Healthy & Secure Computing

hsc
HEALTHY & SECURE
COMPUTING

Restoring IT Infrastructure

A Manual for Disaster Recovery

September 15th 2005

CompuMentor
home of techsoup.org

Copyright © 2005
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
- to make derivative works
- to 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 website: http://www.creativecommons.org/by-sa/2.5/legalcode

Your fair use and other rights are in no way affected by the above.

Table of Contents

IT Disaster Recovery – After The Fact

INTRODUCTION

This IT resource was developed by CompuMentor's Healthy & Secure Computing campaign and was created in the aftermath of the Hurricane Katrina tragedy. It provides advice on getting technology systems working again in small- and medium-sized nonprofits where business continuity plans were not sufficient or did not exist.

CompuMentor is a US-based nonprofit dedicated to providing technology support to nonprofit organizations. Here is a list of CompuMentor programs that are providing technology resources to nonprofits recovering from disasters:

+ **TechSoup.org**, an online portal for nonprofit technology articles, information and advice. (www.TechSoup.org)
+
+ **TechSoup Stock**, a product philanthropy program providing donated and discounted software and hardware for nonprofits and public libraries in the USA and Canada. (www.TechSoup.org/Stock)
+
+ **Health and Secure Computing campaign**, an initiative to enable nonprofits to set up and manage a strong, stable, basic technology infrastructure. (www.CompuMentor.org/HSC)

Our technology-related resources for nonprofits and public libraries affected by Hurricane Katrina can be accessed at:

http:/www.TechSoup.org/Katrina

In the coming weeks, we will produce an updated version of this manual which will be available online at http:/www.TechSoup.org/Katrina

Please send any comments on this document to: hsc@compumentor.org

PICKING UP THE PIECES

Recovering from a disaster is difficult even in the best of circumstances. Technology is unlikely to be at the top of your agenda, yet taking a few minutes to address some key issues will help your organization to recover and quickly move from crisis management back to 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 being clear about what you absolutely must have to keep your organization viable. So the first thing to look at isn't your technology – start instead with a Business Impact Analysis (BIA).

Follow the BIA process we've included in **Appendix A**. Fill in as much of the worksheets as you can that is applicable to your situation, and use it to help prioritize where to put your resources and what to focus on first.

Once your organization has identified what it needs to do, you can focus on obtaining the technology you need to do it.

Every organization is going to have different priorities about what technologies are "must haves", so a one-size-fits-all prescription is not appropriate here. However, here are some hints about how to develop 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 determine which equipment you need to bring back to life. Restoring and repairing systems can take significant time, and focusing your efforts where they will make the most impact is one of the keys to a successful triage.

   For mission critical data where the machine is physically damaged and you do not have a backup, we strongly recommend having the data professionally recovered. (See the Data Recovery chapter for more information.)

2. **Back up systems.** If you're lucky, you may have backup media in a safe place that is accessible to the organization. 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 good network backup system, you may not need to worry about the data on individual computers.

3. **Servers.** Often the core of many networks, recovering the server may be a high priority, especially if you have a healthy backup.

SAFETY FIRST

Safety First means being sure you have a safe environment to start the recovery. Observe the following precautions for your own safety.

1. If the floor or any electrical wiring or computer equipment may be wet, be SURE the power is off before you enter the room or touch any metal or wet surfaces or equipment. If you're sure 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 a safe, dry environment, it's important to be sure you have good, reliable electric power before connecting or turning on any computer equipment. Plugging in and observing an electric light to be sure it isn't flickering or a lot dimmer or brighter than normal is a good start. You can also try plugging in things you can afford to lose – a radio or an old computer, etc.

3. Turn off computers when they will not be used for an extended period to avoid power surges and brownouts. Unplug the computers, if possible. If a storm with lightening 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 comes back on. Computers you don't want to lose should have a short-term power backup system or uninterruptible power supply (UPS), which also provides 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 upon or taped to the floor to provide protection in high-traffic areas.

5. Physical safety is also important. Be sure tables are sturdy enough to handle the equipment placed upon them and that stacked equipment won't fall, especially when it is connected to cables, etc. 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 on.

6. Ventilation is also very important. Be sure 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 the computer equipment when it is too hot to work comfortably.

HARDWARE RECOVERY

Read the Safety First precautions above before continuing with this section.

1. IF a machine is visibly damaged and the data it contains is mission critical (see Triage chapter) – STOP RIGHT NOW and go to the data recovery chapter. DO NOT SWITCH ON MACHINES OR TRY TO DRY OUT DISKS YOU INTEND TO HAVE PROFESSIONALLY RECOVERED.

