The Resilient Organization: A Guide for Disaster Planning and Recovery

Version 2.0, August 18, 2009

If you adapt all or part of this guide for a particular organization type, country, or disaster, **we'd love to see it** and, if applicable, publish it through our various channels. Send us an email at btc@techsoup.org.

Contributors

Andrew Conry-Murray
Elliot Harmon
Kevin Lo
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/)

In This Guide

Introduction

TechSoup created the first version of this guide — originally titled *Restoring IT Infrastructure: A Manual for Disaster Recovery* — shortly after Hurricane Katrina struck the southern United States and left numerous nonprofits and public libraries scrambling for solutions. Although many organizations told us that the information and recommendations in the first guide helped them get back on the ground more quickly, many of you pointed out that the guide was only half written: where were the instructions for disaster *planning*? We hope that this version is the answer to that question.

Don't think of the suggestions in this book as mere precaution against a natural or man-made disaster; think of them as tips for keeping your organization limber and ready for any new opportunity or challenge. Using our suggestions for documentation, backup, and unified communications, you can build a tech infrastructure that will be reparable after a disaster. Perhaps more importantly, though, you can use those same strategies to serve your constituents in new ways when an unexpected opportunity arises. The provisions that ease rebuilding your tech infrastructure also let you build an ad-hoc office to carry out your mission in a new place or circumstance. For this reason, we hope that this guide will not only prepare you for a crisis, but deepen your nonprofit's impact in times of health too.

Who Should Use This Guide

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

One unfortunate irony is that for many nonprofits, disasters are the times when your constituents are most in need of your services. Part of a recovery plan, therefore, is a triage phase in which you evaluate which programs must continue to receive full staff attention and which ones you can slow or pause during the rebuilding process. This guide is intended to help you simultaneously continue key operations and rebuild your infrastructure.

Although some of our recommendations may still be applicable, this guide is not intended for NGOs whose continued efforts in a time of disaster may be putting their staff in danger. If your NGO is trying to recover during a civil war or other period of political upheaval or if your work requires your staff to stay in an area in

which a disaster is taking place, you might find more appropriate information from your local Red Cross or Red Crescent.

This guide necessarily focuses on your technology infrastructure in disaster preparation and recovery. Of course, disaster preparation and recovery have other components — including financial and human resources issues — which we unfortunately can't cover in depth.

Laws and standards about encryption and security vary a lot from country to country. Please consult materials appropriate to your country for specific security recommendations, especially if you manage health records or any other data protected by law. In the United States, health data is protected by the Health Insurance Portability and Accountability Act (HIPAA). For information on making sure your database meets HIPAA standards, see the Idealware article In Search of HIPAA-Compliant Software.

In Search of HIPAA-Compliant Software
http://www.techsoup.org/learningcenter/software/page11924.cfm

How to Use This Guide

This guide is divided into two sections, *Preparing for Any Predicament* (Page 10) and *Disaster Recovery* (Page 41). It goes without saying that for nonprofits who are recovering from a disaster, the second section will carry more immediate relevance than the first (and vice versa); regardless of your current situation, however, reading the entire guide can give you a deeper understanding of the issues surrounding disaster planning and response. If you're improving your nonprofit's preparedness, reading about the recovery process will inform many of your decisions. If you're rebuilding after a disaster, this is the perfect time to think about ways in which you can make your new tech infrastructure nimbler.

If you're focusing on disaster preparedness, we've provided a checklist on Page 40 to guide you through the process. The checklist summarizes most of the recommendations in the book; it's an easy way to keep track of tasks and track your progress.

As you document the technologies and strategies you implement in the disaster preparedness section, you'll simultaneously be *creating 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, with this guide and other resources as supplements.

If you're already in recovery mode, Chapter 9: Post-Disaster Operations Analysis (Page 67) is intended to help you through the triage process and development of your recovery plan. The worksheets in Chapter 9 parallel Part II of the guide so you can complete them as you work through the recovery process.

Printing This Guide

You might find it worthwhile to print the guide so that you can continue to refer to it during the disaster planning or recovery process. Please consider saving paper by duplexing (printing on both sides of the page) or using a print management tool. For more information on using paper responsibly, see TechSoup's Reduce Your Paper Use campaign.

	Duplexing: How to Print or Copy on Both Sides http://blog.techsoup.org/node/579 Choosing Print Management Software http://blog.techsoup.org/node/575 Reduce Your Paper Use http://www.techsoup.org/greentech/paper/

Symbols in This Guide

The following symbols appear throughout the book:

 **Additional Resources:** To make the book easy to use in both electronic and printed forms, we've provided both URLs and clickable links for additional online resources.

 **Tips and Warnings:** This symbol denotes information that can save you time or help you avoid a dangerous situation.

 **Your Stories:** We surveyed over 300 NGOs around the world in research for this guide (see footnote on page 11). This symbol denotes results from the survey and follow-up interviews as well as stories from other contacts in the nonprofit sector.

 **Excel Charts:** Chapter 9: Post-Disaster Operations Analysis includes several example charts to aid your operations analysis. The charts are available for your use in an Excel file, which you can download from our Disaster Planning and Recovery Toolkit (see below).

Additional Resources

More resources are available in TechSoup's Disaster Planning and Recovery Toolkit. Throughout this book, you'll see links to additional resources at TechSoup.org and elsewhere on the Internet, formatted like this:

Disaster Planning and Recovery Toolkit
http://www.techsoup.org/toolkits/disasterplan/index.cfm

We encourage reader collaboration using the tsdp (TechSoup Disaster Planning) tag in social bookmarking site Delicious. In each chapter of this book, we provide a link to a set of tsdp-tagged bookmarks. For example, in the chapter on backup you'll find the following link:

Delicious:tsdp+backup
http://delicious.com/tag/tsdp+backup

For easy reference, all of the additional resources we reference in this book are also tagged in Delicious. If you find additional resources that you think would be useful for others, you can add them by tagging them tsdp (along with any other pertinent tags) in Delicious. This is the first time we've tried to facilitate collaboration in this way, and we're excited to see what resources readers will bring to the community.

Part I: Preparing for Any Predicament

Disaster preparedness isn't just about being ready 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 by adopting certain technologies and strategies, you can deepen your nonprofit's impact and make your work faster and more efficient.

In this section, we'll discuss simple strategies to prepare your nonprofit or public library for new challenges and opportunities. First, we'll talk about communications strategies that work just as well outside your office as inside. Next, we'll help you document essential processes to reduce downtime during an emergency. Later, we'll discuss backup strategies to protect your data from computer damage. Finally, we'll talk about ways to protect your systems from man-made disasters, malicious and otherwise.

Chapter 1: Your Office Is Everywhere

As we said in the introduction to this book, disaster planning isn't just about being ready when a fire or flood damages your computers. It's a way of thinking about your nonprofit'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 unbounded by technological limitations, an organization whose office is everywhere.

Disasters Happen Everywhere

Many of the organizations we surveyed[1] 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.

The point is that disasters happen everywhere, and there's no way to prevent every possibility; instead, focus on operating your organization in such a way that it can resume operations swiftly.

Unified Communications

Delicious: tsdp+unifiedcommunications
http://delicious.com/tag/tsdp+unifiedcommunications

Unified Communications Options for Nonprofits
http://www.techsoup.org/learningcenter/networks/page11697.cfm

Unified Communications (UC) refers to a large family of technologies and organizational practices that simplify and integrate multiple forms of communications like phone conversations, email, video and web conferencing, instant messaging (IM), voicemail, fax, and SMS messages.

The central idea behind UC is that if an employee can access and reply to a message using whatever device is convenient at the moment (regardless of what sort of device the message was generated on), 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 not require employees' physical presence in the office.

[1] In research for this book, we surveyed a total of 346 NGOs and public libraries in 12 countries. The survey was open both to organizations that had had disasters damage part of their IT infrastructure and ones that hadn't. We also had follow-up discussions with a several organizations. Some of the respondents we cite chose to remain anonymous.

Evaluating Your Organization's Needs

Remember that UC refers not only to certain technologies, but also to business practices that encourage a smooth flow of communications among several media; thus, before selecting a UC strategy, it's a good idea to take an inventory of how your organization currently communicates both internally and externally. 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? After you implement a UC solution, whose job will it be to maintain it? 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 choosing the best technical approach. Train your staff to use new communications solutions and make sure they have time to learn and ask questions.

Selecting and Implementing a Unified Communications Strategy

Hosted VoIP Services

Adopting a hosted Voice over IP service can deepen your organization's ability to communicate during a disaster. A hosted VoIP service in the office is functionally similar to POTS (plain old telephone service) lines, but it doesn't require that all employees work in a single, physical office. During a disaster, an employee can bring VoIP equipment home and use it with her home Internet connections, or have the VoIP service forward her calls to a mobile phone.

There are numerous VoIP services on the market. Two services with a strong focus on unified communications are Vonage and 8x8, Inc. An organization can sign up with either service for a monthly fee of approximately 40 to 50 dollars a month for each phone line.

8x8 uses a special, Internet-connected phone, while Vonage provides an Internet router with a standard telephone jack. Both services can deliver voicemail messages by email. Both also allow users to receive calls out of the office by ringing one or more phone numbers at the same time as the office phone. 8x8 also allows users to place calls from a mobile phone, which is especially useful for organizations that need to place a lot of international calls. For an additional fee, Vonage offers a voice-recognition service that can transcribe voicemail messages and send them to users by email or SMS.

BetterWorld Telecom provides VoIP and other telecommunications services exclusively to nonprofits and sustainability-focused businesses. BetterWorld offers a free audit, in which a representative can examine your current

telecommunications setup and recommend a suite of services to improve your UC capabilities and reduce your cost and environmental footprint.

Unlike 8x8 and Vonage, BetterWorld offers a private branch exchange (PBX) service independently of its VoIP service; in other words, BetterWorld can enhance the UC capacity of your current public switched telephone network (PSTN) system even if you don't want to switch to VoIP. Look at BetterWorld's Solutions page for an overview of the telecommunications services they offer. BetterWorld holds a strong commitment to environmental and social justice issues.

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.

List of Commercial VoIP Services
http://www.dmoz.org/Business/Telecommunications/Services/VoIP/

Betterworld Telecom
http://www.betterworldtelecom.com/

Vonage Features
http://www.vonage.com/features.php

8x8 Business VoIP features
http://www.8x8.com/business_services/

Voicemail-to-Email Online Services

Depending on your workflow and the size of your organization, a voicemail-to-email service could greatly help you in a time of 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, generally allowing 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 simply forward the email message. Popular services include Google Voice (formerly Grand Central), YouMail, and RingCentral. Many of these services also let you have a single telephone number that will forward to multiple numbers at once.

	Google Voice https://www.google.com/voice/ YouMail http://www.youmail.com/ RingCentral http://www.ringcentral.com/

Electronic Fax Services

If your nonprofit uses fax messages, you might want to consider an electronic fax service like MyFax. In a time of disaster, you might be away from the office or no longer be able to use a landline fax line; with an electronic fax service, you'd still be able to send and receive messages. These services are discussed at length in the TechSoup article Electronic Fax Alternatives for Your Nonprofit.

	Electronic Fax Alternatives for Your Nonprofit http://www.techsoup.org/learningcenter/techplan/page10992.cfm MyFax Offering at TechSoup Stock http://www.techsoup.org/stock/Category.asp?catalog_name=TechSoupMain&category_name=Protus

Your Backup Web Presence

	Delicious: tsdp+website http://delicious.com/tag/tsdp+website

In many ways, your nonprofit'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 nonprofit will turn to your website for updates. Unfortunately, maintaining your website during a disaster — let alone adding needed updates — may be too difficult, especially if your computers are damaged. That's why it's a good idea to construct a backup web presence that you can use during a crisis to keep your constituents informed.

It's good to think about how you're using technology to reach out to your community long before a disaster strikes, for many reasons. We don't have time to go the nuances of your nonprofit's social media strategy here, but here are some resources to get you started:

	Eight Secrets of Effective Online Networking http://www.techsoup.org/learningcenter/internet/page8075.cfm New Media, Old Media, and Your Nonprofit http://blog.techsoup.org/node/690 Expand Your Reach with Flickr and Twitter (Webinar, requires name and email address) https://cc.readytalk.com/play?id=04jpzxrp We Are Media http://www.wearemedia.org/

Depending on the needs of your organization, it might be a good idea to set up an emergency website that can keep followers aware of developments surrounding a disaster more quickly than your regular site. For example, you can send updates to your Twitter feed from mobile phones and other devices, so you can communicate with friends of your organization through Twitter even without a computer or regular internet access.

