.
3. Make sure that tables are sturdy enough to support the equipment placed on them. Make sure that stacked equipment will remain upright and stacked, especially when it is connected to cables or other peripherals. Allocate a little extra time to make sure everything is stable, neat, and orderly. If you fail to plan properly and you rush to restore equipment to its original condition, it often leads to undesired consequences.
4. Once you have a safe, dry environment, it's important to make sure that you have good, reliable electric power before you connect or turn on any computer equipment. A good first step is to plug in an electric light to make sure it shines steadily and provides the same amount of illumination that it normally would. You can also try to plug in things you can afford to lose and test them out. An example of something you can afford to lose might be a radio or any other device that requires only a small amount of power. You may need to purchase or rent power-generating equipment to clean up, charge devices, or verify equipment — it depends on the urgency and situation.

5. To avoid power surges and brownouts, turn off and unplug computers when they will be unused for an extended period. If a lightning storm is expected or the power goes out, turn off and disconnect computers and other sensitive equipment. Keep them off until the power is back on and stable. Power surges often occur when the power returns. Computers should have a backup system for short-term power or uninterruptible power supply (UPS), which also provide isolation. Laptops are isolated by their power supplies and batteries, but reliable power is still important to avoid damage. Your UPS may have exhausted its battery power during an outage, but its surge protection capabilities may be unaffected.
6. Ventilation is also very important. Make sure the vents on any equipment are unblocked. Computers can run in a warm environment as long as they have adequate ventilation. Avoid the tendency to put computers right next to each other or position the vents next to desks or cabinets. Use a fan to keep the air in motion in the room and around the computers if you think they might get too hot. Turn computers off if you leave the room and let them cool down before they are turned on again. Consider whether you can work during the cooler part of the day and turn off computer equipment when it is too hot to work comfortably.

Hardware Recovery Tips

Once you have verified the operating environment, proceed to assess the situation with your hardware.

1. Clean and dry hardware that you intend to revive yourself. Postpone or avoid any attempt to plug in or operate a computer until it's completely dry and free of mud, dirt, or other debris. Your computer may work, but if you turn it on prematurely, you can destroy an otherwise healthy machine. It's important to open up the chassis of your computers to make sure they are clean and dry inside and out. If there's any debris, remove it carefully so that you protect the computer from the tendency to overheat from reduced air flow.
2. If you need to touch or put your hand or tools near any part inside the computer, wear a wrist strap with electrostatic discharge (ESD). Or, you can work on an antistatic mat. If you lack a wrist strap or mat, touch a grounded object (such as metal water pipes) before you touch the computer. Before you open the computer's case, be sure all power sources are turned off, the computer is unplugged, and laptop batteries are removed.
3. Make sure devices such as routers, switches, and printers are completely dry before you power them up. If possible, wait to attach peripherals and cables to computers or avoid this entirely, unless you are sure the equipment works properly.
4. Check your components twice. Even if a computer fails to start right away, put it aside to check later. Be sure to sort and label the equipment. These actions allow you to figure out what does work and what is broken. After that, you may be able to build computers that work from operational parts of different broken computers. Use your triage list to focus your efforts where they will make the most impact.
5. Once you get a computer to run, back it up if its data is more recent than your backup's.

Reestablish Communications

Reliable communication — both external and internal — will be essential to rebuild your infrastructure and to continue your core programs.

Your staff may need to work at home and/or use mobile phones. If so, you can have your office numbers temporarily forwarded to the appropriate landline or mobile numbers. Most hosted VoIP services allow you to redirect lines to outside numbers. If you have Internet access either via the fixed or mobile lines, consider using Skype or a similar softphone service. It may be that your disaster recovery effort will continue for a while; if so, you should also consider whether to use alternate messaging services such as Whatsapp or iMessage instead of SMS.

Change all of your outgoing voicemail messages to include basic information about your charity's efforts to rebuild. The message should briefly outline any changes in your organization's services and instructions on how to stay informed.

Your staff may need to use personal mobile phones for work during the recovery effort. If so, find out whether their mobile plans include enough minutes per month to cover the increased usage. If they lack sufficient minutes, it can be much less expensive to temporarily upgrade them to unlimited minutes rather than reimburse overage fees.