2. For hardware you intend to get working yourself, clean and dry your hardware. Don't attempt to plug in or operate a computer until it's completely dry and free of mud and dirt. Your computer may be just fine, but turning it on prematurely can destroy an otherwise healthy, though wet, computer. Take the time to open up the chassis of your computers, to make sure they are clean and dry, inside and out. If there is any debris, remove it carefully so the computer won't overheat from reduced air flow. Wear an ESD wrist strap or work on an anti-static 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 the power is off, the computer is unplugged, and laptop batteries are removed.** .

3. For other devices, such as routers, switches, and printers, make sure they 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 on 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 AND INTERNET CONNECTIONS

Local area networks

A local area network can be badly damaged by flooding. Network cabling can become waterlogged and non-functional. Patch panels and jacks can be water damaged as well. The switches, hubs, routers, and other electronic devices on your network may well be knocked out by the water. Fully restoring a complicated network can take time and effort, but it's possible to build out an ad hoc local area network quickly.

To build a simple network, start with an Ethernet hub or switch. Ethernet and TCP/IP networking technologies are the most common networking technologies in use, and are relatively robust and easy to setup in an ad hoc fashion. The hub or switch forms the backbone of your network and 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 for connecting two switches or hubs together.

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, pull equipment to the floor, and otherwise cause havoc. If you need to run 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 becomes very difficult to remove.)

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

Another option for an ad hoc network is the use of 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 WiFi security technologies. WEP, which is associated with 802.11b networks, and WPA, which is associated with 802.11g networks. WEP is no longer considered very secure, but is adequate for an ad hoc network. WPA is much more secure, and is appropriate for both ad hoc and permanent networks.

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 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 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 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 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. X can be any number between 1 and 254. Every computer or device should share the first three sets of numbers, and then 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, and which one is appropriate for your situation depends on what services are available to you and what equipment you have access to. The following is a list of scenarios for obtaining Internet connectivity for temporary offices while providing services in an area affected by a disaster.

+ **Solution A**

High-speed connection on site. If the host site for the organization 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 the service center is not in a room with Internet access.

Pro: Fast, potentially no monetary cost.
Con: Few shelters/service center sites may have high-speed Internet access.
Equipment required: SOHO router, cabling ~$150.

+ Solution B

Wi-Fi bridge. Depending on the location, there may be a Wi-Fi access point near the service site. With the right equipment, the signal can be brought onto a wire and redistributed to one or more computers. In some circumstances there would be no cost for the connection. In other cases, there would be a charge for connecting (to a T-Mobile hot spot at Starbucks, for example). This might require an antenna mast or temporary mounting of an antenna on the roof of the building.

Pro: Potentially fast, possibly no per-minute charges.
Con: Somewhat complicated to set up.
Equipment required: Wi-Fi/Ethernet bridge, antenna, cabling, router/access point ~$600.

+ Solution C

Dial-up. An individual computer could dial in to an ISP over a telephone line. Several computers could be serviced via a wired or wireless LAN by means of a router with a modem built in, or a computer with a modem and Internet Connection Sharing turned on.

Pro: works anywhere there is an available phone line.
Con: Connection slow, monthly cost to maintain account.
Equipment: none for individual computers, for dialup LAN ~$400.

+ Solution D

Mobile Phone/Data card. Individual computers can access the Internet using either PC cards or mobile phones attached by a cable. Such an Internet service connection could be shared on a network by a computer with Internet Connection Sharing.

Pro: Works anywhere there is cellular service, faster than dial-up.
Con: Per-minute charges could be pricey.
Equipment: $200 - $300 per laptop.

+ Solution E

Satellite Internet service. Dish captures a broadcast a signal; can be shared with clients over wired or wireless LAN.

Pro: Works almost anywhere. Somewhat faster than dial-up.
Con: Expensive, not particularly easy to set up.
Equipment: Also expensive. Satellite equipment, possibly LAN equipment runs ~$400.

Sharing a network

Sharing a network or Internet connection with multiple organizations may be the only available solution. This 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, comes into 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 before failing.

Organizations with concerns around privacy and confidentiality may want to use a second router to segregate off their sections of the network. It's possible to use multiple routers to create a number of different sub-networks that all tie into the core network.

For organizations that have less stringent security needs, sharing a single network should not present many difficulties. The key to smoothly sharing a network 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 – 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 lost data and your backup plan does not provide protection for this sort of catastrophe, there is still hope.

+ **Prioritize**

In Triage section we talked about working out what is critical to your organization. You also need to decide how much you're prepared to spend to recover

+ **Try your backups**

Tapes and CDs can be surprisingly resilient, so try them out, even if they look bad. Make sure the media and equipment is dry and, if possible, try reading from the tape or CD drive that you originally recorded from. If that doesn't work, try several different CD or tape drives. Sometimes you just need a higher quality drive to recover information you thought was gone forever.