We've created an example of a simple ad-hoc website that displays an organization's Twitter feed automatically using Javascript. During an emergency, you could add essential information to the top portion of the page, including contact info and any changes to your organization's programs and services. Since the page displays your Twitter updates automatically, it's easy for your volunteers, donors, and constituents to stay in the know.

If the main way you communicate with your constituents online is through a blog or Facebook page, you can use the RSS feeds from those sources to display updates on your emergency homepage as well.

What's most important is that your emergency website display up-to-date news and contact information, especially if your organization provides support to people impacted by disasters.

	Sample Emergency Website http://backup.idiolexicon.com/ How to Add a Twitter Feed to Your Website http://remysharp.com/2007/05/18/add-twitter-to-your-blog-step-by-step/ Displaying RSS Feeds on Your Website http://www.techsoup.org/rss/rsswebsite.cfm

Chapter 2: Documentation and Your Master Key

	Delicious: tsdp+documentation http://delicious.com/tag/tsdp+documentation

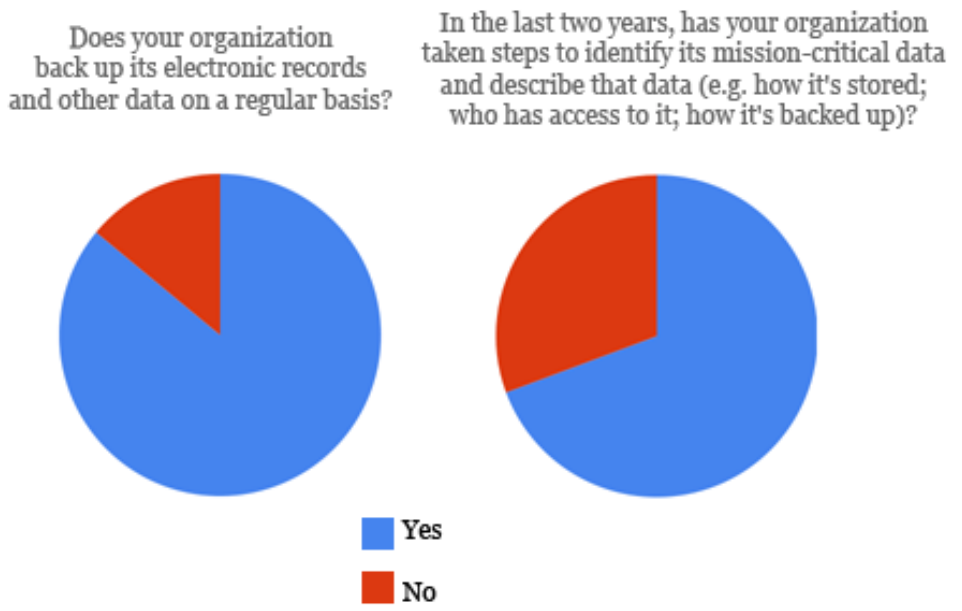
Documentation is your first and most important defense against a disaster, natural or otherwise. No matter the state of your technical infrastructure, you should have the following information available in a form that's easily accessible for anyone who might be tasked with repairing, restoring, or changing 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, with each manager contacting 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 his or her name and contact info)
- Software registration information, including keys

Although you may have pieces of this information scattered in various binders and email accounts, you'll thank yourself later for compiling it safely and accessibly in one place. Losing your web hosting information or communication with the one volunteer who knows all of your passwords can exacerbate a disaster.

	**Mac users:** See Apple's instructions for exporting your Keychain data.
	Exporting your Keychain data (Mac) http://support.apple.com/kb/HT2980#key

Backups and Documentation



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.

Storing Your Documentation

We recommend a three-tiered approach to storing your documentation: hard copies, personal storage devices, and online. It's essential that you keep the hard copies of your documentation somewhere sheltered from both natural disasters and theft, such as a waterproof safe or a safe deposit box. For electronic information, be sure to encrypt it (see Encrypting Your Master Key below). In both cases, keep copies in two different places that are unlikely to be hit by a single disaster. As one nonprofit told us after recovering from Hurricane Ike, "Consider your entire city a potential point of failure."

The Master Key

Your master key is a simple USB flash drive (also referred to as a thumb drive) where you keep all of the information you'll need to restore your technology infrastructure after a disaster or respond to any other unforeseen incidents. It is a place where you can compile all of your important documentation and other crucial information safely and conveniently. Flash drives are available for as little as $15 or as much as $300 USD, but in most cases, you should be able to find a quality drive that meets your needs for less than $50. Flash drives from respected

brands like SanDisk, Lexar, and Kingston are sturdier than generic drives and generally include better warranties. Think of your master key as the nexus of your nonprofit's operations and keep it with you at all times.

One of the nonprofit professionals we surveyed suggested that in addition to the recovery and maintenance information outlined above, your master key should also include essential information about your nonprofit; for example, it might include PDF versions of up-to-date marketing collateral and PowerPoint slides for your rehearsed introduction to your nonprofit's mission and message. This way, you'll always be ready to introduce potential donors, volunteers, or beneficiaries to your nonprofit's work. Although this type of information doesn't necessarily fall under "emergency preparation," having it on hand at a moment's notice is an earmark of an organization that's prepared for anything.

Once a week or so (can vary depending on your level of activity), check the documents on your master key to see if there's anything that needs to be updated.

Essential Contact Information: Are You Ready?

We spoke with the director of development and operations at a human services organization in California. She said that her organization was ready for a hardware failure, with a combination of local and remote backups, with the most critical data being backed up multiple times every day. She admitted, though, that the organization's communications were considerably less prepared.

With a staff of eleven, "Everyone has everyone else's phone numbers programmed into their personal mobile phones. But we also have a youth program for about 25 students and there is only one staff member who knows how to contact their parents. If that staff member were unavailable during a disaster, it could take the rest of us a few hours to find everyone's contact information."

After our interview, she set a meeting with her staff to identify critical information and make sure everyone has appropriate access to it in case of an emergency.

Encrypting Your Master Key

It's easy to store the documentation listed above and any other essential data on a flash drive, but you should be sure to encrypt any sensitive information so that it doesn't get into the wrong hands by accident. If your documentation is in Microsoft Word format, you can encrypt the data directly from Word itself (see File Encryption in Microsoft Office, Page 35).

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 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 that can 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, making it easy to access your encrypted files from any computer without downloading new software.

	Free OTFE http://www.freeotfe.org/ TrueCrypt http://www.truecrypt.org/

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 thinking about who should have a master key, consider the problems that could befall your nonprofit; for example, if you live in a flood-prone area, be sure that it least one is in an area that's not susceptible to flooding. If the executive director does not live in the same city as the main office or is on vacation for part of the year, the decision-maker who works in the ED's absence should have a key.

	**A Note on Passwords** There are various philosophies surrounding how frequently you should update your passwords. In this guide, we've made the decision to emphasize storing your passwords safely over changing them frequently. One thing to note, though, is that it's advisable not to use the same passwords for highly sensitive accounts (like your web hosting and backup services) as for day-to-day nuisance logins (like online newspaper access and other low-security online services). For more information, see the TechSoup article Password Tips for Privacy.
	Password Tips for Privacy http://www.techsoup.org/learningcenter/internet/page6912.cfm

Storing Your Documentation Online

There are various approaches to storing 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. For this reason, we don't recommend storing your documentation on web applications like Microsoft Office Live and Google Docs.

Encrypt your data (see Chapter 4: Privacy and Encryption, Page 34) and upload it to your backup service (see Remote Backup, Page 29). Alternatively, you could send the encrypted files to a webmail account like Yahoo or Gmail (do not send them unencrypted).

Disaster Planning Is for Employees Too

"Employees and volunteers need to have their own personal disaster plans in place as well so they can spend the effort needed at the organization when a disaster strikes."
—Karen Roberts, Senior Resource Association, Vero Beach, FL

Chapter 3: Remote and Local Backup

Delicious: tsdp+backup
http://delicious.com/tag/tsdp+backup

Backing Up Your Data
http://www.techsoup.org/learningcenter/software/page6089.cfm

The No-Excuses Guide to Automated Online Backup
http://www.techsoup.org/learningcenter/internet/page5813.cfm

The best way to prepare for any disaster is to keep your data backed up. There are two broadly defined approaches to backup:

- Remote backup: Your computer automatically sends your data to a remote center at specified internals.
- Local backup: Your computer copies your data to a second hard drive or other media source, either manually or at specified intervals.

Either route (or both) may be appropriate for your nonprofit. One thing to keep in mind is that if you live in an area that's susceptible to natural disasters, then it may not be a good idea to trust local backup alone. It's possible that a disaster could claim both your primary and back-up drives, even if you keep the back-up drive at a different location in the same city.

Regular backups are vital insurance against a data-loss catastrophe. Developing a solid back-up plan requires an investment of time and money, but the cost is far less than the burdensome task of recreating data for which no backup exists.

What to Back Up

Before jumping into a backup solution, you should first put together a list of what assets need to be backed up. Of course you should back up the data on all of the desktops, laptops, and servers in your office, but that might not cover all of the data that your organization may need to recover.

Save Time by Spending Time
Susan at the Eagle's Nest Foundation is no stranger to IT disasters. ENF's remote campsite frequently deals with power and Internet failures. Susan had this to say about regular backups: "It's better to 'waste' the time backing up than to dread the effects of a disaster that could happen any time. Redundancy in communication options is very important, as is having off-site resources for communication when your systems are down. We have two offices in different parts of the state: this gives us an excellent natural backup strategy."

Home Computers and Handheld Devices

Do one or more of your employees, contractors, or volunteers work from home? Are they saving their work on a personal computer? If so, this data should be part of a regular backup strategy.

Many remote backup services allow you to install a client on a home computer and designate specific folders on that computer to be backed up. As a simpler alternative, require that homework be saved to a work computer every day. Employees can do this simply by transferring data on a flash drive or by accessing the office network through VPN (see TechSoup's Introduction to Virtual Private Networking). For handheld devices, refer to the device's manual for backup instructions.

You should also think about keeping an additional backup of essential files *on your mobile device*. For more information, see Backing up Data on Mobile Devices on Page 31.

Introduction to Virtual Private Networking
http://www.techsoup.org/learningcenter/networks/page4775.cfm

Website

Is your organization's website regularly backed up? If you don't know, ask your web hosting provider. Find out how regularly the provider backs up your website data and how recovery is handled if an accident occurs. Be sure to check with your provider: even if they offer a backup service, it may be opt-in only.

Especially if your provider doesn't perform backups (but even if it does), there are many reasons to keep a copy of your website on an office computer. If you start the habit of editing your site on your computer rather than directly through an FTP connection, then you can test the site before uploading it and you'll always have the up-to-date site ready to upload in case of computer failure or human error; what's more, you won't need an internet connection to make edits to your site or find information on it.

Documentation

Remember all that documentation you did in Chapter 1 (Page 16)? Don't forget to back it up too. Keep it on your USB master key, but be sure it's also stored securely in a backed-up folder on your computer (for more about security, see Page 33).

Internal Data

Does your office have a lot of internal data stored only in hard copies? For example:

- Government forms, such as 501(c)(3) paperwork
- Financial information
- HR information
- Contracts
- Leases

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).

Email

If your organization uses an in-house email server, it must be a part of your backup plan. Many email servers include their own backup utilities; check the user's manual for more information. If mail is stored locally on users' computers and *not* on the mail server, the mail folder on each computer must be backed up.

If you only use a popular webmail service like Hotmail or Google Apps for Nonprofits, these services are generally considered safe from hardware failure. If you use a webmail service that was offered through your Internet service provider, find out whether the ISP backs up your email.

	**Tip** Microsoft offers a backup utility for Outlook 2003 as a free download.
	Outlook Add-in: Personal Folders Backup http://www.techsoup.org/learningcenter/downloads/techstructure/page8259.cfm

Bookmarks

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. Check the application's Help tool or consult the web for details.

Social bookmarking sites like Delicious have gained a great deal of popularity in recent years, thanks in part to their immunity to hardware failure. For more information, see the TechSoup article Thirteen Tips for Effective Tagging.

Thirteen Tips for Effective Tagging
http://www.techsoup.org/learningcenter/webbuilding/page5508.cfm

Best Practices for Backup

All backup routines must balance expense and effort against risk. Few backup methods are 100-percent airtight — and those that are may be more trouble to implement than they're worth. That said, here are some rules of thumb to guide you in developing a solid backup strategy.

Plan your backup strategy: Develop a written backup plan that tells you:

- What's being backed up
- Where it's being backed up
- How often backups will occur
- Who's in charge of performing backups
- Who's in charge of monitoring the success of these backups

All of this information should be included in the documentation.