Your organization may also lack consistent access to the Internet. Even so, your web presence is a central way to inform the public. You can tell them about your organization's recovery efforts and any changes to the services that you provide. If power and Internet access is consistent enough, you should be able to update your website normally. If you are still in recovery mode, a more direct method would be to update your Facebook and Twitter statuses with whichever device is operational. You should also take the opportunity to communicate with your allies to coordinate and potentially pool resources.

Network Recovery

In the case of a flood or other inundation, a local area network (LAN) can be badly damaged. Network cables can become waterlogged and cease to function. Patch panels and jacks may also be damaged; switches, hubs, routers, and other electronic devices on your network may be shorted out by the water. Full restoration of your network to its original condition can take time and effort. It may be worthwhile to try to get a few devices back on first.

First, verify that the networking devices are safe to use. After this, try to plug in your modem to a reliable power source and see whether the lights come on as they normally would. Usually there would be a green light and a label such as "online" and "power." It is possible that the settings were saved during the outage. If the modem has LAN ports, you can try to connect your computer in directly rather than use your regular networking devices. This is a good short-term solution until you or your IT consultant are ready to do more detailed reconfiguration. If it is safe to do so and there's a need, expand the network by the addition of a hub or a switch.

Once you have a hub or switch that works in place, you can start to connect computers to the network via standard Ethernet cables. Try to run the cables along the base of walls and out of the way of foot traffic. Ethernet cables are easy to trip over, and when pulled abruptly, can break connectors and jacks and pull equipment to the floor. If you need to run a cable across a traffic path, try to tape the cables to the floor to keep them out of the way. (Note: When you pull up taped-down cables, try to pull the tape off the cable while it is still on the floor. If you pull up the tape and cable together, it is likely that the tape will wrap around the cable. This can be very difficult to remove.)

Prior to the disaster, your organization may have had a wireless network installed. If so, it may be more efficient to use the wireless network first to access the Internet, because it is easier to add additional users. A wireless network is also less reliant on a static location. However, you may lack access to certain servers — it depends on your network configuration — so do be aware of potential limitations. You may have had wireless access from your broadband modem previously and your settings may have been retained. If so, then you should be able to use the same wireless settings as before. If wireless access has been lost, you will need to reconfigure the modem. You should refer to the documentation that you have set aside as recommended in earlier chapters, or via the master key of information.

Mobile Internet Connectivity

In times of disaster recovery, there will be a greater reliance on mobile networks for both personal and official business. Numerous agencies, private citizens, and relief groups need to use the same networks to communicate with one another within the same region. Therefore, it would be ideal if the organization prioritized the use of this scarce resource.

If regular fixed broadband is currently nonoperational, but your work or personal mobile broadband is available, you should use it as needed.

Data Recovery

If you have backup, you can try to restore it only if your equipment is stable enough for recovery. If you have a NAS or removable hard drive, verify that its status lights come on. Also check that you do not hear any abnormal sounds when you plug it in. However, if there is even a remote chance that your power is unstable, then you should abandon the attempt to restore.

Look for other places where you may have inadvertently stored your data. Perhaps you emailed copies of your files to a consultant and what you need is in their inbox. Perhaps printouts of the data exist that you can re-enter (data entry is often less expensive than hired help from technology experts). If you do find a copy of your data, back it up and make a copy before you do anything else. Only use this copy and save the original in case something goes wrong with the duplicate.

If you have lost data during a disaster and your backup plan lacks a strategy to address this sort of catastrophe, there is still hope. The information that follows can help in your data recovery efforts:

- Look for the name, type, and, model number of your computer anywhere on the case.
- Try to find the recovery discs for the operating system.

- Remember to consider warranties and manufacturer support. Call the manufacturer to see if they can help fix your computer.

If the lost information is extremely important to your mission (such as your donor list, for example), you may want to pay for data recovery. There are a lot of companies that recover data. Costs vary — it depends on the level of damage and the amount of reconstruction that is necessary.

How to Manage If Passwords Are Lost

Even though a system is functional or revived, you still may have lost the passwords to access it. Here are some ways to restore access.