+ **Use a data recovery company**

If your information is mission critical (such as your donor list) you may want to pay for data recovery. There are a lot of companies that do this. See **Appendix C** for a list. Costs can range from just a few hundred dollars to tens of thousands. Many companies are offering free assessments to those affected by Hurricane Katrina. One data recovery vendor offers this advice:

1. Never assume that data is unrecoverable, no matter what it has been through.
2. Do not attempt to power up visibly 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. Do not attempt to clean or dry waterlogged drives or other media.
5. 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.
6. Do not use common software utility programs on broken or water-damaged devices.
7. For mission critical situations, contact a data recovery company before any attempts are made to reconfigure, reinstall, or reformat.
8. When shipping your hard drives, tapes, or other removable media, package them in a box that has enough room for both the media and some type of packing material that allows for NO movement. The box should also have sufficient barrier room around the inside edges to absorb impact during shipping.
9. If you have multiple drives, tapes, or other removable media that need recovery, ship them in separate boxes or make sure they are separated with enough packing material so there will be no contact.

+ **Look for other sources of your data**

Think about other places you may have inadvertently stored the data. Perhaps you e-mailed your database to a consultant and it's sitting in their e-mail in-box somewhere. Perhaps printouts of the data exists that you can type back in (data entry is often less expensive than calling on technology experts). **If you find a copy of your data – back it up and make a copy before you do anything else**. Use only the copy you have made, and save the original in case things go wrong with the copy.

MOVING YOUR WEB SITE

If your normal Web host was in an area that was badly affected (or maybe 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 head 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 registration: The name of your site (e.g. www.mywebsite.org) - which is separate form the actual Web site content that is hosted by a Web host. This domain name can be registered separately, but is often done for you by a Web hosting company, which is why most people do not think of them separately.

Web host: The company providing the disk space for your Web site. This may have even been your own organization, but even in those cases, you may want to move your Web hosting to another service (since your hands may be full right now).

Web site content: You may have backups of your Web site. If not, you may just want to get a simple page up with contact information and a status update for your supporters.

E-mail hosting: Your e-mail may also be provided by an outside company—either the same as your Web host, your Internet Service Provider (ISP), a different company, or you may have hosted in-house.

We've provided guidance below on what to if your Web site is down; you need to move your email to another host; or your Web site is OK, but all of your access records and passwords are gone.

For all 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 this site can help you find this information:

http://www.dnsstuff.com

Enter your domain name in the WHOIS lookup box (left column, first blue box).

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.**

See below for more on how to decipher this information.

Note: If the domain registrar is Network Solutions, you have to go to Network Solution's Web site to do this information lookup: http://www.networksolutions.com/whois

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.

+ **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. Dotser.com has a good small-business Web hosting service for $15 / month and it supports both Linux and Windows platforms. Being able to pick the right platform is important if:

a) you have backups of your site, which may have been built on a specific platform;

b) 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*.

+ **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). Usually this is as easy as

logging in to your domain registrar's control panel and updating the information yourself. Depending on the registrar, you may need to contact your Web host directly and ask them to do it—and you'll have to prove who you are (otherwise anyone could "hijack" a 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—again you will have to prove who you are.

In the best scenario, the person (or entity) listed as the admin contact in the WHOIS information you looked up on DNSstuff.com would match the current contact information. If the contact listed is an individual, you can usually make requests via the e-mail address listed as the admin e-mail contact in the WHOIS lookup. However, if that information is wrong, old, or "masked" in the WHOIS lookup, you can sometimes prove who you are with a fax 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 do at this stage.

While some registrars may be flexible around these issues, given the circumstances, this is also a ripe time for fraud, so it is likely you will be required to very clearly prove who you are if you need to transfer domains. On the registrar's Web site, they usually have information about how to contact them for changes if you have lost your password or your admin contact information is out of date.

+ Load the Web site

Once you have the Web host and domain registrar pointing to the right address, you can begin uploading your Web pages, either simple contact pages if you have no backups or the original Web site if you do have backups.

E-mail hosting

If your Web hosting company was also hosting your e-mail, you will want to use your new Web host to also provide your e-mail hosting. This may require you to pay for extra e-mail hosting services, or it may be included (up to a certain number of e-mail addresses). However, you will need to update what is called your MX record, which is similar to updating your Web site domain address. Typically, your e-mail 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).

No 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 convincing them of who you are, 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 in the WHOIS lookup on DNSstuff.com listed above.

On the WHOIS information page:
The "Sponsoring Registrar" is your domain registrar.

You can also see who registered your domain for you 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 fine, but you do not have direct access to the domain control panel, and so you'll 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 e-mail address is masked, making it harder for you to find out what e-mail address to use to contact the registrar. Hopefully, the street address is correct (and matches your letterhead), making it easier to send it 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 "Name Server". Sometimes it is obvious (dns.webhostcompany.com), and sometimes it's just an IP address. You can use DNSstuff.com to do a "reverse lookup" of an IP address to find the Web site name for that company. Note that this will not always reveal who the Web host is.