Give highest priority to crucial data: Your database and accounting files are your most critical data assets. They should be backed up before and after any significant use. For most organizations, this means backing up these files daily. Nonprofits that do a lot of data entry should consider backing up their databases after each major data-entry session.

Core files: Back up your core documents (such as your Documents folders) and email files at least once a week, or even once a day. Each organization needs to decide how much work it is willing to risk losing and set its backup schedule accordingly.

Some data is easy to recreate: It is not usually necessary to back up the complete contents of each hard drive — most of that space is taken up by the operating system and program files, which you can easily reload from a CD if

necessary. The only exception is if your organization has a dedicated file server; in this case, it's a good practice to conduct a full backup of your server before every major update so that you have a way to restore its entire hard drive. A proper file server should also be running a server-class operating system, with software or hardware RAID (redundant array of inexpensive disks).

RAID (Wikipedia)
http://en.wikipedia.org/wiki/RAID

Test your backups before you need them. Make sure your backup software has full read-back verification. Design a recovery plan, and try restoring a few files to a different computer at a different location so you can test your plan before you actually need it.

Local Backup

If you use local backups, remember that storing data off-site is crucial. Natural or manmade, any disaster that impacts your computers is likely to impact an external backup drive in the same office.

We recommend rotating 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 is the 2x2x2 rule: two sets of backups held by two people at two different locations. Although it may sound overly cautious, you will be glad to have a system like this in place should disaster strike.

Keep Your Friends Close and Your Backups Distant
In the wake of Hurricane Ike, one organization we spoke with had displaced staff working remotely in four different cities. One staff person reminded us that if you're storing your backups in the same city as your office computers, there's a danger that one catastrophe will destroy both: "Consider your entire city a potential point of failure!" This advice can also apply to remote backup and web hosting services.

Choosing Backup Hardware

Choosing appropriate backup hardware is key to an effective local backup strategy. As with any technology, there are probably several "right" solutions for your organization. Here are some guidelines for choosing backup hardware that will work for you.

- **Determine how much data you need to back up.** Take a look at 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 not impossible to add 1 GB of data per person per year.

- **Choose a backup device that uses media with a storage capacity of at least twice the total amount of data you need to back up.** This will give you room for growth, and will also allow you to perform "incremental" backups on the same tape with a "full" backup. For many organizations, tape drives are a great choice, combining high reliability and reasonably fast speeds with large storage capacities. Tape drives have become the standard in backup media, and with the proper backup procedures in place they are a reliable alternative. For larger organizations with an IT infrastructure in place, tapes are a great choice.

- **Consider your drive's speed and how it interfaces with your computer.** When you have a large amount of data to back up, a big storage device isn't much good if you can't write data to it quickly.

  Internal Drives: IDE and SCSI are common internal-drive interfaces. All PCs have built-in IDE connections, and devices using these interfaces are usually less expensive. Keep in mind that there are also different standards for IDE. Older IDE drives are now called PATA (Parallel ATA) and the newer standard is called SATA (Serial ATA). Be sure to verify compatibility with existing hardware when making a purchase.

  External Devices: Although ultra-wide SCSI is the fastest, you will also encounter devices that use USB and IEEE 1394 (Apple FireWire). Most PCs don't include built-in SCSI adapters, so you may need to add an SCSI card to use an SCSI device. Higher-end server-class hardware comes with a built-in SCSI or the newest standard SAS (Serial Attached SCSI).

  Network Attached Storage (NAS) is a type of device that offers disk-based storage like a dedicated file or backup server, but in a small and efficient chassis. While specific features such as scheduled backup or FTP access depend on the model, all NAS implement some form of hardware RAID which makes them a reliable form of backup hardware.

RAID (Wikipedia)
http://en.wikipedia.org/wiki/RAID

Choosing Backup Software

Having cost-effective and reliable backup hardware is only half of the equation. Many backup devices come with backup software that works for most data-storage needs. The Professional Editions of Windows XP and Vista (but not Home Edition) come with their own backup software under Start > All Programs > Accessories > System Tools > Backup, which are adequate for individual users. For an organization-wide backup strategy, however, a dedicated program such as Symantec's Backup Exec or EMC's Retrospect is preferable. Consult the software documentation for details to determine specific needs. Microsoft offers an in-depth description of the most common types of backup — full, incremental, and differential.

Locating Files for Backup

Once you have the hardware and software in place, you need to know the location of the data you wish to back up. While most Windows users store data in their documents folder, there is also a tendency to keep files and folders on the Desktop, which you'll need to back up as well. Special database- or financial-software packages may store files in their program directories, so be sure to make copies of these, too. Finally, be sure to understand how your email is set up and where your messages (sent and received), calendar (if your email application has one), and contact information are stored.

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. 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

Additional Backup Tools

What about CDs, DVDs, flash drives, and external hard drives?

As organizations' content and data needs grow exponentially, data storage costs are also decreasing. CDs, DVDs, USB flash memory devices, and external hard drives are becoming increasingly affordable. With that in mind, should you use these devices as your primary means of backing up? Here are a few considerations.

Pros

- Low cost aside, the main advantage to using these devices is their ubiquity and accessibility. If you made a direct copy of your files to a disc or flash memory device, for example, they can be easily be read by any modern operating system on another computer (Windows 2000 and above; Linux kernel 2.2.x and above; Mac OS X) with a DVD or CD drive or functioning USB port. This means you can "restore" your data, even without specialized backup hardware. Moreover, in the event of a disaster, you can often recover data more quickly from a CD, DVD, flash memory device, or external hard drive than from a specialized tape format or device.

Cons

- External hard drives, though convenient and cost-effective, may not always be conducive to best backup practices, such as making routine off-site copies or conducting incremental backups.

- Since it is easily readable, from a data-security point of view, direct copies of data stored on CDs, DVDs, flash memory devices, and external drives pose more of a problem in the event of loss or theft. Even with password encryption, this data is less secure than it would be in a harder-to-read backup archive.

Although discs have fewer compatibility issues overall, the data stored on them may not be readable on every workstation, especially if your nonprofit has older hardware or donated machines with varying specifications. With writable DVDs, for example, there are a plethora of standards (DVD-R, DVD+R, DVD-RW, DVD-RW, to name a few). For a guide to formats, read Webopedia's DVD Formats Explained.

DVD Formats Explained
http://www.webopedia.com/DidYouKnow/Hardware_Software/2007/DVDFormatsExplained.asp

Does that mean that CD, DVDs, and flash memory devices, and external hard drives are useless? Absolutely not! Here are some ways to use them:

- Use CDs and DVDs to archive old data. Old information — such as audit records or historical data — may still be of value to your organization. CDs and DVDs are also appropriate for storing data that you won't need to modify, such as photos and finished printed materials. Both generally involve large files that you may need to refer to but aren't likely to go back and change. Archiving old data files to discs is also a great way to supplement your tape-based backup strategy, because it lets you save resources by backing up big chunks of files that won't change. Plus, disks make your archives portable — and it's easy to store a copy off-site.

- Use flash memory devices for transferring files, or as a secondary backup. Flash memory devices are great for making quick, easy, redundant backups of super-critical files such as databases and accounting files.

Standardizing Practices Across Multiple Branches

Cincinnati's Freestore Foodbank serves over 7000 individuals a month in the greater Cincinnati area, and those numbers double in November and December. Before undergoing a major overhaul of their tech infrastructure, the Foodbank's multiple branches had a lot of trouble communicating and working together, both internally and externally. Johnna Higgins writes:

"Our growth was previously hampered by our inability to communicate and share information over multiple sites on a reliable network using standardized software. The servers were old, the software was ancient, and no one had the same version of word processing or spreadsheet software. It was difficult to share files between sites let alone between computers, as well as send things out to donors, board members, or anyone asking for information. Our mail was hosted externally for the upper staff and through POP mail from our internet provider for the remaining the staff. Without a common desktop platform, working together was difficult and cumbersome. There were no backups because the DAT tape drive that was being used had quit working, and there were no monies to replace it. Through the Microsoft donation program at TechSoup, we have been able to purchase software that we would not have been able to afford otherwise, make a multi-year plan for network and desktop standardization, formulate a reliable backup plan, and find a way to protect ourselves from potential disasters, bring e-mail in-house, and work towards bringing stability and security to our organization.

"We began with the implementation of updated server technology. A server was purchased for each site and new server operating software and licenses were purchased and loaded onto them. Having a common operating system helped to end some of the issues that were happening between sites which was a huge time savings for the 1.5 members of the IT staff. It allowed us to take advantage of Active Directory for the first time and control access to files, form policy groups, enforce policies, and helped us to secure some of the holes that were causing problems. From there, the standardization of the desktops began with the purchase of XP licenses and office licenses to bring us up to a level where we could share documents and not worry about what version or what program the document was created in. Productivity rose and fewer client files were delayed in reaching necessary desks as most of the paperwork is now available electronically. This is especially important now because we are seeing more than 200 clients daily.

"One of the most critical purchases that we made was the Data Protection Manager (DPM) software for doing shadow copy/replica backups of our files. It allowed us to take our data and save it off-site by having each site

	have its own DPM server located at the opposite site. It also allowed our user base to recover different versions of documents if they were accidentally overwritten or deleted. This advantage became especially important during the September 2008 windstorms when our Liberty Street location was without power for four days. We were still able to be partially operational because the site's data was protected at another location and was restorable to another server." Read the rest of Johnna's story at TechSoup's Show Your Impact.
	Raising the Bar: Serving Hunger and Poverty in Cincinnati http://www.showyourimpact.org/raising-bar TechSoup Stock: Data Protection Manager http://www.techsoup.org/stock/product.asp?catalog_name=TechSoupMain&category_name=Servers+MS&product_id=LVS-40539&Cat1=Microsoft&Cat2=Servers+MS&CatCount=2

Remote Backup

Automated online backup programs require only an Internet connection, a small software program, and a few minutes of your time. To perform a backup, you simply install the software on every computer containing data you want to back up; set up a backup schedule; and identify the files and folders to be copied. The software then sends copies of the files to a remote repository via the Internet.

Note that online backup is not equivalent to *online file storage*, a service that lets you upload individual files and folders for future retrieval.

Automated online backup is ideal for small nonprofits (say, two to ten people) that need to store critical information such as donor lists, fundraising campaign documents, and financial data, but lack the equipment or inclination to set up dedicated on-site storage.

With local storage, all the data is within your reach — and therein lies both its value and its risk. You can always access your information when necessary, but that information is vulnerable to loss, whether through theft (someone breaking in and stealing computer equipment) or damage (such as a leaky water pipe or a natural disaster). Online remote backup moves the data out of your office and to a third-party facility, usually a large, shared datacenter. This means you don't incur the capital expense of purchasing backup equipment, and in the event of a disaster you can still recover critical data (assuming you choose a remote facility outside the radius of earthquakes, floods, hurricanes, or other potential disasters).

Automation is another key benefit to remote backup. A software program won't forget to make an extra copy of a critical folder; a harried employee at the end of a

busy week might. By taking the backup task out of your users' hands you avoid the problem of, “I forgot.”

Choosing a Remote Online Backup Provider

A downside to online remote backup is that you have to entrust critical data to a third party. Thus, due diligence is required on your part to ensure that the provider you choose is reliable and financially secure. Otherwise, you might end up with a company that has sloppy data-protection habits or goes out of business.

When shopping for a provider, ask to speak with one or two customers who have used that provider. You should also ask for specifics about each provider's storage facilities. The following are some other important questions to ask:

- Has the provider built its own data center, or do they co-locate with a third-party provider?
- What redundancy have they built into their system to ensure that your data will always be available? For instance, do they make backups of your backup?
- Will your information be kept on hard disk or moved to tape? How do they secure physical access to the equipment where data is stored?
- Will your data be stored in a secure facility?
- Who has network access to the machines that store your data?
- Does the backup provider automatically encrypt your data? (Some services recommend that you encrypt your own data before backup.)
- Does the provider offer a guarantee or insurance of a successful recovery?

You should also discuss pricing. Are there additional charges to the base price? Will the company notify you if you are nearing your allotted storage capacity, and how much do they charge if you exceed that capacity?

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

Backing up Data on Mobile Devices

Your mobile device probably doesn’t have enough memory to store all of your organization’s data (nor would it be the most convenient place to do so), but it is worth considering what data it would be most essential to have at your fingertips in an unexpected scenario. In the chapter on documentation, we suggested storing documentation on your device; consider storing your most essential documents there as well; for example, what information or files would be key as you wait to regain Internet connectivity so that you can restore from a hosted backup?

Of course, if you're storing sensitive data on your mobile device, those files must be encrypted. For instructions on how to encrypt your files, see the device's manual.