- Windows computers — There are many ways to restore a lost Windows password, and it varies by the version. Generally, it requires that you download an image file to create a boot disk, or download a piece of software to overwrite an existing password. This can be a complicated process, so unless the recovery is extremely urgent, it is advised that you leave this process to your IT consultant.
- Apple computers — You can use a Mac OS installation CD to reset the passwords on a computer.
- Routers, firewalls, and other network equipment — If you still have it, check the instruction manual that came with the equipment. Most network equipment comes with default passwords. All equipment can be hard-reset to the factory settings — usually you push down the reset button during startup or in a set pattern. If the manual that you need is lost, you may need to search for it on the Internet via another connected device.

If You Need to Move Your Website

Your normal web host may have been located in an area that was badly affected, or you may have hosted your website yourself. If so, you may need to move your website to a host in a more stable area. This should be done only if you have confirmed with the web host that their disaster recovery is unable to meet the standards of your organization. In other words, check their blog or social networking presence; if you discover that they will still be nonfunctional by the time when you will need them, move your website to a host that is unaffected.

While this is normally straightforward, it becomes difficult if the details about your site are poorly documented. If you're in that situation, this section will help.

A website consists of typically three (plus one) components, all or any of which may have been affected:

- Domain registrar — Your website's domain name (www.mywebsite.org, for example) is different from your site's content, which is stored by a web hosting provider. Although your domain name can be registered separately, it is often registered with a hosting provider.
- Web hosting provider — A web hosting provider supplies the disk space and network for your website. You may also have hosted your own website. If so, you may want to move this hosting to another provider after a disaster in order to restore your website as quickly as possible.

- Web content — You may have backups of your website. However, if you lack these, you may want to publish a simple page quickly with contact information and status updates for your supporters. If you are unable to do that, you may want to temporarily post a blog separate from your usual hosting provider. A service like Blogger.com or wordpress.com will host a blog for free. If you use social networking and microblogging sites, you should post frequent status updates.
- Email hosting — Your email may be hosted by an outside provider: either the same service as your web hosting provider, an Internet Service Provider (ISP), or elsewhere. Or you may have hosted in-house.

Below, you'll find guidance on what to do if:

- Your website is inaccessible.
- You need to move your email to another host.
- Your website is unaffected, but all of your access records and passwords are gone.

For each of these situations, you will need to get as much information as you can about your current host and domain registration. If your own records have been mislaid, tools on the website DNSstuff can help you find this information, if you can get online.

To retrieve your site's information on DNSstuff.com, enter your domain name in the site's WHOIS lookup box. The resulting WHOIS information page will tell you:

- The registrar ("Registrant")
- The contact person for the domain ("Administrative Contact")
- The name server and IP addresses ("Discovered Name Servers")

Scenario 1: Website Is Inaccessible

If your web hosting company is down and you need to get some sort of presence on the web as soon as you can:

1. Choose a New Web Host.

You likely do not need to re-register your domain name (see below), but you will need to pay for a new web hosting service. The ability to pick the right platform is important if you have backups of your site, which may have been built on a specific platform. It's also important if you hope that your original web host will return and you want to maintain the same platform in case you switch back. Your website may have included a database on the web host's servers. If so, the availability of the correct database platform (for instance MySQL, or MS SQL Server) is also essential. Finding a web host can be a daunting task, but it is advised that you find a reliable one with redundancy and resources.

2. Update Your Domain Registration.

Once you have paid for a web hosting service, you have to update the information at your domain registrar. This will "point" the address of your domain to the new web host (as opposed to the old one). Often, you can do this if you log in to your domain registrar's control panel and update the information

yourself. However, it depends on the registrar — you may need to contact your web host directly and ask them to do it. If this is the case, be prepared to prove who you are. The same is true if your domain was previously registered by a company that is now defunct and you need to transfer your domain name to a registrar that is still operational.

In the best scenario, the person (or entity) listed as the admin contact in the WHOIS information that you looked up on DNSstuff.com will match the current contact information. Some registrars, given the circumstances, may be flexible around these issues. However, times of disaster are often ripe for fraud. So it is likely you will still be required to convincingly prove who you are before you can transfer domains. A registrar's website will usually provide contact information in case you have lost your password or your admin contact information is outdated.