If your organization was hosting its Web site in-house, the WHOIS results can be very confusing, so try to clear that up before getting lost in recursive searches.

DEALING WITH LOST PASSWORDS

You may have lost access to passwords for some systems. Here are some ways to regain dominion:

+ Admin rights on computers

For 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

If you don't have Internet access, or you'd like more assistance, look in the resources in **Appendix C** for services that will help you do this.

For Macintosh computers, you can use a Mac OS install 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)". This is actually a reference to the root user. Do not confuse it 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/account name and password, try sending an e-mail 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 these are 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.

CLAIMING INSURANCE

Often insurers want detailed information on the systems you had before they'll pay out. But many of you may not have kept good records of your computers or may have lost what you had.

If so, others may have kept this information for you. Some people to ask:

+ **Vendors**

  If you know whom you purchased technology from, the company may be able to provide you with copies of your receipts which will 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 too.

+ **Funders**

  If your technology was paid for by a funder you may have provided them with receipts or other details on the purchase. Ask for copies of your grant reports.

If all this fails, do not panic! Your insurer is likely to be flexible. Talk to your agent about what they need from you in the absence of full inventory. In the meantime, put together the information you can remember on a form like the one we've included in the retrospective Disaster Analysis in **Appendix A**.

DONATED OR BORROWED TECHNOLOGY – WHAT YOU NEED TO KNOW:

Depending on your situation, you may be relying on borrowed, donated, and free equipment and services. You're probably wondering how to start. Here are the most important things to think about as you rush to get services restored and functional using this equipment.

Working on your Business Impact Analysis (see the Triage chapter) as soon as you practically can is still a priority. 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 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 so you can 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's computer, or one loaned to you by a friend, 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, while respecting the constraints imposed by the equipment's owners.

+ **Set expectations with the lender**

Make sure you and the lender understand what's acceptable and who carries responsibility if anything goes wrong. If there are known issues with the equipment, you need to know about them before deciding if it's 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 might want to have a formal contract.

+ **Set up a separate 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.

All recent versions of Windows, Macintosh, and Linux allow for the creation of additional user accounts. For Windows, look under the User Accounts or a Users and Passwords section of Control Panel. For the Macintosh, look under the Accounts system preferences pane.

+ **Get a firewall and virus protection in place**

See **Appendix C** for suggested security products.

+ **Transfer to new equipment properly and promptly**
  - Back up all of your data from the borrowed equipment.
  - Move your backups over to your new equipment.
  - Check to assure 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 (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 functions and features you may rely upon may not be available to you. Go slowly at first, making sure that the software and hardware you are using will be 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, reformat the hard drive and reinstall the operating system and your software.

USING FREE SERVICES

A lot of companies are offering free use of their online products to organizations affected by Hurricane Katrina. If you've lost everything, these might be just what you need to get back on your feet. But entrusting your information to an unknown system could also be a costly mistake that will hurt your organization in a few months time.

Make sure:

+ **To 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**
+ **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 youto 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.**

See **Appendix C** for a list of free or inexpensive online services for nonprofits.

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 who volunteered long hours, vital knowledge, and great resources:

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

Bryan J. Sharkey, BC and DR Consultant London, United Kingdom

Allan Thompson, Santa Clara County FireSafe Council (http://www.SCCFireSafe.org)

Other members of the nonprofit technology community also helped with suggestions and ideas, including people from the Riders listserv and NPower (http://www.NPower.org/).

APPENDIX A
RETROSPECTIVE BUSINESS IMPACT ANALYSIS

Appendix A Table of Contents

Objective

The objective of this document is to retrospectively assist in recovery of the nonprofit following a major disaster.

Part I – People

To recover from a disaster, it's important to respond quickly and effectively; identifying needs, prioritizing resources, and communicating clearly. This chapter covers organizing people and communication during the crisis so that you are able to accurately analyze the impact on of the disaster on your organization and prioritize recovery efforts.

+ **Having determined whom in your organizations makes which decisions; make sure there is a cross-checking process. Try to communicate simple messages.**
    - A message pad and to-do list in the absence of a Risk or Issues Register will suffice
+ **Beware of Rambos making dynamic decisions, especially if this can risk life and limb.**
    - Some people feel they must be seen to be dynamic – try to harness this energy by getting them to organize coffee, sandwiches etc.
+ **If you have a plan, great! – If not, establish a modus operandi**
+ **Ensure you're receiving accurate feedback from Emergency Services regarding the current status; keep up to date with their chain of command. They may also require information from you. (Do not assume that Emergency Services will keep you informed and never assume that the danger is over).**
+ **It is essential to appoint good public relations both internally and, if necessary, externally. (Don't believe everything you see on the news or read in the press – it's their job to sensationalize).**
+ **Call staff, using a cascade principle via normal chain of management. (i.e. start at the top and each person should call the people they directly manage). Make sure everyone is covered! To do this, you will need up-to-date home and mobile telephone numbers which must be readily accessible.**
+ **Establish a help desk, maybe two, one for customers and one for staff. If you don't, the switchboard will be swamped.**
+ **Start to evaluate the likely impact on the organization.**
+ **Do you need to activate third party contingency suppliers (e.g. Salvage companies, mobile computer room suppliers)? It may be worth contacting them to put them on notice of potential need.**
+ **Set up project teams and get key decision-makers to meet regularly.**

