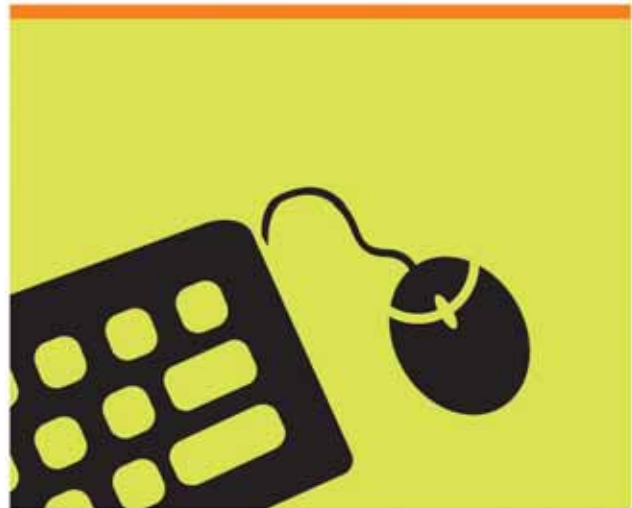


healthy&secure
computing



Restoring IT Infrastructure

A Manual for Disaster Recovery



techsoup.org

Copyright © 2007
CompuMentor and Bryan J. Sharkey

This document is licensed under the Creative Commons **Attribution-ShareAlike 2.5 license**.

You are free to:

- Copy, distribute, display, and perform the work.
- Make derivative works.
- Make commercial use of the work.

Under the following conditions:



Attribution. You must attribute the work to *CompuMentor, home of TechSoup.org*.



Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under a license identical to this one.

- For any reuse or distribution, you must make clear to others the license terms of this work.
- Any of these conditions can be waived if you get permission from the copyright holder.

This is a summary of the terms of this license. For full information please see the [Creative Commons Web site](#).

Table of Contents

IT DISASTER RECOVERY - AFTER THE FACT	1
PICKING UP THE PIECES.....	2
TRIAGE	3
SAFETY FIRST.....	4
HARDWARE RECOVERY	5
NETWORK RECOVERY	6
<i>Local Area Networks.....</i>	<i>6</i>
<i>Sharing a Network</i>	<i>9</i>
DATA RECOVERY	10
<i>Dealing with Lost Passwords.....</i>	<i>11</i>
MOVING YOUR WEB SITE.....	12
<i>Web Site is Down</i>	<i>13</i>
<i>Email Hosting is Down</i>	<i>14</i>
<i>No Access to Records.....</i>	<i>14</i>
FILING INSURANCE CLAIMS	15
BORROWED OR DONATED TECHNOLOGY	16
BORROWED TECHNOLOGY.....	17
DONATED TECHNOLOGY	18
<i>Using Free Services</i>	<i>18</i>

IT Disaster Recovery — After the Fact

Introduction

This IT resource, originally created in the aftermath of Hurricane Katrina, was developed by CompuMentor's Healthy & Secure Computing initiative to help get technology systems working again in small- and medium-sized nonprofits when business continuity plans are either insufficient or nonexistent following a disaster.

This manual is part of TechSoup's disaster planning and recovery toolkit, which gathers information relevant in the different stages of a disaster, and outlines the measures organizations should take to prepare for a disaster of any magnitude. The most recent version of this document can be found on the toolkit at <http://www.techsoup.org/toolkits/disasterplan>.

CompuMentor is a United States-based nonprofit offering technology support and resources to nonprofit organizations around the world. CompuMentor's programs include:

[TechSoup](#), an online portal for nonprofit technology articles, information, and advice.

[TechSoup Stock](#), a product philanthropy program providing donated and discounted software and hardware for nonprofits and public libraries in the United States and Canada.

[Healthy & Secure Computing](#), an initiative to enable nonprofits to set up and manage a strong, stable, basic technology infrastructure.

Please send your feedback on or questions about this manual to hsc@techsoup.org.

Picking up the Pieces

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.

Triage

Knowing where to start and what to spend your resources on when you're trying to recover from a crisis can be overwhelming. You can make the best of the situation by identifying what steps are absolutely necessary to keep your organization viable.