3. Upload Your Website.

Once you have set up the web host and domain registrar to point to the right address, you can begin to upload your web pages. This is true for simple contact pages (if you lack any backups). It's also true for the original website if you do have backups and have access to them.

Scenario 2: Email Hosting Is Down

If your web hosting company also previously hosted your email, you will want to use your new web host to also provide your email hosting. You will need to update what is called your mail exchange (MX) record, which is similar to an update of your website's domain address. Typically, your email host will give you information about what your MX record should be (usually it's an address like mail.mydomain.com or an IP address).

Scenario 3: Records Are Inaccessible

Maybe you can access your website, but you lack any of your access records or passwords. In this case, you will need to contact the domain registrar (or web host). After they verify your identity, ask them to change your login and password information.

Thankfully, most of the basic steps you'll need to take to find domain registration information are outlined by the WHOIS lookup on DNSstuff.com. Use the lookup to find the relevant information under the "Sponsoring Registrar."

You can also see who registered your domain for you. It may have been registered by an individual at your organization (in which case that person may have the login and password information). Or it may have been registered by your web hosting company. If the latter is the case, your domain registration may still be current, but you will be unable to directly access the domain control panel. In this case, you will need to request the IP address and MX record updates, and will be unable to update them yourself. Ask your web host to help you.

The key to prove who you are — the admin contact listed in the WHOIS record — is usually listed after the "registrant" information. Sometimes the email address is masked, which makes it harder for you to find out what email address to use to contact the registrar. Hopefully, the street address is correct (and matches your letterhead), because this makes it easier to send written requests.

If you are uncertain who your current web host is, you can try to look at the bottom of the WHOIS page for a "Name Server." Sometimes, this is obvious (dns.webhostcompany.com), while other times this is just an IP address. You can also use DNSstuff.com to do a "reverse lookup" of an IP address to find the site name for your organization. Note that this will only sometimes reveal who the web host is, however.

If your organization previously hosted its website on premise, the WHOIS results can be very confusing. So, try to resolve any internal network or server issues before you get lost in recursive searches.

Chapter 7: Guidelines for Non-Technical Disaster Planning and Recovery

This chapter is designed to help you to identify, assess, and recover vital personnel, services, and equipment after a disaster. Use the checklists and charts below to ensure that the recovery process proceeds as smoothly as possible. They will help you to manage your personnel and assets throughout the process.

Quick Disaster Checklist

The following checklist[1] is a quick reminder for all staff on how to prepare and respond:

How to prepare:

1. List all aspects of disasters so that the IT department can think of appropriate solutions to address any possible disaster.
2. Train employees and volunteers on your disaster plan before a disaster strikes. A disaster rehearsal may be useful.
3. Save instructions for a disaster on every desktop.
4. Provide necessary toolkits for a disaster for each employee too.

How to respond:

1. Announce the emergency to staff, volunteers, and stakeholders immediately.
2. Ask employees to follow the disaster instructions.
3. Deliver the materials and toolkits for aid.
4. Repair or replace damaged computers and their accessories as soon as possible.

People and Deliverables

To recover from a disaster, it's important to respond quickly and effectively. Identify needs, prioritize resources, and communicate clearly. The checklist below can help you to organize people and communication during a crisis. This will enable you to accurately analyze the impact of the disaster on your organization and to prioritize recovery efforts.

Personnel and Communication Guidelines

- If you have a plan, then follow it as you did in your practice drills. While some things will happen differently than you pictured them, most things will probably go as planned.
- If you lack a plan, then you need to determine how you will proceed; decide who will do what, and when.
- Once you have determined who in your organization is responsible to decide what, ensure that there is also a process in place to cross-check these decisions.

[1] Courtesy of Ruishen Sunding from Peizheng College in Guangdong, China.

- Beware of individuals who make drastic decisions, especially if these decisions could put lives at risk. In addition, some people feel that they must be in the midst of the action to be helpful. Try to harness this energy — delegate tasks that are appropriate to their skills and the situation's needs.

- Avoid the tendency to assume that first responders will keep you informed. (First responders are employees of public services that handle emergencies and other aspects of public safety, such as public utility crews, emergency response teams for communities, and firefighters.) Always assume that the danger continues to be a threat. Contact first responders to ensure that you receive accurate and current updates on the status of the situation. These agencies and personnel may also require information from you.