+ **Discourage other staff from turning up to help. (Everyone wants to join the adventure, especially the guy who forgot to back up his computer.)**

+ **Keep it controlled and, above all, professional at all times**.

Deliverables

+ **Staff Call Tree**
+ **Supplier Contact List**
+ **Plan of Action**

Who does what where and when?

+ **Seating plan and supplies for new work environment**
  - Desk
  - Telephone
  - Diary
  - Paper
  - Pens etc.
+ **Forget technology at this stage, IT can come later**
+ **Identify through staff, daily work schedules, and processes (Document for Recovery)**
  - Clients
  - Work in Hand
  - Orders
  - Delivery Schedules
  - Appointments (Re-arrange)

Floor Plans

+ **Create Floor Plans for new premises or revised floor plans for recovered premises**
  - Function
  - People
  - Replacement or Temporary Staff

Part II – Process

- Link to BIA – Process will be defined in this documentation

Deliverable Tracking

Item	Start Date	Completion Date

Technology

Technology Refresh – Key Applications by Business Unit

(RTO = Required To Operate)

Application Name	Business Unit	Office	Server ID	<=24hr RTO	72hr RTO	7 Day RTO
Windows XP				N	N	Y
Microsoft Office						

Technology Refresh - Key Recovery Staff

Assuming all staff is available, the table below highlights the key personnel required in the recovery of systems and at what location those systems will be recovered.

Service Type	Implementers	Location

Project Planning and Rollout

- Plan your recovery using BIA as a first pass, prior to attempting to recover. **Seriously consider dry runs rather that just jumping into recovery**. A day's worth of planning will save time, energy, and pain.

Transport requirements

- List all transportation requirements. (e.g. Private Cars, taxis, public transport. Ensure that you detail parking and special needs).

Expense Codes

- Keep track of expenses so you can let funders know the impact of recovery on your finances. Consider booking all time expenses to a disaster recovery expense code.

Accommodation

- List all accommodations required by type and duration. Don't forget items such as rations, etc.