The first aspect of your organization to look at isn't your technology, however. Instead, start by conducting a business impact analysis (BIA), which will help you decide where you should concentrate your resources and focus immediately following a disaster.

To conduct a post-disaster business impact analysis, follow the process we have included in **Appendix A**. (Appendix A's customizable worksheets may be downloaded separately.)

Once your organization has identified what needs to be done and in what order, you can focus on obtaining the technology you need to begin the recovery process.

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

1. **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 make the most impact is one of the keys to a successful triage.

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.)

2. **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.
3. **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.

Safety First

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. 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.
3. 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.
4. 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.
5. Physical safety is important. 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.
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

If a machine is visibly damaged and its data deemed mission critical, **STOP RIGHT NOW!** and skip to the Data Recovery section below. 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 are any debris, remove them 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.

Network 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 chart lays out a list of scenarios for obtaining Internet connectivity for temporary offices providing services in an area affected by a disaster.

Comparison Chart: Options for Restoring Internet Connectivity

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

Solution	Pros	Cons	Equipment/Cost	Notes
High-Speed On-Site Connection	Fast, may be free.	Shelters or service center sites may not have high-speed Internet access.	About \$150 for SOHO router and cabling.	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.	Can be fast; possibly no per-minute charges.	Somewhat complicated to set up.	Usage charges will vary depending on the type of access (for example, Muni Wi-Fi or T-Mobile HotSpot). Wi-Fi/Ethernet bridge, antenna, cabling, router/access point ~\$500	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.	Works anywhere there is an available phone line.	Connection is slow; there is a monthly cost to maintain your account.	None for individual computers; About \$400 for a dialup LAN.	Several computers could be serviced via a wired 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.
Mobile Phone or Data Card	Works anywhere there is cellular service; faster than dial-up.	Depending on the data plan, per minute and data-transfer charges can add up.	<i>Mobile Phone:</i> Most mobile phones now can transmit data natively. Some (such as a Blackberry or a Nokia) can be used as a modem <i>Data Card:</i> A one-time fee of \$150 to \$250 per laptop.	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 a signal.	Works almost anywhere; somewhat faster than dial-up.	Expensive; not particularly easy to set up.	About \$400 for satellite and possibly LAN equipment.	Can be shared with clients over a wired or wireless LAN.

Sharing a Network

Sharing a network or Internet connection with multiple organizations may be the only available solution. 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 Triage section of this guide, 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:

1. Do not attempt to clean or dry waterlogged drives or other media by yourself.
2. Do not use common software utility programs on broken or water-damaged devices.
3. 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.
4. 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.
5. 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 or her inbox somewhere. 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:

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.
 - Choose Reset Password from the Installer menu (or Utilities menu in Mac OS X 10.4 Tiger). *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 Web site'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

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 Web site of the manufacturer of the device.

Moving Your Web Site

If your normal Web host was in an area that was badly affected (or if you hosted yourself), you may need to move your Web site 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 Web site, all or any of which may have been affected:

Domain Registrar

Your Web site'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 Web site. 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 Web site, if 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 do if your Web site is down; if you need to move your email to another host; or if your Web site 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 Web site [DNSstuff.com](http://www.dnsstuff.com) (<http://www.dnsstuff.com>) can help you find this information.

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.



QUICK TIP: If the domain registrar is Network Solutions, you have to go to Network Solutions' web site <http://www.networksolutions.com/whois> to look up this information.

Scenario 1: Web Site 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 Web site 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 Web site). 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 Web site will usually provide contact information in case you have lost your password or your admin contact information is out-of-date.

3. Upload Your Web Site.

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 Web site (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 Web site'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 Web site, 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 Web site 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 the Post-Disaster Impact Analysis in **Appendix A**.

Borrowed or Donated Technology: What You Need To Know

Depending on your situation, you may be relying on borrowed, donated, or free equipment and services. Where should you start in this case? Below, we'll list the most important things to think about as you rush to get services restored and functional using donated, borrowed, or free equipment.

Working on your business impact analysis (see the Triage, chapter 1) 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 have lent or given you equipment to help you get through the immediate future. If you are fortunate enough to have been offered help, accept it! And while you're doing so, be aware of the following points to avoid some of the common pitfalls of using technology tools that have not been prepared specifically for you.