- Make sure that you rely on a dependable news source for information. If you have the resources, appoint someone to handle public relations in order to ensure that the information that you receive and send out is consistent.

- Contact staff via a phone tree that follows your normal chain of management. Instruct top-level managers to contact their direct reports and so forth, so that everyone is covered. To do this, you will need to create lists of home and cell phone numbers that are both up-to-date and readily accessible.

- Establish a help desk or two — one for customers and one for staff — to avoid the possibility that you might overwhelm the switchboards.

Once the above process is set in place, you can begin to evaluate and address the disaster's likely impact on the organization.

1. Will you require contingency suppliers who are third parties (such as salvage companies, or computer room suppliers who are mobile)? Even if you're still uncertain, it may be worth it to contact them and notify them of potential need.

2. Set up project teams and get key decision makers to meet regularly.

3. Make it clear to staff that only staff who are absolutely essential should come in to the office to help. As tasks are delegated to those staff, establish a communication protocol for status updates.

4. Keep the situation and environment controlled and professional at all times.

Deliverables Checklist

☐ Plan of action
☐ Staff phone tree
☐ Recovery document that identifies where important data are kept, such as:
    - Key allies
    - Main donors

- Funders
- Contractors

☐ Supplier contact list
☐ Supplies for your new work environment

- Desk
- Telephone
- Diary or notes
- Paper
- Pens or other instruments to write with

☐ Your organization's current floor plan. This will help when you need to make new arrangements or if you plan to need more space.

Tasks and Deliverables Chart to Track Progress

Use this chart in conjunction with the Deliverables Checklist to ensure that required tasks are completed after a disaster.

Task	Start Date	End Date	Expected Deliverable

Operations

Use the charts and guidelines that are below to identify the technology and personnel that are required to keep your operations functional after a disaster.

Technology Priorities Assessment

Use this chart to identify the essential applications that are required to operate your organization. Determine which applications are needed over the next 24 hours, the next three days, and the next week.

Department	Location	Application	Workstation/Server ID	Needed Within 1 day?	Needed Within 3 Days?	Needed Within 7 Days?

Technology Refresh: Key Recovery Staff

Here we assume that all staff are available. Given that is true, the table below allows you to identify the personnel who are essential to recover your systems and where these systems will be recovered.

Service Type	Assigned Personnel	Location

Project Planning and Rollout

Plan your recovery carefully, and consider whether you should conduct a practice session. A day's worth of planning can save you time, energy, and pain.

- Transport requirements — List the transportation you will need (cars, taxis, public transit) during the recovery phase. Remember to include parking and any special requirements.
- Expense codes — Keep track of expenses so that you can inform funders about the impact of recovery on your finances. Consider whether you should track all time spent on recovery with an expense code (a special one for disaster recovery) when your accounting systems are operational again, for example.
- Accommodation — List all accommodations that you need during your recovery by both type and duration. Remember to include additional items like food and other supplies.
- Maps and directions — List maps and directions that you may need during recovery. For example, you could use an online mapping service to save maps and directions to the nearest hospital, fire station, or community center.

Communications

Use the forms below to keep track of contacts that you'll need during your recovery.

Technology Recovery Contacts

Name	Role (Such As Network, Database, Systems)	Type of Vendor (Such As Consultant, Company, Corporation)	Preferred Contact Method (Email/Mobile/IM)	Contact Info