Communications

Contact Lists

Recovery Contacts

Name	Address	Type of Vendor	Telephone	Mobile
Bryan Sharkey				07808 582360

Desktop Recovery Contacts

Name	Address	Type of Vendor	Telephone	Email

Network Recovery Contacts

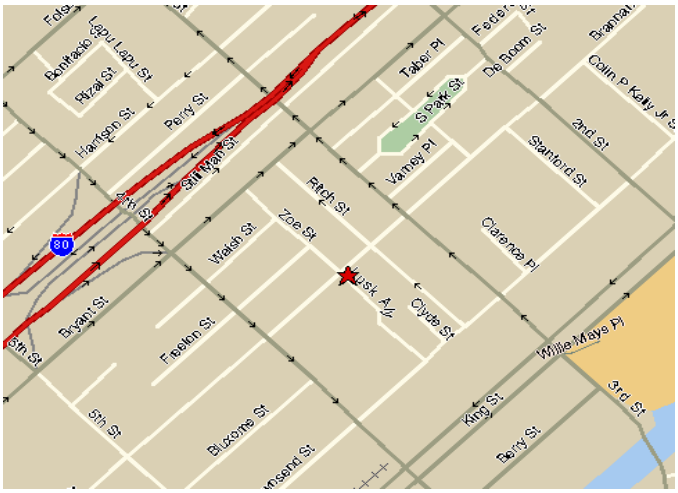
Name	Telephone	Fax	Mobile	Email

Escalation Contact List

Name	Role	Location	Work	Mobile

Directions

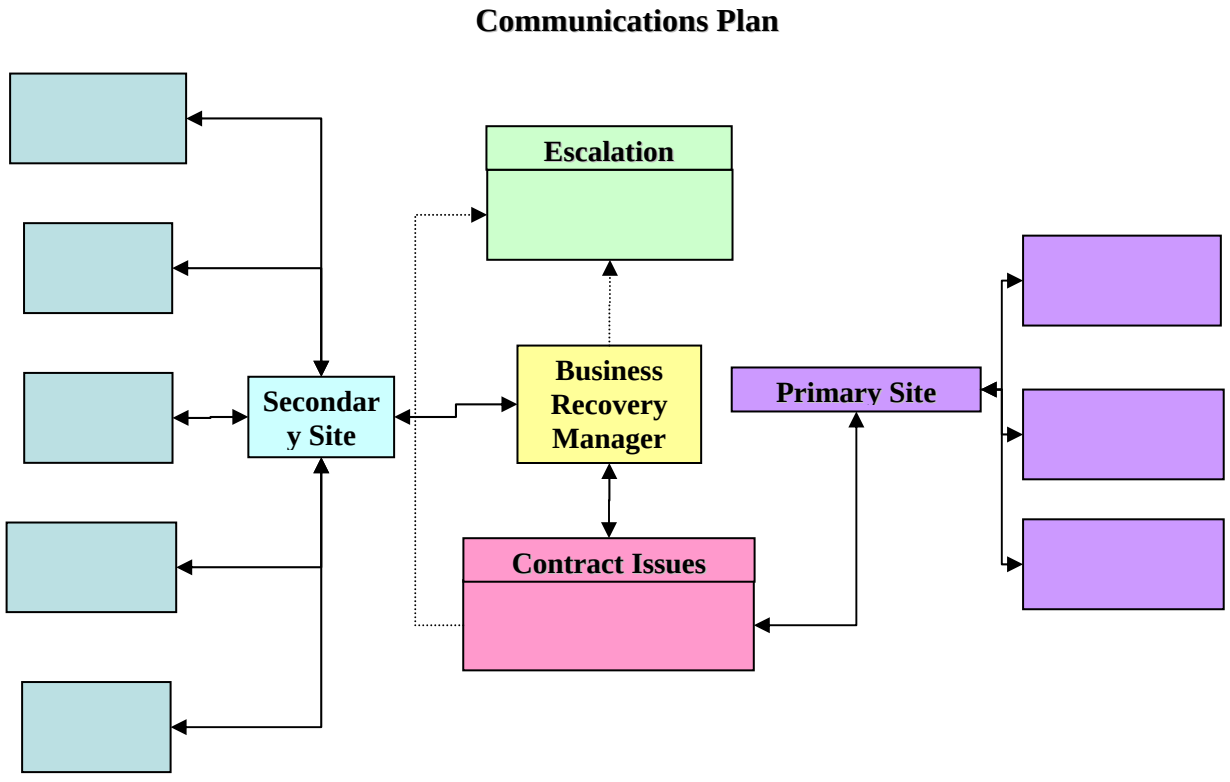
Insert Directions and Maps (These can be downloaded from Internet sites). Example:



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

Communications Plan



BUSINESS IMPACT REVIEW QUESTIONNAIRE

BUSINESS UNIT INFORMATION

OVERVIEW OF THE BUSINESS UNIT

Location :

Business area :	Product area :

Describe business function :

Describe overview statement of the recovery objectives for your business unit :

Number of staff :

Please provide an **organization** chart for your business unit.

Rate the CRITICAL nature of the business function based on the impact of its unavailability:

Impact	Rating	Comment
Critical for business survival	1	
Serious damage	2	
Significant damage	3	
Major impact	4	
Minor impact	5	

BUSINESS PROCESS

What are the business processes performed by your department? Include the name and a brief description of the business process:

Process Name	Description

Analysis of Key Processes

Identification of Key Processes

Name of Process:	
Description:	
Questionnaire completed by:	
Date:	

(N.B Please use additional sheets for more than one process).

Legal & Regulatory

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

Yes	No	Comment

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

Yes	No	Comment

If YES:

List regulations (if known)	
Describe the conflict or situation	
Describe consequences (i.e. penalties)	

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 that prevents normal business operations from taking place.

Revenue

Estimate the expected revenue loss to the nonprofit if this function were not performed following a disaster:

		Assumptions and Justification
Revenue loss after 3 days	USD.	
Revenue loss after 1 week	USD.	
Revenue loss after 2 weeks	USD.	
Revenue loss after 1 month	USD.	

Costs

Estimate what additional costs (fines, claims, cancelled contracts, lost discounts, interest payments, etc.) the nonprofit would incur if this function were not performed following a disaster:

		Assumptions and Justification
Additional costs after 3 days	USD.	
Additional costs after 1 week	USD.	
Additional costs after 2 weeks	USD.	
Additional costs after 1+ month	USD.	

Health and Safety

Health and safety would be compromised if this process were not performed following a disaster:

			Rank
Health and safety definition:		3 days	
A process, if not performed, may directly or indirectly impact the health and safety of employees, customers or other third parties.		1 week	
		2 weeks	
		1+ month	

Operating Efficiency

Operating efficiency <u>within</u> the nonprofit would be affected if this process were not performed following a disaster:

			Rank
Operating Efficiency Definition:		3 days	
These are processes which directly effect the internal day-to-day business of the nonprofit and may have an impact on other important functions or processes.		1 week	
		2 weeks	
		1+ Month	

WORKFLOW RELATIONSHIPS

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	Purpose of interface

Staff Relocation Requirements

List the number of desks and type required?
Desk and phone :
Desk, phone, and PC:
Admin. and printing:
Other (please specify) :

Immediate Requirements

Business unit name	Must be near	Would like to be near	Maximum distance	Phone ability	Brief description of reason

Business Partners

List any business partners that you interact with.