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.

1. Set 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 if it is suitable for your organization. A written agreement will help make sure you know where you stand if things don't work out; likewise, if the equipment is particularly valuable, you might want to have a formal contract.

2. Set up a separate user account.

This helps separate your information from the machine's owner. It makes it easy for you to see what's yours, stops you from accidentally deleting the owner's data, and lets you adapt your environment without affecting theirs.



QUICK TIP: All recent versions of Windows, Macintosh, and Linux allow for the creation of additional user accounts. For Windows, look under "User Accounts" or "Users and Passwords." in the Control Panel. For Mac OS, look under the "Accounts System Preferences" pane.

3. Get a firewall and virus protection in place.

As it is borrowed equipment, take measures to protect the computer from viruses and other malicious activity. Ideally, it will already be updated, but take extra precautions, especially if there is existing data on the computer.

4. Transfer to new equipment properly and promptly.

Once you no longer need the borrowed equipment:

- Back up all of your data from the borrowed equipment.
- Move your backups over 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 out 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 the old machines. If possible, reformat the borrowed machines (note, however, that this will destroy all of the data in the owner's accounts as well).

Donated Technology

If you're using donated computers and equipment, this equipment is not likely to be in the same condition as the equipment you are used to working with, so the functions and features you may rely on may not be available to you. Go slowly at first, making sure that the software and hardware you are using are adequate for the task at hand. Trying to shoehorn a project or application into an ill-fitting computer system can result in significant wasted effort and time. If you are unfamiliar with the systems you're using, keep things as simple as possible until you learn how to effectively use the tools you have at your disposal.

As soon as you're able to, reformat the hard drive and reinstall the operating system and your software.

Using Free Services

If you've lost everything, there may be free services and products in your community available to you. However, entrusting your information to an unknown system could also be a costly mistake that will hurt your organization in a few months time. Below are some guidelines for using free services.

- Keep it simple. Don't try to implement new ways of doing business that you're not familiar with, unless this is absolutely necessary. Consider keeping important information in simple spreadsheets, or even in paper folders, and re-entering it into your data systems once they are up and running
- Remember: It takes less time to learn a new system than to recover your old one.
- You can download any data you've entered (for free!) in an acceptable format when you're ready to move back to your old system (or on to a new one)
- The discounted or free services you're using are going to be available, at an acceptable cost, long enough for you to transition to something permanent. (After all, you don't want to be scrambling again in three months). If the offer doesn't state a time limit, investigate further.

Acknowledgements

We don't do this alone! CompuMentor would like to thank those who helped in the creation of this document. In particular, three technology professionals volunteered long hours, vital knowledge, and great resources:

Karen Forchione, Senior IT Manager for a major corporation in San Francisco, California.

Bryan J. Sharkey, BC and Disaster-Recovery Consultant, London, United Kingdom.

Allan Thompson, [Santa Clara County FireSafe Council](#)

Other members of the nonprofit technology community also helped with suggestions and ideas, including people from the Riders listserv and [NPower](#).

Appendices

Appendix A — Post-Disaster Operations Analysis

This appendix 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 the separate file *hsc-disaster-recovery-worksheet.xls*

I. 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.

1. Staffing and Communication Guidelines

1. 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.
2. If you don't have a plan, then you would need to determine how you will proceed; decide who will do what, and when.
3. 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.



QUICK 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

4. 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
5. 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.
6. Make sure that you are 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.
7. 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.

8. 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.

2. 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

This chart, in conjunction with the Deliverables Checklist, can be used to ensure that required tasks are completed following a disaster.

TOOLS



Sections with this icon can also be found as separate worksheets in the *hsc-disaster-recovery-appendix-worksheets.xls* file to facilitate customization.

Task	Start Date	End Date	Deliverable

II. Operations

Use the charts and guidelines below to identify the technology and personnel required to keep your operations going following 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 over the next week.