Alternatives to Regular Backups

TechSoup strongly advises that every organization should regularly back up its critical data. Using the options outlined in this chapter, you should be able to find a backup solution that meets your needs and doesn't break the bank. Recognizing, though, that organizations' needs vary widely and that some organizations may be unable to heed our advice, we cautiously offer some suggestions for nonprofits that can't make regular backups.

If it's impossible to commit to a backup strategy, *keep your organization's documents on systems with backups built into them*. For example, Google offers a special bundle of its Google Apps services free to 501(c)(3) nonprofits. The bundle includes an email and chat client as well as a word processor, spreadsheet, and presentation software, all accessible through any standard web browser. Similarly, Microsoft now offers a web-based version of Office called Office Live Workspace. A free Office Live Workspace account includes 5 GB for storing your files. In both cases, since your information is stored on Google's and Microsoft's servers, loss of data is unlikely, though possible.

Alternatively, you can set up your own self-hosted web applications on your web hosting provider's servers, assuming your provider backs up website data regularly. OpenGoo is a free, open-source suite that includes an email client as well as a word processor, presentation software, a shared calendar, shared bookmarks, and more. You can install OpenGoo on your web server and provide your staff with accounts to access it.

Are these tools as secure as running Microsoft Office and Outlook on your own computer? No, and they're not appropriate for storing highly sensitive information. But for many of your nonprofit's day-to-day operations, they're a better alternative than risking a major data loss. For more information, see Are Web-Based Collaboration Tools Secure? on Page 34.

Of course, should you lose Internet connectivity, online services will be unavailable. Keep that in mind as you determine which files are crucial to store locally.

	Google Apps for Nonprofits http://www.google.com/a/help/intl/en/npo/index.html OpenGoo http://www.opengoo.org/ Google Apps, OpenGoo, and the Future of Office Software http://blog.techsoup.org/node/594

Chapter 4: Privacy and Encryption

Delicious:tsdp+security
http://delicious.com/tag/tsdp+security

What level of protection is necessary for your organization's data? This complicated question will have a variety of answers for different organizations and types of data. In some instances, state and federal laws may dictate a certain level of encryption for sensitive data. In all instances, protecting the people who trust you with their personal information should be your first priority.

Are Web-Based Collaboration Tools Secure?

The most well-known web-based collaboration tools are Google Docs and Microsoft Office Live Workspace; others include Zoho, OpenGoo, and Writeboard. In the past few years, these tools have grown beyond a niche market into a feasible alternative to traditional office software. But how secure are they?

In short, it depends. Since Google Docs launched, there have been a handful of high-profile reports of security breaches. Some incidents resulted from user error (for instance, a user accidentally sharing a sensitive Google document with all of his contacts) while others have demonstrated legitimate security holes. One tech support representative for Office Live Workspace summed up the situation succinctly: "Security has been taken seriously in the development of OL Workspace but we live in an era where major banks, corporations, the White House, and even the FBI have had their security breached by hackers. Decisions on security … have to be taken by users at a personal level."

Note that encryption of individual files is not possible in either Google Docs or Office Live Workspace; your files are protected by a single login password, similar to how most webmail services work. Like Gmail, Google Docs allows Transport Layer Security access; simply point your browser to https://docs.google.com/ and change your bookmark to include the https protocol. These services are fine for planning events or collaborating on fundraising letters, questionable for keeping track of donor data and other sensitive information, and unacceptable for health records or any other information protected by law.

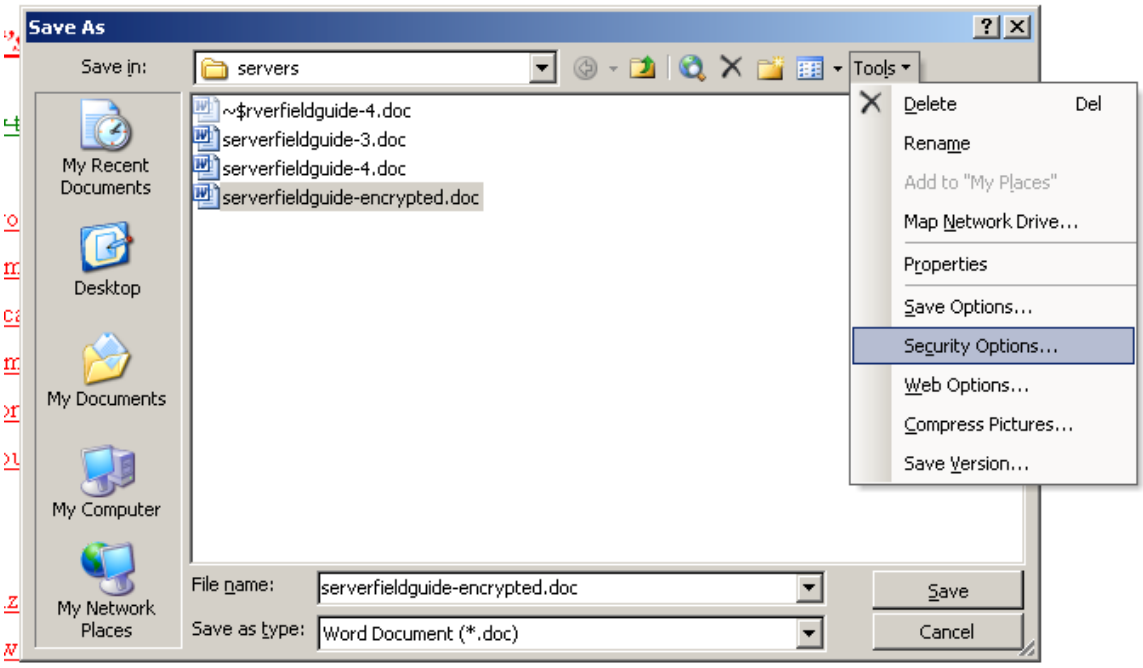
Transport Layer Security (Wikipedia)
http://en.wikipedia.org/wiki/Transport_Layer_Security

Google Docs (Secure Version)
https://docs.google.com/

Discussion on security of Office Live Workspace
http://ask.officelive.com/workspace/qna/t/3941.aspx

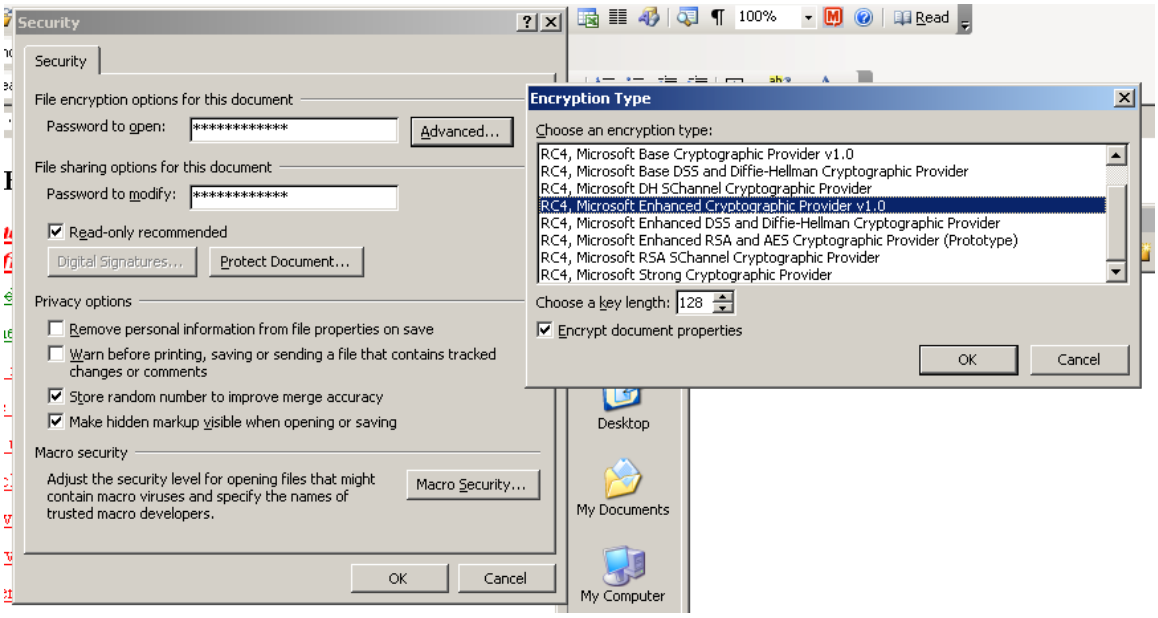
File Encryption in Microsoft Office

There are a few different ways to encrypt individual files with sensitive information. For documents created in Microsoft Office, the easiest way to encrypt is from within Office itself. When you save a document, open the **Tools** menu and select **Security Options**.



The Security dialog box opens. This is where you enter a password for opening the file and, optionally, a second password for modifying it.

Microsoft Office 2003 and later allows file encryption comparable to that used by banks, but not by default. The default encryption method is "97/2000 compatible," which an experienced thief can crack with relative ease. For professional file encryption, use RC4 encryption with a 128-bit key length.



Adjusting File Permissions in Operating Systems

Most operating systems allow users to designate certain files, folders, or drives as accessible only for specified users. Generally, you can find user access information by right-clicking on the file or folder and selecting **Properties**. Below are links to more specific information for each operating system.

Windows Vista Ultimate and Enterprise include Bitlocker, a utility that lets you encrypt an entire volume. For Mac users, you can also encrypt your entire home directory using the FileVault application, included in Mac OS 10.3 and later.

How to Encrypt a File in Windows XP
http://support.microsoft.com/kb/307877

Troubleshooting Permissions Issues in Mac OS X
http://support.apple.com/kb/HT2963

FileVault (Wikipedia)
http://en.wikipedia.org/wiki/Filevault

Bitlocker Drive Encryption (Wikipedia)
http://en.wikipedia.org/wiki/BitLocker_Drive_Encryption

Note that if you're using file permissions to protect sensitive data, you should not stay logged in when you're away from the computer. Shut down, log off, or lock the computer when you're going to step away from it.

Protecting Constituents' Personal Information

Protecting the private information of your donors, constituents, and volunteers is of the utmost importance. If you have not already, password-protect your CRM and donor database applications. (Check the user's manual or help documentation if you're not sure how to do this). Log out of these applications every time you leave the computer.

Many countries have individual laws and standards regarding encryption of personal data, particularly health information; please consult materials appropriate to your country for specific security recommendations. The Health Insurance Portability and Accountability Act (HIPAA) protects health data in the United States. For information on making sure your database meets HIPAA standards, see the Idealware article In Search of HIPAA-Compliant Software.

In Search of HIPAA-Compliant Software
http://www.techsoup.org/learningcenter/software/page11924.cfm

Chapter 5: Human-Made Disasters and Accidents

Delicious:tsdp+humanmade
http://delicious.com/tag/tsdp+humanmade

The measures we've discussed thus far will prepare you for most natural disasters, but what about smaller disasters and accidents? There's no way to prevent every accident, but some minor preparations can minimize the impact of any eventuality.

Protect Critical Organization Logins

Here at TechSoup Global, we employ a simple policy for staff passwords. For any service or application that directly impacts outside users, we don't select the "Remember my Password" or "Keep me Logged in" options. For example, although we may let our FTP clients store the passwords for our internal FTP site, we always manually log in to the FTP site where we house our website. This simple rule keeps staff from accidentally deleting important files from the website.

Similarly, when you're working in your donor database or website, log out of the application when you leave your desk. These policies aren't only about protecting your systems from vandalism; they also protect your systems from simple human error.

End-of-Employment Policy

Have a policy in place for when your organization's relationship with an employee ends, and make this policy available to any employees who would like to see it. Here are some examples of the sorts of things this policy should include:

- Archive the former employee's email (don't delete it). Forward the email address to the former employee's manager.
- Change any passwords that the employee had access to, including passwords for the organization's presence on any social networking sites. If applicable, have the employee make a list of any accounts and passwords he set up on behalf of the organization.
- Back up the former employee's computer. Reformat it before giving 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 an employee might receive at his old email address. Second, you

might discover in a disaster that the employee forgot to document a crucial piece of information.

These measures do not denote mistrust of the former employee. An end-of-employment policy provides for the smooth, professional transition that all workers deserve.

Disaster-Planning Checklist

Here's a quick checklist to keep track of your progress in implementing the strategies covered in this guide. Not every item on the checklist applies to every organization. As you work through the disaster-planning process, be sure to document new technologies and strategies that you implement, and keep staff informed of new procedures and policies.