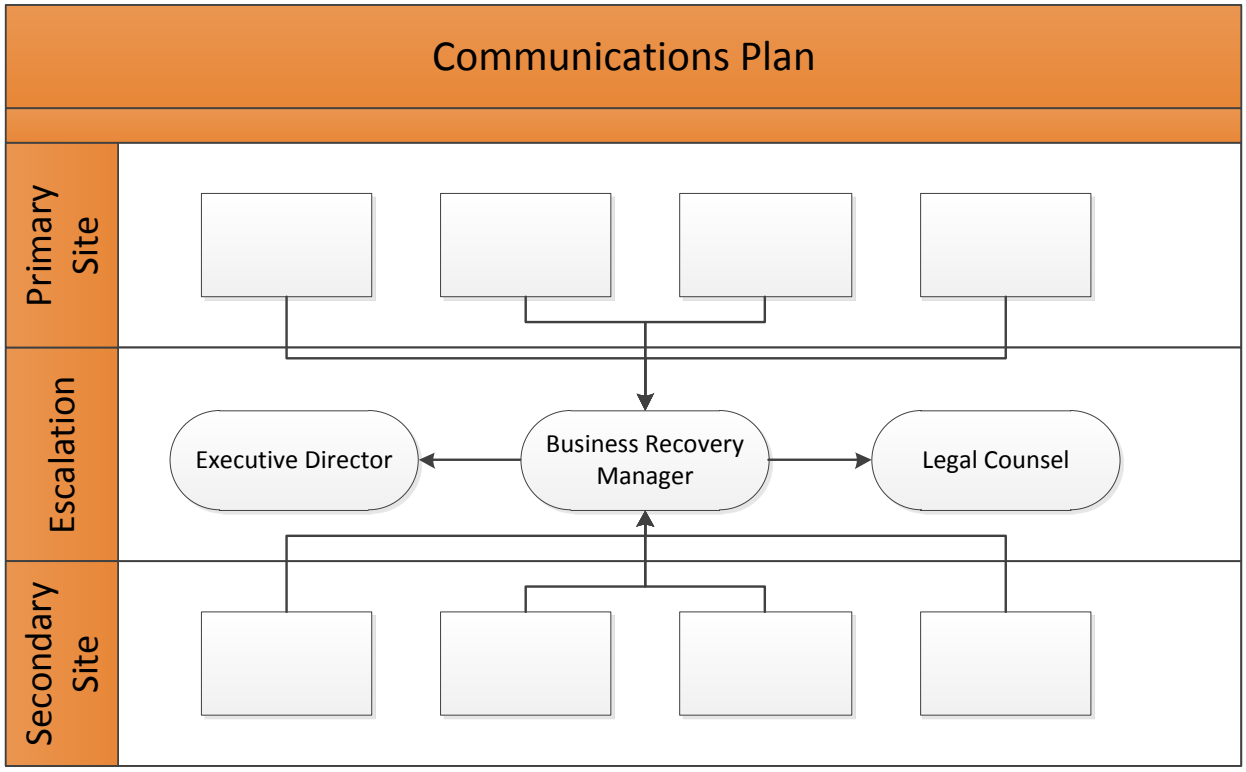
An internal list of contacts is a good way for everyone to know who to call during the recovery process, or if a certain individual needs to be prompted notified of specific developments.

Contact List for Internal Escalation

Name	Role During recovery	Location	Job Scope	Mobile Contact

Communications Plan

A diagrammatic communications plan will help your organization visualize the channels of communication during an emergency. Every organization's structure, personnel, and culture facilitate a different set of processes. Here is an example of a communications plan for an organization with two sites and one designated business recovery manager:



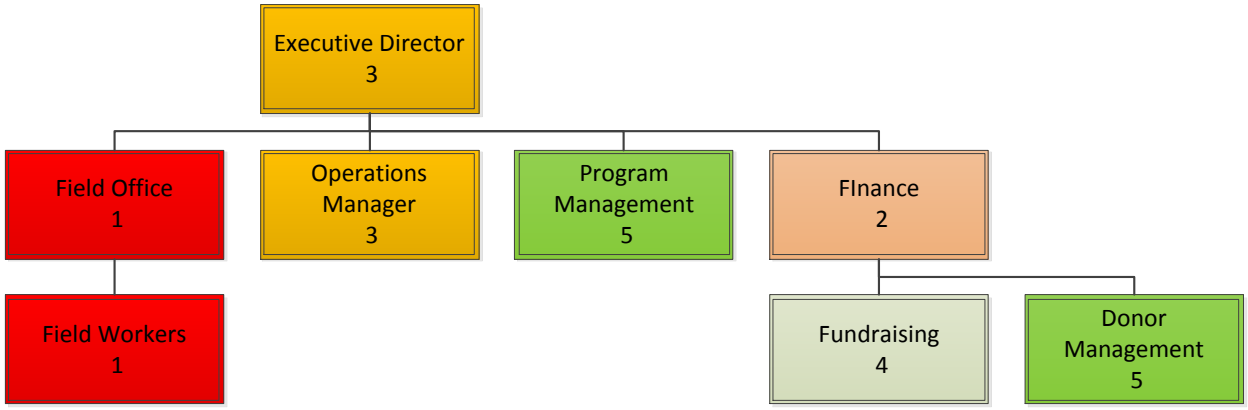
Business Impact Assessment Questionnaire