Office	Division (Such as Development, Finance)	Application	Workstation/ Server ID	Needed Within 24 Hours	Needed Within 1–3 Days	Needed Within 1 Week
San Jose Clinic	Finance	PeaceTree	Spica	N	N	Y

📍 Technology Refresh: Key Recovery Staff

Assuming all staff is available, the table below allows you to identify the key personnel required to recover your systems and where these systems will be recovered.

Service Type	Assigned Personnel	Location

Project Planning and Rollout

Plan your recovery using your Business Impact Assessment before you attempt to acquire or replace services or equipment. Consider conducting a dry 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

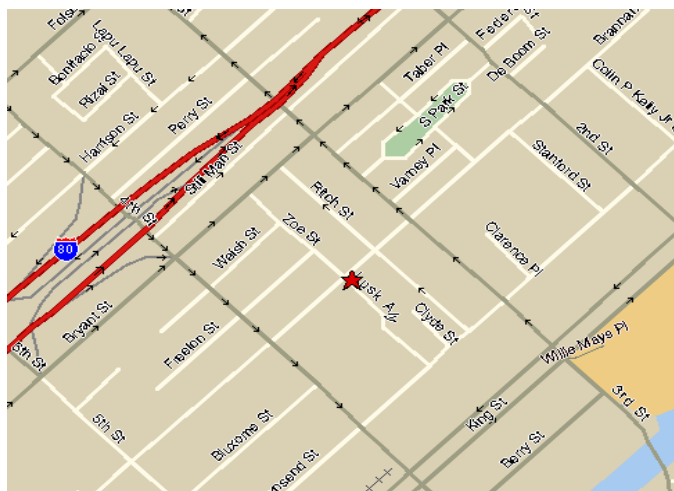
Accommodation

List all accommodations you need during your recovery by both type and duration. Don't forget to include additional items such as food and other supplies.

Maps and Directions

List maps and directions that you may need following a disaster. You can print out maps and directions to the closest hospital, fire station, or community center. These can be downloaded from Internet sites for the purposes of this document, but it is also handy to keep paper maps handy as well.

We have provided an example below.



**435 Brannan Street
Suite 100
San Francisco, CA 94107
Tel: (415) 633 9000**

From the North

Take US-101 South over the Golden Gate Bridge to San Francisco
US-101 South becomes Lombard Street
Turn Right onto Van Ness Avenue
Turn Left onto O'Farrell Street
Turn Right onto Stockton Street (Stockton becomes 4th Street)
Turn Left onto Brannan Street

III. Communications

Contact Lists

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

📍 Technology Recovery Contacts

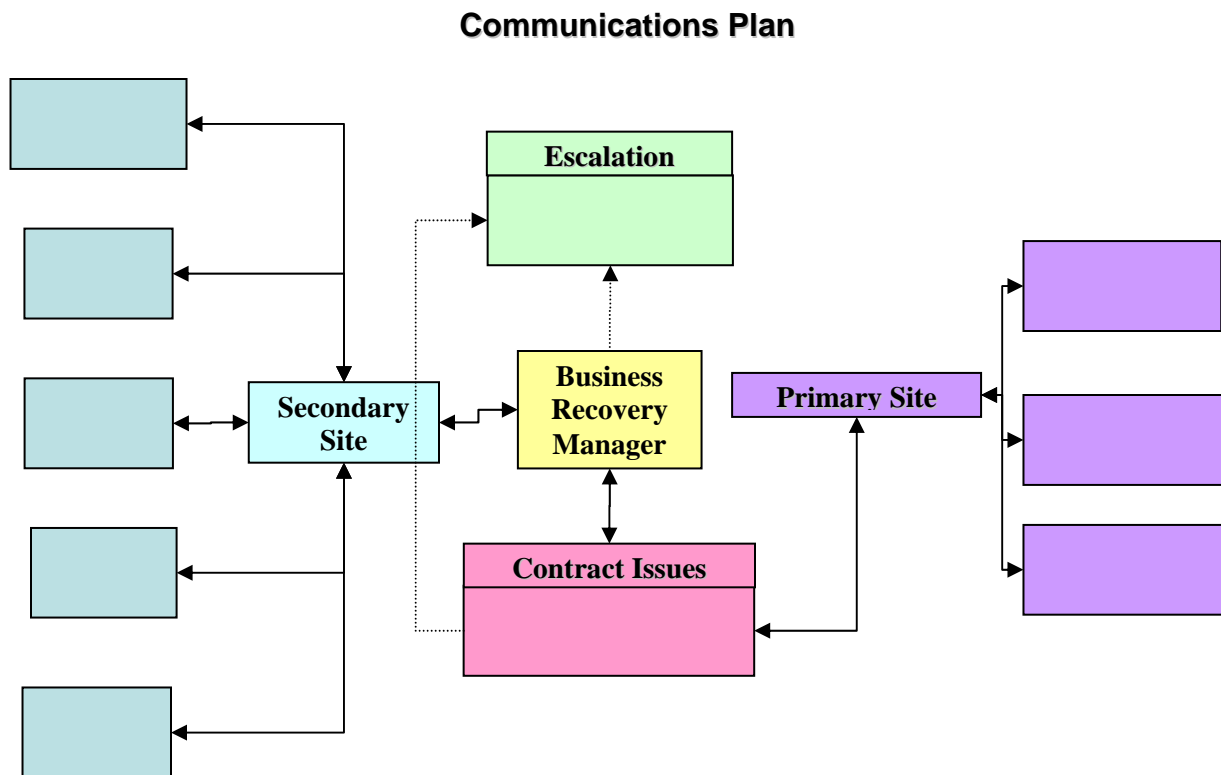
Name	Role (E.g. Network, Database, Systems)	Address	Type of Vendor (Consultant, Firm, Corporation)	Contact Information (Phone Number, IM, Skype, Address)
Bryan Sharkey				