Chapter 1: Your Office Is Everywhere

☐ Implement unified communications systems or adopt a backup communications plan
☐ Create a backup web presence

Chapter 2: Documentation and Your Master Key

☐ Document all critical systems and processes
☐ Store physical hard copies of documentation safely and securely
☐ Store documentation on an encrypted flash drive
☐ Back up documentation online

Chapter 3: Remote and Local Backup

☐ Choose and implement a backup strategy
☐ Document your backup strategy and train staff members in backup and retrieval
☐ Back up data not included in backup strategy (e.g. website, paper records, etc.)
☐ Routinely check backups

Chapter 4: Privacy and Encryption

☐ Assess security needs for all of your organization's data
☐ Encrypt all critical or sensitive data
☐ Use secure logins for donor and constituent databases
☐ Check compliance with HIPAA or other applicable standards

Chapter 5: Human-Made Disasters and Accidents

☐ Enact a policy for critical logins
☐ Develop an end-of-employment policy and make it available to employees

Part II: Disaster Recovery

Part II is intended for organizations trying to recover their IT systems after or during a disaster. We'll start by discussing triage, the process of choosing priorities and determining 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.

In Chapter 7, we'll offer some tips for repairing a broken computer. In Chapter 8, we'll recommend options for donated, discounted, borrowed, and shared technology. Chapter 9 consists of worksheets and instructions to guide you through post-disaster impact analysis and triage.

There's no way that one book could include instructions for responding to every disaster or accident that could befall an NGO or public library. In developing this guide, we've chosen to favor information and techniques that can apply to a wide range of organizations, which in some cases has meant a sacrifice of depth in particular topics or recommendations for organizations in particularly unusual circumstances. We've included links to several outside resources, and we also encourage you to add your own resources via the tsdp tag in Delicious.

Chapter 6: Picking up the Pieces

Delicious:tsdp+recovery
http://delicious.com/tag/tsdp+recovery

Recovering from a disaster is difficult even in the best of circumstances. Yet while technology is unlikely to be your top priority after an earthquake, fire, flood, or other catastrophe, taking a few minutes to address some key issues will help your organization recover, returning quickly from crisis management to normal day-to-day operations.

The fear and panic that often accompany a disaster, combined with a need to make quick decisions, makes it difficult to go through a thorough, in-depth assessment and planning process. If you have a lot of time to think about your priorities, there are some excellent resources available, which we'll point you to in later chapters; however, in this chapter, we'll assume that you're deciding your priorities in a hurry. We'll also assume that you don't have a document that spells out your recovery priorities. If you do have that document, look there first. The following suggestions might make a good supplement, but the recovery priorities that you and your colleagues decided upon in the calmer times that preceded the disaster will probably give you better guidance than the generic suggestions here.

Safety and communication are the highest priorities in any crisis or emergency. Are you and your colleagues, friends, and family members all in a safe, secure location? Do you have the food, water, clothing, and medical care that you need?

Communicating with friends, family, colleagues, and emergency responders comes next. If you need help, is your message getting to emergency responders, disaster relief agencies, and others? If you're safe, you need to broadcast that message as well so that loved ones and emergency responders don't worry unnecessarily and devote resources to you that should be going elsewhere. Furthermore, most disasters and emergencies are fast-moving, evolving situations where updates about weather, food supplies, disaster response, and other factors can make the difference between life and death. In an emergency situation, communication has to be two-way.

Third, consider your program and service priorities. Who are your constituents and what services do they rely on? Which key financial systems (like accounting, payroll, grant management, and reporting) does your organization need for day-to-day operations? Is your donation-processing system functioning? Donors may be rushing to help you in an emergency, so it might be vital that you recover this system quickly. Also, it's always much easier to discuss and document your priorities before a disaster occurs. It's still necessary and valuable to consider priorities after a disaster, but the pressure of an emergency situation makes it hard to see the big picture.

Of course, this sequence — safety, communication, priorities, recovery — is an ideal one. Circumstances might prevent you from fully assessing your situation and prioritizing among competing options. For example, you might find yourself waiting

in your office for an all-clear signal, unable to reach your IT personnel. In these situations, you can still take steps to diagnose and repair damaged systems.

Technology Triage

Once your organization has identified what needs to be done and in what order, you can focus on obtaining the resources, funds, advice, and technology you need to begin the recovery process. Under ideal circumstances, your organization documented its recovery priorities before disaster struck. However, when this isn't the case, it's still worth taking time to consider carefully the order in which you'll repair damaged equipment and systems.

Every organization is going to have different technology priorities following a disaster, so a one-size-fits-all prescription is not appropriate; however, there are some general guidelines for developing a good technology triage list:

1. **Communication is king.** In most disasters, reestablishing communication with the outside world is the first priority during and immediately after a disaster. In the section below on communication, we'll discuss the reasons that communication channels are so important and some of the different ways you can send and receive information during an emergency. As soon as possible after a disaster strikes, it's crucial to inform any stakeholders whose relationship with the organization might have been impacted.
2. **Consider your constituents next.** Focus on services, functions, programs, and audiences first, before you consider machines, networks, and applications. Who supports you and who do you support? Who relies on you the most? Who might be suffering as a result of the disaster and in need? Which programs must continue through the time of rebuilding, and which ones can be postponed?
3. **Key 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 bring back to life first. Restoring and repairing systems can take a significant amount of time, and focusing your efforts where they will have the most impact is one of the keys to a successful triage.
4. **Backup systems.** If you're lucky, you may have stored backup media in a safe place that you can access. In the event that the backup media and hardware are unusable, you'll need outside help recovering the data. Determining the state of your backup system may be a priority. If you have a reliable network backup system, you may not need to worry about retrieving the data on individual computers.
5. **Servers.** Recovering the server — the core of many networks — may be a high priority for your organization, as it is probably the key to recovering your data and getting the rest of your network up.

To recover mission-critical data from a machine that is physically damaged (and for which you do not have a backup), we strongly recommend hiring a data-recovery professional. (See Data Recovery, below, for additional information on retrieving lost data.)

Quick Disaster Checklist

Guangdong Peizheng College's three campuses in China have occasionally been impacted by power surges and equipment failures. Ruishen Sunding shared with us these disaster preparation and recovery checklists:

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, not after. A disaster rehearsal may be useful.
3. Save instructions for a disaster on every desktop.
4. Necessary toolkits for a disaster should be handy 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.

Reestablishing Communication

As we said above, reestablishing communication should be a top priority. This means establishing communication among the staff and volunteers, as well as communication with donors, beneficiaries, and friends of the organization. Reliable communication — both external and internal — will be essential both to rebuilding your infrastructure and to continuing your essential programs.

Telephone Communication

Are your telephones intact? If not, it's probably a good idea to reestablish telephone communication. If your staff will be working at home and/or using mobile phones, you can contact the telephone provider and 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 (see Unified Communications, Page 11). If you have Internet access, consider using Skype or a similar softphone service.

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

	**Tip** If the staff will be using personal mobile phones for work during the recovery effort, find out whether their mobile plans include enough minutes per month to cover the increased usage. If not, temporarily upgrading them to unlimited minutes can be much less expensive than reimbursing hundreds of minutes overage.
	Softphone (Wikipedia) http://en.wikipedia.org/wiki/Softphone

Internet Communication

Even if you don't have consistent access to the Internet, your web presence is a central way to keep the public informed about your NGO's recovery efforts and any changes to the services you provide.

Make sure your website has clear instructions for where to find the latest updates, be it on a social networking site, blog, microblog, or other venue. If you have temporary internet access (or a contact or volunteer has internet access), it's a great idea to adjust your homepage so that the most recent updates are clearly displayed. One option would be to have Twitter updates appear at the top of your homepage automatically (see Your Backup Web Presence, Page 14).

As a last resort, you could even call your web hosting provider and have them redirect your website to your microblog or other page where you can easily post updates. Of course this tactic temporarily sacrifices the look and feel of your own website, but if there's essential information to communicate to your stakeholders, this is a quick way to do it without Internet access.

Safety – For Yourself and Your Damaged Equipment

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

1. If the floor or any electrical wiring or computer equipment is wet, check to make sure the power is off before you enter the room or touch any metal, wet surfaces, or equipment. If you're positive the power is off and it is safe to move the equipment, it should be moved to a safe, dry environment with reliable electric power.

2. If you have to use temporary extension cords and cables to make connections, they 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 they are connected to.

3. Make sure tables are sturdy enough to handle the equipment placed on them and that stacked equipment won't fall, especially when it is connected to cables or other peripherals. Take a little extra time at this point to make sure everything is stable, neat, and orderly. Rushing and cutting corners may lead to more losses later.

4. Once you have a safe, dry environment, it's important to make sure that you have good, reliable electric power before connecting or turning on any computer equipment. Plugging in an electric light to make sure it isn't flickering or a lot dimmer or brighter than normal is a good first step. You can also try plugging in things you can afford to lose — for example a radio or any other device that isn't power-intensive — and testing them out.

5. To avoid power surges and brownouts, turn off — and, if possible, unplug — computers when they will not be used for an extended period. If a lightning storm is expected or the power goes out, turn off and disconnect computers and other sensitive equipment until the power is back on and stable — power surges often occur when the power returns. Computers you don't want to lose should have a short-term power backup system 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 to the power supply.

6. Ventilation is also very important. Take care not to block the vents on any equipment. Computers can run in a warm environment as long as they have adequate ventilation. Don't put computers right next to each other or with the vents next to desks or cabinets. Use a fan to keep the air moving in the room and around the computers if you think they might get too hot. In general, if you are hot and uncomfortable, it is too warm for your computers to be running. Turn them off if you leave the room and let them cool down before they are turned on again. Consider working during the cooler part of the day and turning off computer equipment when it is too hot to work comfortably.

Hardware Recovery

Warning
If a machine is visibly damaged and its data deemed mission-critical, **stop right now** and skip to Chapter 7: Tips for Reviving Broken Computers (Page 58). Do not power on machines or try out disks that you intend to have professionally recovered.

1. Clean and dry hardware you intend to revive yourself. Don't attempt to plug in or operate a computer until it's completely dry and free of mud, dirt, or other debris. Your computer may be just fine, but turning it on prematurely can destroy an otherwise healthy machine. Take the time 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 the computer won't overheat from reduced air flow.

2. Wear an electrostatic discharge (ESD) wrist strap or work on an antistatic mat if you need to touch or put your hand or tools near any part inside the computer. If you don't have 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 dry before powering them up. If possible, do not attach peripherals and cables to computers unless you are sure the equipment is working properly.

4. Check your components twice. Even if a computer doesn't work right off the bat, put it aside to check later. Once you've got some idea of what is working, and what is not, you may be able to build a few "Frankenstein" computers using functioning parts from otherwise broken computers. Use your triage list to focus your efforts where they will make the most impact.

5. For devices that won't start, check out our troubleshooting tips in Appendix B.

6. Once you get a computer running, back it up if possible. For backup instructions, see Chapter 3: Remote and Local Backup on Page 21.

Network Recovery

Tip
As in hardware recovery, safety is essential in the network recovery process. Educate your staff and volunteers in safety precautions before beginning recovery.

Local Area Networks

In the case of a flood or other inundation, a local area network (LAN) can be badly damaged. Network cabling can become waterlogged and cease to function. Patch panels and jacks may also be damaged, while switches, hubs, routers, and other electronic devices on your network may be shorted out by the water. Fully restoring a complicated network can take time and effort, but it's possible to build an ad hoc LAN quickly.

Wired Networks

To build a simple network, start with an Ethernet hub or switch. Ethernet and TCP/IP networking technologies are the most common networking technologies, and are relatively robust and easy to set up. The hub or switch, which forms the backbone of your network, manages network traffic between the different computers and devices on your network. To create an ad hoc network, just about any hub or switch will do. If you need to add capacity, most devices include a crossover switch or port, which can be used to connect two devices together using a basic network cable. Some newer devices include auto-sensing ports that automatically adjust to connect two switches or hubs.

Once you have a working hub or switch in place, you can start connecting computers to the network using 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 yanked, can break connectors and jacks and pull equipment to the floor. If you need to run a cable across a traffic path, try taping the cables to the floor to keep them out of the way. (Note: When pulling up taped-down cables, try pulling the tape off the cable while it is still on the floor. Pulling up the tape and cable together is likely to result in tape wrapping around the cable, which can be very difficult to remove.)

Most computers include Ethernet network interface cards with RJ-45 jacks (which look like large telephone connection jacks) that connect them to networks. If your computers do not have network cards, they are relatively inexpensive and can be easily installed in any PC.

Wireless Networks

Another option for creating an ad hoc network is to use wireless technologies. The 802.11b and 802.11g standards, often referred to as Wi-Fi, are easy to use and well supported. The older and slower 802.11b standard is less secure, but also somewhat cheaper than the newer, faster, and more secure 802.11g standard. In any event, either technology is acceptable for an ad hoc network.