Create an organization chart for your business unit. Then, rate each department or division in terms of its unavailability in the event of a disaster. Use this scale:

1. Most important to immediately accomplish our mission
2. Significant damage

3. Serious damage
4. Major impact
5. Minor impact

The sample organization chart below shows how a community health clinic rated its departments.



Legal and Regulatory Requirements

Are there any legal or regulatory requirements or penalties for loss or delay of the service provided? If so, it would be crucial to note this:

Service Whose Delivery Is Required	Regulation Requirement	Penalties? From Delay/Disruption/Either?	Responsible Party	Provision Verified? (Yes/No)

Consequences of the Inability to Perform Functions

Under the following headings, please indicate your assessment of the business impact if your organization were unable to perform this function during the recovery process. Estimate the potential impact to your constituents if this function is paused.

Operations	Immediacy	Potential Impact	Assumptions	Justification for Interruption

Additional Costs

Estimate what additional costs (fines, claims, cancelled contracts, lost discounts, interest payments, etc.) the organization would incur if operations were not restored after a disaster.

Operations	Immediacy (1/3/7 Days)	Lost Revenue	Other Costs	Penalties for Non-Provision	Total Costs

Health and Safety

Use the chart below to outline how health and safety might be compromised if certain processes were not performed after a disaster. Rank them in their importance to business continuity.

Process	Responsible Party	Immediacy	Rank (1 – 5)

Work Flow Relationships

Use this section to describe the work flow relationships that are relevant for your organization.

Internal Party	External Party	Work Received/Sent?	Type of Work	Rank (1 – 5)

Data and File Recovery

The following charts serve as a way to organize and see what data is missing.

Report Requirements

Use this chart to keep track of all of the reports that you have and need. Note if a report is of a central or critical nature and its special requirements.

Report/File Name	Author	Last Modified By	Last Known Location	Encrypted?	Priority (High/Mid/Low)	Recovered?	Checked Out By

Voice Recovery

Use this chart to identify your phone requirements after a disaster.

Number at Primary Site	Replacement Available?	Necessary at Recovery Site?	Single Line?	Two Lines?	Speakerphone	Recording	Private Line?

Supplier Contact Details

Use this chart to keep track of your suppliers and any information that could be relevant to restore continuity.

Supplier Name	Contract Type	Reference Number	Contact Details

About This Guide

This is the second major revision of *The Resilient Organization: A Guide for Disaster Planning and Recovery.*

The initial version of this guide — originally titled *Restoring IT Infrastructure: A Manual for Disaster Recovery* — was written shortly after Hurricane Katrina struck the southern United States in 2006.

Based on feedback from the first version, in 2009 we added additional instructions for disaster planning. We had also surveyed organizations whose input helped enrich this content. Many of the organizations we surveyed had had their work disrupted by wildfires, earthquakes, and hurricanes, but those weren't the only disasters reported. There were a few stories of sabotage from former employees, one organization whose office was destroyed by an angry mob, and even one organization that had a vandal walk in during office hours and smash a computer. Nearly all of the disasters reported resulted in damaged computers, lost data, or both. Although 86 percent of the organizations we surveyed back up their records on a regular basis, only 69 percent have clear documentation of how and where critical data is stored. Remember that regular backups and clean, clear documentation go hand in hand.

In 2013, we made the information more concise and actionable, as well as made some key revisions pertaining to cloud and mobile adoption. We also translated the guide into certain languages for our global audience, and produced it in e-book form.

Contributors

Andrew Conry-Murray

Ariel Gilbert-Knight

Elliot Harmon

Kevin Lo

Ginny Mies

Chris Peters

Bryan J. Sharkey

Partners

Cisco (http://www.cisco.com/)

Collaborating Agencies Responding to Disasters (http://www.cardcanhelp.org/)

ONE/Northwest (http://www.onenw.org/)

Symantec (http://www.symantec.com)