Business Partners	Cut-off time

VITAL RECORDS

Data/Files Recovery

It is up to each business unit manager to identify where any critical files needed for recovery are stored.

Report Requirements

Critical reports required

Report Name	Frequency	Number of copies required for recovery	Where the report is stored

Sensitive Documents/Forms

Do you have any critical, sensitive documentation/forms that are required to be stored off-site?

Document description	Where stored Off-site

Hardware/Software Resources

Indicate how many items are used and what is required in a recovery mode.

Equipment	Current	Day1	Day2	Day3	Day4	Day 5	Week 1+

List the software and applications that your business unit uses and would require in recovery mode.

Software Name	LAN	Hard Drive				Recovery availability Time frame

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

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

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

Miscellaneous Resource Equipment

Supply description	Amount needed

Voice Recovery

Indicate your phone requirements

Type of dial tone lines	Number at primary site	Number at required recovery site
Single line		
w/speaker phone ability		
w/recording		
Two line		
w/speaker phone ability		
w/recording		
Speaker Phone		
Private Lines		
w/speaker phone ability		
w/recording		

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 lasted updated

Do contingency plans exist that provide step-by-step instructions for the recovery and performance of this business function?

Supplier Contact Details

Supplier Name	Contract Type	Reference No	Contact Details.

APPENDIX B
TIPS FOR REVIVING BROKEN COMPUTERS YOURSELF

Computers are more resilient than most people realize! And, as most of us do not follow the golden rule of backing up data frequently, it is probably worth trying a couple of these tips before declaring your computer dead. The computer may not be in a usable condition, but you may be able to recover critical data.

Some of the tips have been gleaned from real-life experiences that were published on TechRepublic.com, some are last-resort actions that are not recommended by manufacturers. We offer them here to provide ideas, though 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.

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

+ **You do not 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 TIPS

+ **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 up and see if the manufacturer can do anything to fix it.**

Finding this information will ensure that anything you attempt will have a greater chance of success.

WAIT UNTIL THE COMPUTER IS **TOTALLY** DRY BEFORE ATTEMPTING ANY OF THESE TIPS!

+ **"The sounds of the game"**

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.

+ **"Put the right spin on things"**

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 was fine, tap the drive lightly on the side to see if it spins. Sometimes that works. (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.

+ **"Back to the Bios"**

If the drive is spinning and the cables are properly seated, check the "Detect IDE Hard drives" in the bios. For some reason, on some of the older motherboards, it will pick up a drive that "AUTO" won't pick up.

+ **"Freeze it" – Last resort!**

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.

+ **"Drop It" – another Last resort!**

Sometimes a hard drive that has been running forever won't spin after being shutdown for awhile. 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.

These 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 if possible. 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.

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.

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

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

Other problems: 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 the preceding problems can prevent you from starting Windows XP Professional in normal mode, 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.

Table D.2 lists these tools according to the preferred order of use, from tools 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, watch the screen.
- When you see the message **Please select the operating system to start**, press F8.
- Use the arrow keys to highlight the appropriate safe mode option (safe mode or safe mode with networking, if you want to test the network), and then press Enter.

You can use the same steps to go back to the Last Known Good Configuration (see table D.12).

Table D.2 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. Backup (Ntbackup.exe) enables you to restore system settings and data if your 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.
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 does not solve the problem. ASR is available in safe or normal mode.

USEFUL LINKS

www.techrepublic.com
www.microsoft.com
www.mac.com

APPENDIX C
RESOURCE LISTS

These resources have not necessarily been tried by CompuMentor. Check out any service or product before you buy.

DATA RECOVERY FIRMS

OnTrack
Nationwide (800) 872-2599
http://www.ontrack.com/
Free assessments for those affected by Katrina.

Drive Savers
(800) 440-1904
http://www.drivesavers.com/
The company is reducing its service fees by one third and waiving its typical $200 attempt fee. The discount will remain in affect until November 30, 2005.

Data Recovery Group
North Carolina (888) 462-3299
http://datarecoverygroup.com/

Lazarus
California (800) 341-DATA
http://www.lazarus.com/

Reynolds Data Recovery
Colorado (800) 223-7483
http://www.data-recovery.com/

Gillware
Wisconsin (877) 624-7206
http://www.gillware.com/

FIREWALLS AND VIRUS PROTECTION

Firewalls for standalone computers:

If your computer is directly connected to the Internet and you do NOT have a firewall on your network, you should use a software firewall on your computer. The following products contain software firewalls and anti-virus tools. To help ensure they will protect your computer, make sure you read the instructions and use them correctly:

Zone Alarm
http://www.zonealarm.com/ (15-day free trail)

Symantec's Norton Internet Security
http:///www.TechSoup.org/Stock
Available to qualified nonprofits for a small admin fee at TechSoup Stock. *

Firewalls for simple networks:
For a simple, small office network connected to the Internet, we recommend using NAT (network address translation) functionality, available on almost all routers.