Wireless networks consist of access points, which are often built into cable and

DSL routers, and wireless network cards, which allow computers to connect to the access point. Access points, much like wired switches and hubs, have limited capacity. For large installations, more than one access point may be required.

Wireless networks, due to their "broadcast" nature, require the use of basic security precautions. There are two common Wi-Fi security technologies. Wired Equivalent Privacy (WEP), which is associated with 802.11b networks, and Wi-Fi Protected Access Pre-Shared Key (WPA-PSK), which is associated with 802.11g networks. WEP is no longer considered very secure, but is adequate for an ad hoc network. WPA-PSK is much more secure, and is appropriate for both ad hoc and permanent networks.

Devices Setup

Once the computers and devices are plugged in to the network, or set up on the wireless network, they may need to be configured. Many TCP/IP networks use Dynamic Host Configuration Protocol (DHCP) to automatically assign addresses and other information to network devices. Most routers and servers include DHCP servers. You may find that your computers automatically configure themselves properly when plugged into the network. If your device has status lights that blink, stay green, or otherwise light up, these clues may indicate that the device works as well. There might also be tips printed on the device itself.

If your network does not have an active DHCP server, you may need to manually configure the network settings on your computers and devices. For Windows, this is done through the Networking or Network Connections control panel. For Macintosh 8.x to 9.x, this is done through the TCP/IP control panel. For Macintosh OS X, this is done through the Network system preferences pane.

For an ad hoc network, you want to set all the computers up on the same subnetwork (or subnet). This means providing each computer or device with its own unique address. We recommend using a non-routable address range, such as 192.168.100.X, with X being any number between 1 and 254. Every computer or device should share the first three sets of numbers and have a different set of final numbers. Each computer should share the same subnet mask, which should be 255.255.255.0. If there is a functioning Internet router on the network, add its IP address as the default gateway.

It's possible to share a network with other organizations in a somewhat secure fashion. Ideally, we recommend using a router to segment off the different parts of a network.

Internet Access

Many organizations have become increasingly reliant on the Internet to communicate, conduct research, and interact with other organizations. There are many options for restoring Internet connectivity; which one is appropriate for your situation depends on what services are available to you and the equipment you have access to. The following section lays out a list of scenarios for obtaining Internet connectivity for temporary offices providing services in an area affected by a disaster.

Options for Restoring Internet Connectivity

The list below compares the benefits and downsides of several networking solutions following a disaster.

High-speed On-Site Connection

Pro: Fast, may be free.
Con: Shelters or service center sites may not have high-speed Internet access.
Equipment/Cost: About $150 for SOHO router and cabling.
Notes: If your organization's host location has Internet access via T1, DSL, or cable, the connection could be borrowed via a wireless access point or a long Ethernet cable, even if you are not in a room with Internet access.

Wi-Fi Bridge (Depending on your location, there may be a Wi-Fi access point near the service site.)
Pro: Can be fast; possibly no per-minute charges.
Con: Somewhat complicated to set up.
Equipment/Cost: Usage charges will vary depending on the type of access. If you can't use an existing, public connection, building your own connection requires a Wi-Fi/ethernet bridge, Wi-Fi cards for computers, cabling, and an Internet router: approximately $400.
Notes: With the right equipment, the signal can be brought onto a wire and redistributed to one or more computers. This may require an antenna mast or the temporary mounting of an antenna to the roof of the building.

Dial-Up (An individual computer dials in to an ISP over a telephone line)
Pros: Works anywhere there is an available telephone line.
Cons: Connection is slow; monthly cost to maintain account.
Equipment/Cost: None for individual computers; about $400 for a dialup LAN.
Note: Several computers could be serviced via a wireless or wireless LAN by means of a router with a built-in modem or a computer with a modem and Internet Connection Sharing turned on.

Sharing a Dial-Up Internet Connection
http://www.ezlan.net/DialUp.html

Mobile Phone or Data Card

Pro: Works anywhere there is mobile service; faster than dial-up.
Con: Depending on the data plan, per-minute and data-transfer charges can add up. In a disaster, connection can be slowed or stopped by an overload of users in a city.
Equipment/Cost (Mobile Phone): Most modern mobile phones can transmit data natively. Some can be used as a modem as well.
Data Card: A one-time price of $150 to $250 per laptop.
Note: Individual computers can access the Internet using either PC cards or mobile phones attached by a cable. This connection could then be shared on a network using Internet Connection Sharing.

Satellite Internet (Dish captures a broadcast signal)
Pro: Works almost anywhere; somewhat faster than dial-up
Con: Expensive; not particularly easy to set up.
Equipment/Cost: About $400 for satellite and possibly LAN equipment.
Note: Can be shared with clients over a wired or wireless LAN.

Sharing a Network

Depending on the scope of the disaster and resources available, sharing a network or Internet connection with multiple organizations may be the most feasible solution available. Sharing a network is relatively simple, but requires some planning so that each organization can get the resources that it needs. Start by setting up the core network where the Internet connection, if any, enters the office. Most consumer and small business networking equipment can theoretically support around 250 separate computers or network devices, though the more heavily used the network, the fewer devices a router will be able to handle.

Organizations with privacy or confidentiality concerns may want to use a second router to subnetwork parts of the network. It's possible to use multiple routers to create a number of different subnetworks that all tie into the core network.

For organizations that have less stringent security requirements, sharing a single network should not present many difficulties. The key to sharing a network smoothly is to set up each organization's computers with a different workgroup name and provide each computer with a descriptive name. In Windows, you can set up computer and workgroup names using the Computer Name tab in the Control Panel. For Macintosh OS 8.x to 9.x computers, you can set the computer name in File Sharing control panel. For Macintosh OS X computers, you can set the computer name in the Sharing System Preference pane. Macintosh computers do not natively use workgroup names.

Data Recovery

If you have lost data during a disaster and your backup plan didn't account for this sort of catastrophe, there is still hope.

In the Technology Triage section of this chapter (Page 43), we talked about establishing what is critical to your organization to operate following a disaster. You also need to decide how much you're prepared to spend on this recovery.

If lost information is mission critical (such as your donor list, for example) you may want to pay for data recovery. There are a lot of companies that do this. Costs can range from just a few hundred dollars to tens of thousands of dollars. One data-recovery vendor offers the following advice:

- Do not attempt to clean or dry waterlogged drives or other media by yourself.
- Do not use common software utility programs on broken or water-damaged devices.
- Do not shake or disassemble any hard drive or server that has been damaged. Improper handling can make recovery operations more difficult, potentially leading to permanent loss of valuable information.
- Before storing or shipping wet media, it should be placed in a container that will keep it damp and protect shipping material from getting wet. Wet boxes can break apart during transit, causing further damage to the drive.
- When shipping your media, package it in a box that has enough room for both the media and some type of packing material to prevent movement. The box should also have sufficient room around the inside edges to absorb impact during shipping. Ship multiple objects in separate boxes or make sure they are separated with enough packing material so there will be no contact.

If you have backups of non-critical and replaceable data, you can try to restore it, depending on the state of the backup media and device. Tapes and CDs can be surprisingly resilient, so try them out even if they look bad. Make sure the media and equipment is dry; if possible, try reading from the tape or CD drive that you originally recorded from. If this doesn't work, try several different CD or tape drives: sometimes you just need a higher quality drive to recover information you thought was lost. However, if there is even a remote chance that you would permanently damage the media, do not attempt a restore.

Lastly, look for other places you may have inadvertently stored your data. Perhaps you emailed your database to a consultant and it's sitting in his inbox. Perhaps printouts of the data exist that you can re-enter (data entry is often less expensive than calling on technology experts). If you do find a copy of your data, back it up and make a copy before you do anything else. Use only this copy, saving the original in case something goes wrong with the duplicate.

Dealing with Lost Passwords

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

Administrative Rights on Computers

Windows Computers: If you have Internet access and are feeling brave, check out the following link for fairly technical details on how to reset the admin rights on most Windows computers.

Forgot the Administrator's Password?
http://www.petri.co.il/forgot_administrator_password.htm

Macintosh Computers: You can use a Mac OS installation CD to reset the passwords on a computer.

- Start up from a Mac OS X Install CD (one whose version is closest the version of Mac OS X installed). Hold the C key as the computer starts.
- Reset Password from the Installer menu (or Utilities menu in Mac OS X 10.4 or later). *Tip:* If you don't see this menu or menu choice, you probably haven't booted from the CD.
- Select your Mac OS X hard disk volume.
- Set the user name of your original administrator account.
- Important: Do not select "System Administrator (root)," which is actually a reference to the root user and not to be confused with a normal administrator account.

Online Services

For online services where you have simply forgotten the password, use the website's password retrieval tool.

If you no longer have access to the user or account name and password, try sending an email message to the staff person who set up the account and ask for your password.

Routers, Firewalls, and Other Network Equipment

Check the instruction manual that came with the equipment. Most network equipment comes with well-known default passwords. Common passwords include (sometimes capitalized, sometimes not):

- Admin

- Password
- Administrator

Most equipment can be hard-reset to the factory settings, usually by pushing down the reset button during startup or in a set pattern. Check the manuals or documentation that come with the device, or check the website of the manufacturer of the device.

Moving Your Website

If your normal web host was in an area that was badly affected (or if you hosted yourself), you may need to move your website to a host in a more stable area. While this is normally relatively straightforward, it becomes difficult if the details about your site are locked in the mind of someone who is unavailable to you. If you're in that situation, this chapter will help.

There are typically three (plus one) components to a website, 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, which is why many people associate the two.

Web Hosting Provider: A web hosting provider supplies the disk space and network for your website. Your organization may even be your own site's hosting provider; if this is the case, you may want to move this hosting to another provider in the aftermath of a disaster, when your hands may be full.

Web Content: While you may have backups of your website, if you do not, you may want to get a simple page up quickly with contact information and status updates for your supporters. If you can't do that, you may want to temporarily post a blog separate from your usual hosting provider (a service like Blogger.com will host a blog for free).

Email Hosting: Your email may also 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 if your website is down; if you need to move your email to another host; or if your website is OK, 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 you do not have your own record, tools on the website DNSstuff can help you find this information.

	DNSstuff http://www.dnsstuff.com/

To retrieve your site's information on DNSstuff.com, enter your domain name in the site's WHOIS Lookup box, located in the home page's left column, three boxes down. The resulting WHOIS information page will tell you:

- The registrar ("Sponsoring Registrar")
- The contact person for the domain (under "Admin contact")
- The name server — which will inform you of the current web host

	**Tip** If the domain registrar is Network Solutions, then you must use Network Solutions' WHOIS search to look up this information.
	Network Solutions WHOIS Search http://www.networksolutions.com/whois/

Scenario 1: Website Is Down

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. Being able to pick the right platform is important if you have backups of your site, which may have been built on a specific platform, or if you are hoping that your original web host will return and you want to maintain the same platform in case you switch back. If your website included a database on the web host's servers, the availability of the correct database platform (for instance MySQL, or MS SQL Server) is also important.

2. Update Your Domain Registration.

Once you have paid for a web hosting service, you have to update the information at your domain registrar to "point" the address of your domain to the new web host (as opposed to the old one). This is usually as easy as logging in to your domain registrar's control panel and updating the information yourself. Depending on the registrar, however, 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 (otherwise anyone could "hijack" your website). The same goes if your domain was previously registered by a company that is no longer online 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 you looked up on DNSstuff.com will match the current

contact information. If the contact listed is an individual, you can usually make requests via the email address listed as the admin email contact in the WHOIS lookup. However, if that information is wrong, old, or "masked," you can sometimes prove who you are by faxing a copy of an ID, or by answering a secret question that was established when you registered the domain. However, if the admin contact listed is an organization's name, proving who you are usually requires a written letter on your organization's letterhead — which may not be an easy thing to find following a disaster.

While some registrars, given the circumstances, may be flexible around these issues, times of disaster are often ripe for fraud, so it is likely you will still be required to convincingly prove who you are before transferring domains. A registrar's website will usually provide contact information in case you have lost your password or your admin contact information is out-of-date.

3. Upload Your Website.

Once you have the web host and domain registrar pointing to the right address, you can begin uploading your web pages, whether that means simple contact pages (if you have no backups) or the original website (if you do have backups).

Scenario 2: Email Hosting Is Down

If your web hosting company was also hosting your email, you will want to use your new web host to also provide your email hosting as well. You may be required to pay for this extra service, or it may be included (up to a certain number of email addresses). Nevertheless, you will need to update what is called your mail exchange (MX) record, which is similar to updating 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). You have to either enter this information on your domain registration control panel, or ask your domain registrar to update that information for you (again, by proving who you are).