📍 Internal Escalation Contact List

Name	Role During recovery	Location	Job Scope	Phone Number

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:

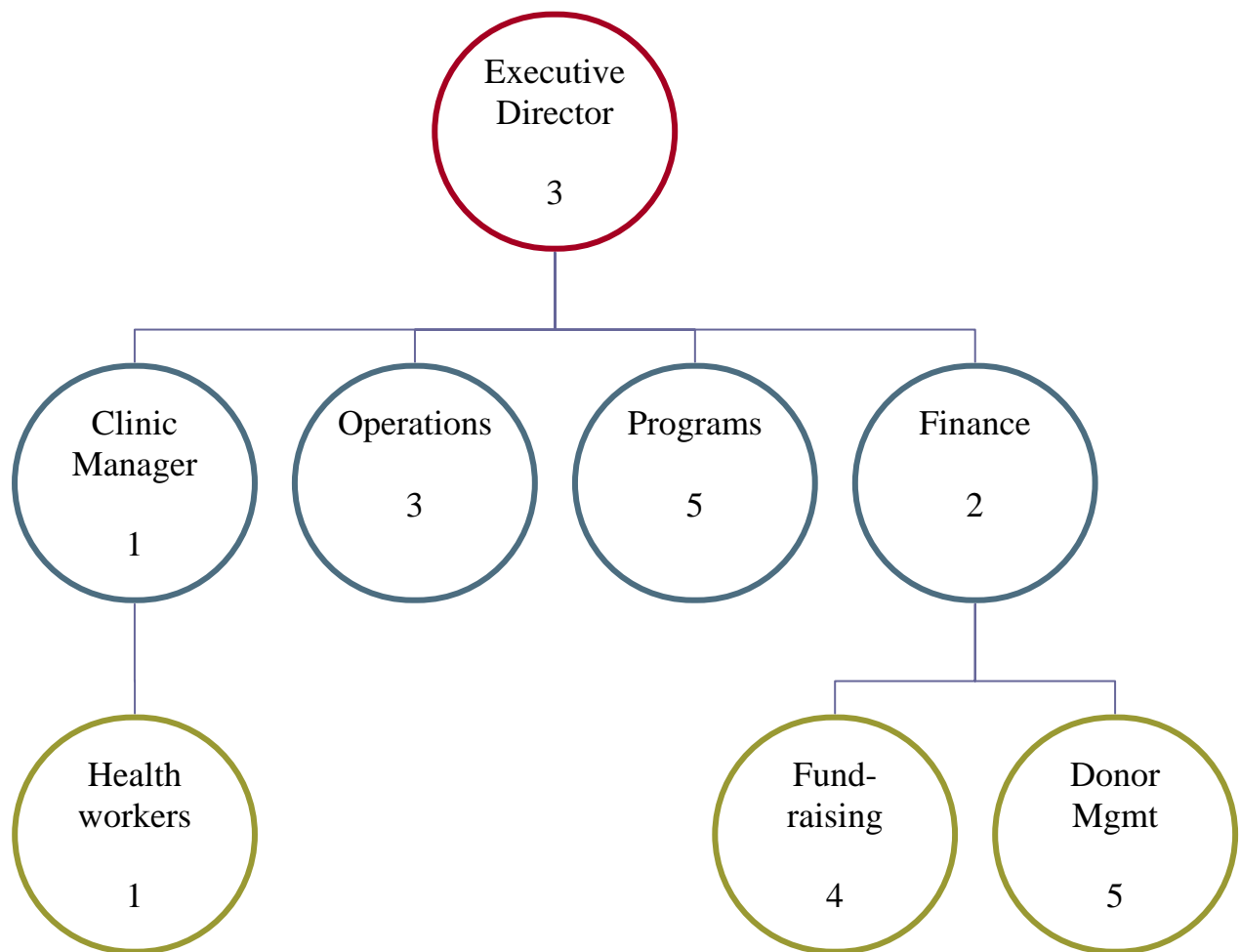


IV. Business Impact Assessment Questionnaire

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.

OVERVIEW OF THE BUSINESS UNIT

Location:

Organizational Focus:

Main 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
<i>Communications</i>	<i>Comm. Coordinator</i>	<i>Issuing press releases</i>

📍 Analysis of Key Processes

Use the following chart to identify key processes in your organization (*Use additional sheets for more than one process*)

Name of Process:	<i>Issue press releases</i>
Description:	<i>Writes up releases about events and call for actions, sends to media outlets</i>
Questionnaire Completed By:	<i>Janice Stevens</i>
Date:	<i>11/06/05</i>

📍 Legal and Regulatory

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

Service	Yes	No

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

Service	Yes	No

If YES:

List regulations (if known).	
Describe the conflict or situation.	
Describe consequences (such as penalties or fines).	

Consequences of Not Performing Function

Under the following headings, please indicate your assessment of the business impact of *not* performing this function following a major incident or disaster.

Potential impact

Estimate the potential impact to your constituents if this function were not performed following a disaster:

Operations	Immediacy (e.g. in the next 3 days, week)	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:

⚠️ **QUICK TIP:** When filling out the Excel sheet, use formulas to facilitate calculations.

Operations	Immediacy	Breakdown	Total Cost
Client intake	<i>Within the week</i>	<i>Generator rental @ 200/d Fuel @ \$50/d</i>	\$2500

📌 Health and Safety

Use the charts 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)
	One week	
	Two weeks	
	One or more months	

V. 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 many desks are required to restore continuity, and what the station will need.

Number of desks required	Phone?	PC?	Printing?	Other needs

VI. Vital Records

Data and File Recovery

It is up to each business unit manager to identify where critical files are stored. 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 the reports that you have and need. Note if a report is of a sensitive 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 the chart below to track how many items are used, what is required during the recovery, and when it will be required.

Equipment/Asset	Current Inventory	Day One	Day Two	Day Three	Day Four	Day Five	Week One 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 yes, when were they last 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

Appendix B: 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

Data-recovery tips 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 USB key fob. USB key fobs 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:

- Restart the computer.
- As it boots, press F8.
- Use the arrow keys to highlight "Safe mode." For details on safe mode options visit: <http://support.microsoft.com/kb/315222>
- You can also use the same steps to go back to the Last Known Good Configuration. A description of which is in Table B. 1

Table B.1 Comparison of Windows XP Professional Recovery Tools and Features

Recovery Feature	Function
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.

	<p>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. For more information about parallel installations, see "Troubleshooting Startup" in this book.</p>
<p>Automated System Recovery (ASR)</p>	<p>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.</p> <p>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.</p> <p>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 does not solve the problem. ASR is available in safe or normal mode.</p>