Firewalls for more complex needs:

If you have complex needs, such as VPN or greater-than-average data privacy requirements, you need the advice of an IT professional.

Cisco PIX firewalls*
http:///www.TechSoup.org/Stock
Available to qualified nonprofits for a small admin fee at TechSoup Stock.

Virus Protection
For straight virus protection in a firewall-protected environment, we recommend:

Symantec Anti-Virus*
http://www.TechSoup.org/Stock
Available to qualified nonprofits for a small admin fee at TechSoup Stock .

***** *These products are available to most 501©(3) organizations through TechSoup Stock – http://www.TechSoup.org/Stock 800-659-3579 ext 700*

Grisoft's AVG Anti-Virus
AVG provides discount pricing on its larger products to nonprofits. Search for "Charity" on its Web site: http://www.Grisoft.com/.

McAfee Anti-Virus
http://www.McAfee.com/

WINDOWS ADMINISTRATOR PASSWORD RESET SERVICES

Password-Reset
http://www.password-reset.com/
Provides downloads to create boot disks, shipped disks, or a telephone walk through to help you reset your passwords. Prices range from $19.99 - $39.99.

NTAccess http://www.softwareshelf.com/files/products.asp?ID=141
Provides a download that will allow you to create boot disks to help you reset your password. Cost: $70.

FREE/INEXPENSIVE TECHNOLOGY SERVICES FOR NONPORFITS

Donated and Discounted technology Products for the Nonprofit Community:

The following nonprofits provide donated and discounted technology products to the nonprofit community.

TechSoup Stock
http://www.TechSoup.org/Stock
(800) 659-3579, ext. 700
TechSoup offers donated and discounted technology products from companies like Microsoft. TechSoup Stock and its donation partners are working to assist disaster relief and rebuilding efforts. See http://www.TechSoup.org/Katrina for details.

Gifts in Kind International
http://www.giftsinkind.org/
Paid membership gives you access to a greater range of products, but not all technology products require membership.

TechFoundation
http://www.TechFoundation.org/
TechFoundation has negotiated discounts with some large and well-known technology vendors, such as Dell and CDW.

Voicemail (of sorts!)

Air America Radio
http://www.airamericaradio.com/katrina/voicemailinfo.html
Set up a free public voicemail system for the duration of the crises. You call **(866) 217-6255** and, once connected, dial your regular phone number and you'll be able to leave and pick up messages from friends and family members who may have left messages for you. This system has no privacy safeguards – anyone can listen to any message – but it could be useful if telephone communication is still difficult.

Online fundraising and constituent relationship management:

Salesforce.com
http://www.salesforcefoundation.com/
Provides up to 10 free licenses for its enterprise edition CRM product to qualifying nonprofits.

eBase
http://www.ebase.org/dl/
A free FileMaker based fundraising/CRM database.

Online communication and collaboration tools

The Stargazer Foundation
http://www.Stargazer.org/
Temporarily waving its online tools' fees for uses that help with the Hurricane Katrina recovery.

SOURCES OF SKILLED HELP

Be careful when engaging a consultant or volunteer whom you do not know for highly skilled tasks. Do your homework. Check references (even if someone has recommended them to you); insist on receiving explanations you are comfortable with; define your project carefully; know your priorities and your budget; set up a separate account on your PC for the consultant to

use; make sure they document the work they do, including all administrator account names, and passwords that they set up.

CompuMentor hosts the TechFinder database, a national database for technology consultants who specialize in working with nonprofits. It's available online at: http://www.TechSoup.org/TechFinder

We've also done outreach in Katrina affected areas to find out if consultants are still operational and if there are others who would be willing to help nonprofits out during this period. We will continue to update this listing as we get new information. The most up-to-date version can be found online at: http://www.TechSoup.org/Katrina

Other places to ask for help:

+ **Recommendations** from fellow nonprofits, board members, neighboring businesses, family, and friends.
+ **Local Technical Colleges:** Students may not be back in class and could be a great source of volunteer help. Check your Yellow Pages for colleges that offer computer classes.
+ **Churches**
+ **Craigslist**

  http://www.craigslist.org/

  A favorite with many people in the technology world. Lists volunteer opportunities (and more) grouped by region.
+ **VolunteerMatch**

  http://www.volunteermatch.com

  A site matching organizations looking for volunteers and individuals looking for volunteer opportunities.