Scenario 3: No Access to Records

If you can access your website, but do not have any of your access records or passwords, you are going to need to contact the domain registrar (or web host) and, after verifying your identity, ask them to change your login and password information.

Thankfully, most of the basic footwork you'll need to do to find domain registration information is provided by the WHOIS lookup on DNSstuff.com, which lists it as the "Sponsoring Registrar."

You can also see who registered your domain for you in order to determine if it was

done by an individual at your organization (in which case that person may have the login and password information), or if it was done by your web hosting company. If the latter is the case, your domain registration may still be current, but you will not have direct access to the domain control panel, and will need to request the IP address and MX record updates, as opposed to doing them yourself.

The key to proving who you are — the admin contact listed in the WHOIS record — is usually listed after the "registrant" information. Sometimes the email address is masked, making 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), making it easier to send written requests.

If you have no idea 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 not always reveal who the web host, however.

If your organization was hosting its website in-house, the WHOIS results can be very confusing, so try to resolve any internal network or server issues before getting lost in recursive searches.

Filing Insurance Claims

Often insurers want detailed information on the systems you had before they'll pay out. But what if you didn't keep good equipment records or lost what you had?

If this is the case, others may have kept this information for you. If you know the vendor you purchased your technology from, it may be able to provide you with copies of your receipts, which would normally include hardware and software specifications. Larger vendors and vendors in unaffected areas are most likely to have access to this kind of information, but try other vendors as well.

If your technology was paid for by a funder, you may have provided them with receipts or other purchase details. Ask for copies of your grant reports, which may detail the information you need for insurance claims.

If all this fails, do not panic! Your insurer is likely to be flexible. Talk to your agent about the insurance provider needs from you in the absence of a full inventory. In the meantime, put together the information you can remember on a form like the one we've included in Chapter 9: Post-Disaster Operations Analysis (Page 67).

Chapter 7: Tips for Reviving Broken Computers

If you have access to your backups, and have practiced for a disaster recovery, your restore procedure should have been in place. However, if you cannot access your backup, or don't have one, it is still worth trying a couple of these tips before declaring a computer dead. Computers are more resilient than most people realize, and though a computer may not be in a usable condition, you may be able to recover critical data from it.

Some of the tips below have been gleaned from real-life experiences published on TechRepublic.com, a resources site dedicated to IT professionals. Some are last-resort actions not recommended by manufacturers. Though we offer them here to provide ideas, we cannot guarantee their effectiveness. We have also provided information from Microsoft.com on Windows XP recovery, for those who do not have access to the Internet.

Because TechSoup cannot guarantee the accuracy or effectiveness of these tips, do not attempt any of them if:

- You don't have a backup of mission-critical data.
- You think it may make your problems worse.
- You do not feel technically qualified to follow the advice.

General Data-Recovery Tips

The following information 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 (or at least remember which version you were running).
- Don't forget warranties and manufacturer support. Call the manufacturer to see if they can help fix your computer.

Real-Life Data Recovery Tips

These data-recovery tips were posted to Techrepublic.com by members.

Warning
Wait until your computer is completely dry before attempting any of these steps.

The following tips assume you can see some sort of electrical connection when you

plug in your computer. As soon as you have a functional drive up and running, ensure that you immediately make a backup onto another type of media. A good media is either a USB-connected external drive or flash drive. Flash drives would probably be a good idea anyway so you can share common files easily prior to restoring your network.

1. *Let's take a look at the hard drive itself. Is it plugged in properly? Loose cables are the most common problem in a case like this. If it is plugged in properly, try to boot the computer again after checking the connections. Sometimes a connector can come loose a bit on one side.*

2. *Next, does the hard drive spin when you turn the computer on? If it doesn't, check the power cable to the drive. If that is fine, tap the drive lightly on the side to see if it spins. (If it does, back it up and order a new drive immediately!) I encountered a drive that acted like this a year ago. If you kept tapping it, it kept spinning. So, for three hours, I sat there tapping this drive until I got all the company's accounting data off of it. Sometimes you have to make sacrifices for your customers.*

3. *If the drive is spinning and the cables are properly seated, check the "Detect IDE Hard drives" in the BIOS. To access the BIOS, press "F2" or "DEL" when the system boots (it depends on the vendor), but it may also say upon boot "Press X to access the BIOS menu". For some reason, on some of the older motherboards, it will pick up a drive that "AUTO" won't pick up.*

4. *If this drive isn't spinning up, putting it in the freezer (sealed in a plastic bag to protect it from moisture) for about an hour will usually get the drive spinning again so you can copy needed files before the drive warms up again.*

5. *Sometimes, a hard drive that has been running forever won't spin after being shut down for a while. The cause of this can be the heads sticking to the platter. As a LAST resort, try dropping the drive onto a firm surface from approximately eight inches.*

Microsoft XP Disaster Recovery Tools

Software and hardware issues can affect the way that your system functions. Severe problems might prevent you from starting Windows XP Professional normally. For example:

- Installing incompatible software, incorrectly changing system configuration settings, or installing faulty device drivers can cause system instability or a Stop error.

- Hardware that is defective, malfunctioning, incorrectly installed, or incorrectly configured can also cause instability or a Stop error.

- Deleted or corrupted system files caused by problems such as user error or virus activity can cause data loss or prevent you from starting the operating system.

Any of these issues can prevent you from starting Windows XP Professional normally, causing certain applications or data to become inaccessible. Windows XP Professional provides several tools that enable you to troubleshoot startup and stability problems and restore system and data files.

The table below lists some of these tools according to the preferred order of use, from those that present little or no risk to data, to those that might cause data loss. With the exception of Windows' Automated System Recovery (ASR) restore phase, Last Known Good Configuration, and Recovery Console, the features in the table are available in safe and normal startup modes. If the following tools and features do not resolve the problem, and you upgraded your system from an earlier version of Windows, you might have the option to uninstall Windows XP Professional.

With many of these tools, you may need to start Windows in safe mode. Safe mode helps you diagnose problems. It starts the computer with only essential files and services loaded, which cuts out a lot of the issues that can cause a complicated, modern computer to break. If a symptom does not reappear when you start in safe mode, you can eliminate the default settings and minimum device drivers as possible causes. If a newly added device or a changed driver is causing problems, you can use safe mode to remove the device or reverse the change.

To start in safe mode:

1. Restart the computer.
2. As it boots, press F8.
3. Use the arrow keys to highlight “Safe mode.”
4. You can also use the same steps to go back to the Last Known Good Configuration (see the list below).

Safe Mode
http://support.microsoft.com/kb/315222

Windows XP Recovery Tools and Features

Last Known Good Configuration: A startup option to use when the system cannot start in normal or safe mode following a driver or application installation that causes a problem. By using the Last Known Good Configuration, you can recover by reversing the most recent driver and Registry changes made since you last started Windows XP Professional.

Device Driver Roll Back: A Device Manager feature that allows you to replace an individual device driver with the previously installed version if the driver was updated after you installed Windows XP Professional. Device Driver Roll Back is available in normal or safe mode.

System Restore: A service that actively monitors your system and records changes to the Registry, to system files, and to certain application files. System Restore allows you to undo recent Registry and file changes by using information previously saved in restore points. Use to restore the system to a previous state. System Restore is available in normal or safe mode.

Add or Remove Programs (in Control Panel): A Control Panel feature you can use to uninstall programs. Use to temporarily uninstall software that you suspect is causing a problem. You can uninstall an application in normal or safe mode. (To reinstall software you will need the program's installation CD or files.)

Recovery Console: A command-line environment that you can use to perform advanced troubleshooting operations. In addition to Last Known Good Configuration and safe mode, advanced users can use Recovery Console to attempt manual recovery operations.

Backup: A tool for saving data, such as the system state, before you troubleshoot problems, attempt workarounds, or apply updates. Backup (Ntbackup.exe) enables you to restore system settings and data if troubleshooting attempts worsen the problem. Use in conjunction with a parallel installation to restore a system that cannot start in normal or safe modes. Backup is available in safe or normal mode.

Automated System Recovery (ASR): A Backup (Ntbackup.exe) option to use when boot and system files become corrupt, preventing your system from starting in normal or safe modes, or using the Recovery Console. This option is more desirable than formatting disks and reinstalling Windows because ASR restores system settings and critical files on the system and boot partitions.

ASR Backup's user interface is the ASR wizard in Backup, which steps you through the process of creating an ASR backup set and an ASR floppy. Windows XP Professional Setup provides the user interface to ASR restore.

Because the ASR process formats disks (which means you'll lose all of your data), consider this a last resort when using Last Known Good Configuration, Device Driver Roll Back, System Restore, or Recovery Console.

Chapter 8: Borrowed, Donated, and Free Technology

Delicious:tsdp+discount
http://delicious.com/tag/tsdp+discount

Depending on your situation, you may need to rely on borrowed, donated, free, or shared equipment and services. Where should you start? In this chapter, we'll list the most important things to think about as you rush to resume your organization's services using donated, borrowed, or free technology.

Working on your business impact analysis (see Technology Triage, Page 43) as soon as you feasibly can is still a priority, as you'll need it to move out of crisis mode. In the meantime, you may have found generous donors who can lend or give you equipment to help you get through the immediate future. If you are fortunate enough to have been offered help, accept it! While you're doing so, be aware of some of the common pitfalls of using technology tools that haven't been prepared specifically for you.

Donated and Discounted Technology

TechSoup Software and Hardware Programs

Since you're reading this guide, it's likely that you're already familiar with TechSoup Global's donation and discount programs around the world. Through relationships with dozens of respected hardware and software companies, we've developed an impressive catalog of hardware, software, and hosted services. We research each product and verify it as a safe and useful tool for some (though not necessarily all) NGOs before listing it on our site.

Some of TechSoup's products are donated by the vendor, while others are offered at a discount. For donated products, the admin fees cover only TechSoup program costs; for discounted products, the vendor receives a portion of the admin fee. In both cases, we've researched the options available on the market to make sure we're giving fellow nonprofits the best possible value.

For U.S. nonprofits and libraries, we also facilitate the Refurbished Computer Initiative (RCI). RCI lets qualifying nonprofits request refurbished computers at competitive prices.

If you're in the United States, visit TechSoup Stock to see our product listing. For organizations in other countries, visit our list of countries to find our partner in your country or region.

From time to time, TechSoup Global's international partners offer special donations and services for NGOs impacted by nationwide disasters. Check with your country's TechSoup partner for more information.

TechSoup Stock (United States)
http://www.techsoup.org/stock/

Refurbished Computer Initiative (United States)
http://www.techsoup.org/stock/rci/

List of Countries (TechSoup Global)
http://www.techsoupglobal.org/countries

Discounted Software Alternatives

Some technology companies offer product donations and discounts to nonprofits directly. Similarly, many software resellers list special prices only for nonprofits. For an up-to-date listing of both, see A Quick Guide to Discounted Software Programs.

If you need software from a certain company, check their website to see if the company makes any special accommodations for nonprofits. Even if you don't find information on a vendor's website, it never hurts to call and ask.

A Quick Guide to Discounted Software Programs
http://www.techsoup.org/learningcenter/software/page5055.cfm

Borrowed Technology

If you're using another organization or individual's computer, you probably can't wipe the machine and set up a fresh account. But you still need to safeguard your organization's data from loss and corruption, as well as accidental disclosure once you return to a more stable environment — all while respecting the constraints imposed by the equipment's owners.

Setting Expectations with the Lender

Make sure you and the lender understand what counts as acceptable use and who is responsible should something go wrong. If the equipment comes with preexisting conditions, you need to know about them before deciding whether it is suitable for your organization. A written agreement will help make sure you know where you stand if things don't work out. If the equipment is particularly valuable, you may want to seek a lawyer's advice drafting an agreement.

User Accounts

A separate account helps differentiate your information from that of the machine's owner. It keeps you from deleting the owner's data and allows you to customize your environment as needed without affecting hers. This measure will also make it much easier to remove your data from the owner's computer and port it to a new one before returning it.

Tip
All modern versions of Windows, Mac OS, and Linux allow for multiple user accounts. For Windows, look under "User Accounts" or "Users and Passwords" in the Control Panel. In Mac OS, select Accounts in the System Preferences pane.

Firewall and Virus Protection

As it is borrowed equipment, take measures to protect the equipment from viruses and other malicious activity. Ideally, the owner will have already implemented malware protection, but take extra precautions to make sure that these tools are up-to-date, especially if there's existing data on the computer.

Removing Spyware, Viruses, and Other Forms of Malware
http://www.techsoup.org/learningcenter/software/page4769.cfm

TechSoup.org Security Corner
http://www.techsoup.org/security/

TechSoup.org Virus Protection Toolkit
http://www.techsoup.org/toolkits/antivirus/index.cfm

Transitioning to New Equipment

Once you no longer need the borrowed equipment:

- Back up all of your data from the borrowed equipment.
- Move your backups to your new equipment.
- Check to ensure that everything is working well. Ideally, arrange for an overlap period of a month when you use your new equipment, but still have access to the old if you find that something isn't working well.
- Once you're sure everything has been successfully moved to your new equipment, delete all of your data and the accounts you were using from old machines. If possible, reformat the borrowed machines.

Tip
Reformatting a borrowed computer will destroy all of the owner's data as well as your own.

Free Technology

As you're rebuilding your technology infrastructure, you may need to keep your costs down by seeking out free alternatives to commercial software.

Open-Source Software

Open-source software is governed by a more flexible license than traditional, commercial software. Users can download and install open-source software free of charge and create and distribute plugins to customize it. In some cases, open-source software is maintained by a community of volunteers; in other cases, it's maintained by a for-profit company that relies on sources of income besides software sales.

In the past few years, several open-source tools have grown a fair amount of popularity in the NGO community. The Nonprofit Open Source Initiative's primer for nonprofits is an excellent place to start learning what open source can do for your organization.

Choosing and Using Free and Open Source Software: A Primer for Nonprofits
http://www.nosi.net/projects/primer

Six Steps to Adopting Open-Source Software at Your Organization
http://www.techsoup.org/learningcenter/software/page5683.cfm

Microsoft Office vs. OpenOffice.org
http://www.techsoup.org/learningcenter/software/page4765.cfm

The Myth of Open Source?
http://blog.techsoup.org/node/430

Web Applications

Web applications like Google Docs and Microsoft Office Live might serve you as a replacement for traditional office software, either temporarily or permanently.

For more information, see Alternatives to Regular Backups on Page 32 and Are Web-Based Collaboration Tools Secure? on Page 34.

Chapter 9: Post-Disaster Operations Analysis

This chapter is designed to help you identify, assess, and recover vital personnel, services, and equipment following a disaster. Use the checklists and charts below to ensure that the recovery process goes as smoothly as possible, and to manage your personnel and assets throughout the process. Certain charts are customizable in a separate Microsoft Excel file available in our Disaster Planning and Recovery Toolkit.

Disaster Planning and Recovery Toolkit
http://www.techsoup.org/toolkits/disasterplan/index.cfm

People and Deliverables

To recover from a disaster, it's important to respond quickly and effectively, identifying needs, prioritizing resources, and communicating clearly. The checklist below can help you organize people and communication during a crisis so that you are able to accurately analyze the impact on of the disaster on your organization and prioritize recovery efforts.

Staffing and Communication Guidelines

- If you have a plan, then follow it as you (hopefully) did in your practice drills. While some things won't go as planned, most things should.
- If you don't have 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 for making which decisions, ensure that there is also a process in place to cross-check these decisions.

Tip
Try to keep communication simple. In the absence of a formal risk or issues register, an old-fashioned message pad and to-do list will suffice.

- Beware of heroic "Rambo" types making drastic decisions, especially if these decisions could risk lives or limbs. In addition, some people feel they must be in the thick of the action to be helpful — try to harness this energy by delegating tasks appropriate to their skills and the situation's needs
- Do not assume that first responders — public services that deal with emergencies and other aspects of public safety (such as public utility crews, community emergency response teams, firefighters, and so on) —

will keep you informed, and never assume that the danger has passed. Contact them to ensure that you are receiving accurate and current updates on the status of the situation; likewise, these agencies and personnel may require information from you.

- Make sure you're relying on a dependable news source for information (in other words, don't believe everything you see on the news or read in the press, which may be sensationalized). If need be, appoint someone to handle public relations to ensure that the information you're receiving is consistent.

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

- Establish a help desk or two — one for customers and one for staff — to avoid overwhelming 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 third-party contingency suppliers (such as salvage companies or mobile computer room suppliers)? Even if you're not yet certain, it may be worth contacting them to notify them of potential need.

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

3. Discourage all but key staff from turning up 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 call tree

☐ Recovery document that identifies where important data are kept, such as:
- Key allies
- Main donors
- Funders
- Contractors

☐ Supplier contact list

☐ Supplies of your new work environment

- Desk
- Telephone
- Diary
- Paper
- Writing instruments

☐ Existing floor plan. This will help out when you need to make new arrangements if you plan to need more space.

Tasks and Deliverables Tracking Chart[2]: Use this chart in conjunction with the Deliverables Checklist to ensure that required tasks are completed following a disaster.

Task	Start Date	End Date	Deliverable

Operations

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

Technology Priorities Assessment: Use this chart to identify the key applications required to operate your organization over the next 24 hours, the next three days, and the next week.

Office	Department	Application	Workstation/ Server ID	Needed sooner than 24 hrs?	Next three days?	Next 7 days?

Technology Refresh: Key Recovery Staff: Assuming all staff are available, the table below allows you to identify the key personnel required to recover your systems and where these systems will be recovered.

[2] The charts in this chapter are intended as examples. Each chart marked with the pencil icon is available for download at TechSoup's Disaster Planning and Recovery Toolkit (http://www.techsoup.org/toolkits/disasterplan/index.cfm). Download the spreadsheet and customize each chart to meet your organization's needs.

Service Type	Assigned Personnel	Location

Project Planning and Rollout
Plan your recovery using your Business Impact Assessment before you attempts to acquire or replace services or equipment. Consider conducting a try run rather than just jumping into recovery. 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. Don't forget to detail 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 tracking all time spent on recovery with a special disaster-recovery expense code when your accounting systems are functioning again, for example.

Accommodation
List all accommodations you need during your recovery by both type and duration. Don't forget 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 you'll need during your recovery.

Technology Recovery Contacts

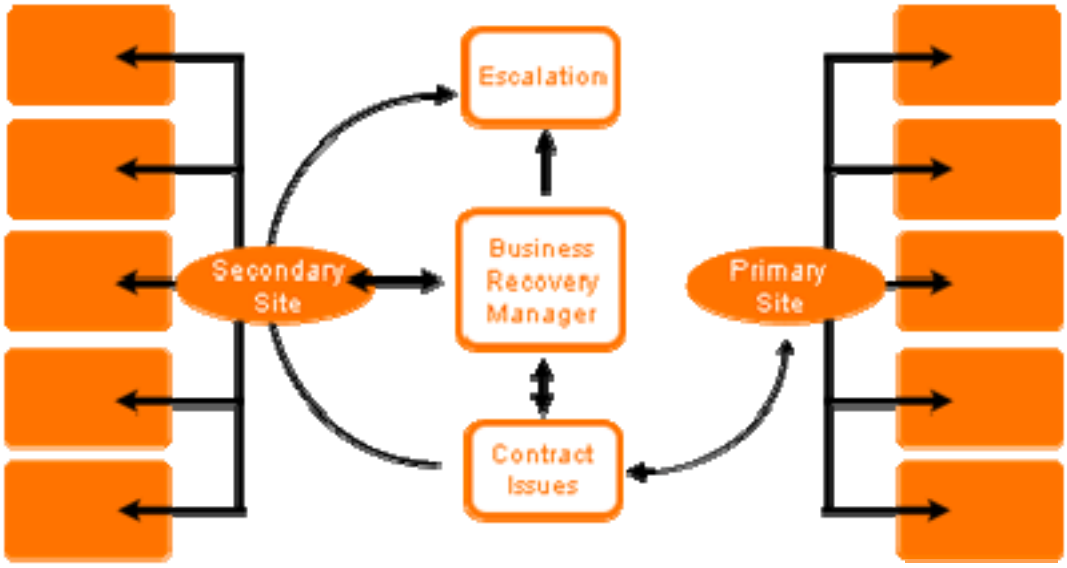
Name	Role (e.g., Network/ Database/ Systems	Address	Type of Vendor (e.g., Consultant, Firm, Corp)	Contact info (incl. cell phone, IM, Skype

Internal Escalation Contact List

Name	Role During Recovery	Location	Job Scope	Cell Phone

Communications Plan

A diagrammatic communications plan will help your organization visualize the channels of communication during an emergency. While every organization's structure, personnel, and culture facilitate a different set of processes, the following is an example of a communications plan for an organization with two sites and one designated Business Recovery Manager:

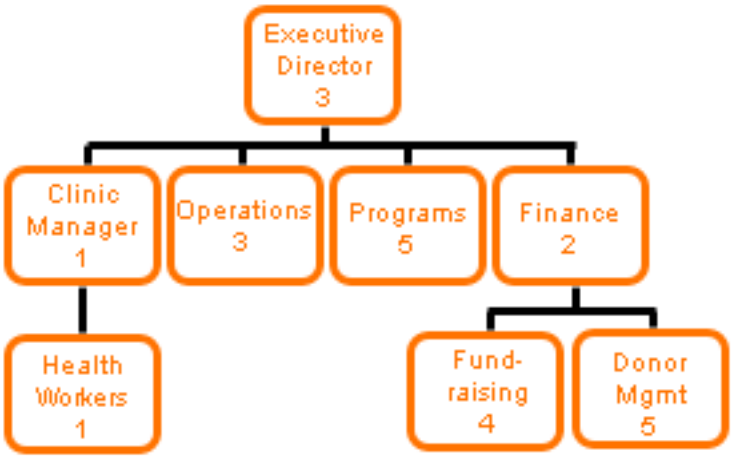


Business Impact Assessment Questionnaire

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

1. Mission critical
2. Significant damage
3. Serious damage
4. Major impact
5. Minor impact

The sample organization chart below represents the ratings of a community health clinic.



Business Unit Information

This chart can be used to record the functions of each business unit in your organization. It can be kept in a known repository at the recovery site for reference.

Business Unit
Location
Organizational Focus
Constituency (if internal, state "internal")
Departmental Function
Recovery Objectives
Number of Employees

Business Process: What are the business processes performed by each of your departments? Include the name and a brief description of the business process.

Department	Key Personnel	Process Name

Analysis of Key Processes: Use the following chart to identify key processes in your organization (use a separate copy of the chart for each process).

Name of Process	
Description	
Questionnaire completed by	
Date	

Legal and Regulatory Requirements

Are there any legal or regulatory requirements for loss or delay of the service provided?

Service	Yes	No

Would a delay or loss of service result in any penalties?

Service	Yes	No

If **yes**:

List regulations (if known)	
Describe the conflict or situation	
Describe consequences	

Consequences of Not Performing Functions

Under the following headings, please indicate your assessment of the business impact of not performing this function during the recovery process.

Potential Impact: Estimate the potential impact to your constituents if this function is paused.

Operations	Immediacy	Potential Impact	Assumptions and Justification

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

	**Tip** When filling out the Excel sheet, use formulas to facilitate calculations.
	About Formulas http://office.microsoft.com/en-us/excel/HP052255841033.aspx

Operations	Immediacy	Breakdown	Total Cost

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

Process	Immediacy	Rank (1-5)

Workflow Relationships

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

Is work received from any other business unit? If so, from whom, and what type of work?

Is work sent to any other business unit? If so, to whom, and what type of work?

Business Interfaces: List any internal or external business interfaces (including companies, banks, and customers).

Interface	Priority (1-5)	Purpose of interface

Staff Relocation Requirements: Use this chart to indicate how mane desks are required to restore continuity, and what each workstation will need.

Number of desks required	Phone?	PC?	Printing?	Other

Vital Records

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 Name	Number of Copies Required	Update Frequency	Where Report is stored	Sensitive?	Special Requirement (e.g., off-site)

 **Hardware and Software Resources:** Use this chart to track how many items are used, what is required during the recovery, and when it will be required.

Asset	Current Inventory	Day 1	Day 2	Day 3	Day 4	Day 5	Week 1 Onwards

List any special equipment used in your business unit, including type, make, and model.

Do you get any special information from the LAN, WAN, or Internet?

List any special requirements for the recovery of the business unit.

Voice Recovery: Use this chart to identify your phone requirements following a disaster.

Number at Primary Site	Number at Required Recovery Site	Single Line?	Two Line?	Speakerphone?	Recording?	Private Line?

Internal Contingency Plans

Are there any manual procedures that can be activated if data-processing facilities are lost for an extended period of time?
Are these procedures documented? If so, when were they lasted updated?
Do contingency plans exist that provide step-by-step instructions for the recovery and performance of this business function?

Supplier Contact Details: Use this chart to keep track of your suppliers and any information that could be relevant to restoring continuity.

Supplier Name	Contract Type	Reference Number	Contact Details