

# Why Everyone Needs a Disaster Recovery Plan

by Cynthia Caldwell and Laz Smith, Geekz, Inc.

Yes, EVERYONE. And I'm not talking about an evacuation plan from your building in case of fire, nor home land security preparedness involving plastic and duct tape. I'm talking about your computer.

What if the computer you are reading this on right now were to just shut off this instant and not come back on? You'd be panicking, wouldn't you? This is the type of disaster I'm talking about.

Hardware fails. It is not a matter of *if* but *when*. Sometimes it can be fixed, sometimes it can't, and sometimes it just isn't cost effective to fix. Even if it can be fixed, it may take time to get the part. And is it still under warranty? What are the terms of the warranty? Do you have to send it in for service or do you have next day on-site service?

Let's use the analogy of your old TV. It's an analog, cable-ready, 36" picture tube you bought 5 years ago. It cost a good bit of money at the time. You've been very happy with it because it has just the features you wanted and you like the layout of the remote. You got an entertainment system that fits its dimensions like a glove. You have it programmed with your favorite channels and have it hooked up to your stereo, DVD player, and Xbox. All is good, until suddenly... POOF! The picture is gone. GAAAAHHHH! It's the day before the big Superbowl party!!! Now what?!?!?

Here's what will likely be going on in your head:

Should I get it fixed or buy a new one? Is it still under warranty? Can I get it fixed in time for kickoff? What will that cost me, especially on short notice? Is it worth getting it fixed since it's not digital and is basically obsolete as of February 2009? Hmm. Maybe this is an opportunity to buy a new one... What make? What model? Do I have enough money right now? Could I get it delivered in time? My neighbor's kid who helped hook everything up is off at college now... how will I get it all hooked up? And will I be able to get one that fits the space as well as this one? And I'm so used to this remote. I like this one. Sigh. And I'll have to reprogram all my favorite channels again... hmm. Can I remember what number is for the Weather Channel? I don't want to deal with this! I can't deal with this! It's overwhelming! Help!

It's just a TV, right? But what if this was your computer? Not only do you have to deal with the computer hardware, but what about the data? All the programs you've installed?

If it's your home PC, you'll be thinking, will I lose my email? My photos? My documents? My Quicken data? My bookmarked sites? My games' high scores? Just how will I survive?

Now imagine it is your office PC – or worse yet, your server. All of your company records. Email. Financials. Customer data. Or what if it is your PBX system hardware and your phones are all down? Did you lose your voice prompts? Voice mail? Just imagine how you'd react in that situation.

Most people have never really thought about this, or at least not enough to put plans in place. And if you are one of the few who have, are you confident in your disaster recovery plan?

## What is a disaster recovery plan?

So what is a disaster recovery plan? The short answer is that it is a thought out plan for how you could recover from a disaster and the actions you should take now to keep the disruption to a minimum. Yes, it covers the big disasters you might be thinking of, like a flood from heavy rains, or your building being leveled by a tornado. Maybe you think the odds are so little it isn't worth worrying about. But disaster recovery plans cover all types of other "disasters" of all sizes, like fire, or burst water pipes, or power surges, or just a simple hardware failure. (Because it *will* fail eventually.) Sometimes you'll have warning of an impending disaster and have time to react, and sometimes you won't.

You are thinking insurance and warranties cover all that, right? Well, yes and no. Sure, assuming you have the right coverage, they'll pay to repair or replace equipment. Many warranty programs require you to send them the faulty equipment for repairs, which can take weeks. And the insurance company might even help you with a temporary setup if necessary. *But what about the data?* How long will it take to get your business back up and running immediately so you don't lose customers or income? And what about all those historical records you need for the IRS?

Some people have fireproof boxes or vaults. They think that they can put their backups in there for safekeeping. These containers are fireproof, but *not heatproof*. Plastic melts. So CDs, DVDs, tapes, etc. are not necessarily protected.

Sadly, you are not alone if you are not prepared for any of this, or have not even thought about this. But this is important. It is your business. Your income. Or, even for the personal PC, it is your tax records. Your memories. A 2000 study by the Gartner Group found that 60% of businesses that experienced a data disaster ceased operations within two years. You might be thinking "I do backups, so I'm ok." *How confident are you that your backups are reliable and sufficient?*

"Great," you're thinking. "Now you are telling me I need to spend a ton of money I don't have. What will this disaster plan cost me? This isn't some scam like the car salesman talking you into the special undercoating on a new car, is it?" Well, the cost is really up to *you*. You need to weigh the upfront expense of a solid disaster recovery plan and investment against the cost if you don't have one. Assume you lost your PC or server and access to its data for a week. Could you still run your business? Would you have employees just sitting around that you still have to pay? How much income would you lose? Would you have clients move their business elsewhere? And long term if you don't get all of your data back, what is the cost of that? What if you lost your A/R records and could no longer collect what is owed you? What if you have to pay someone to manually re-enter paper records like receipts? How will you do your taxes next year?

Look at this logically. Crunch some numbers. Now you can see the rough cost if you *don't* have a disaster recovery plan. So, how much are you willing to invest so that you *do*? Remember, this is really no different than any other insurance plan. You pay money up front

just in case. You may not have an agent or policy number, but the concept is the same. Just like any other insurance, only you can decide how much you can risk by not having as much coverage.

Now, do you have a number? Or maybe you have two numbers – one for a plan for the “minor” disaster and one for the “major” disaster. Now that you have a budget, you can assess what you can get for that money and then adjust as necessary.

## **How do I create a disaster recovery plan?**

So, what are your options? The best thing to do is have a professional come in to do an evaluation and give you a proposal with the right options for your needs, and then train you as needed. A knowledgeable consultant will ask the right questions, not just about your current setup, but also your plans for future growth, your level of technical know-how for implementing a plan, and the time you are willing to invest on an ongoing basis to keep the plan running smoothly.

But you still want a little information before you bring in the pros so you can be knowledgeable on the subject. First, you should answer the following questions. This list isn't all-inclusive, but it should get you thinking in the right direction.

- Do you have the original installation discs and product keys for all of the software you have installed (including the discs that came with the machine)? What about software you downloaded (and don't have discs for)? Do you have the email with the codes you need and/or the setup files stored safely?
- Have you made backups of these original installation discs and have them stored in a separate place?
- Do you know the user names and passwords for all of the accounts that are currently set up with saved passwords? (For example, e-mail passwords are often forgotten.)
- Do you know where all of the software you use stores the data and configuration files? Some let you choose (e.g., Excel) and others by default install it under a data directory where the program is installed (often under Program Files, e.g., Quickbooks). Still others have a fixed location, sometimes tied to hidden folders under the user profile (e.g., Outlook Express), or in the registry.
- If you have more than one computer, do you have a centralized storage place for all of your data, or does each PC have its own set of local files?
- Where is your email stored? In an Exchange server, locally on your PC, or online?
- How much data will need to be backed up? There are several numbers to look at:
  - how much total disk space is being used today, including the operating system
  - how much disk space is for your data to be backed up
  - how much is archivable, (where you could do a one-time backup and it won't change), versus...
  - how much is active, (that needs backing up frequently)
  - how much is critical (i.e., you can't run your business without it)

- How often are you adding or changing data?
- How hard would it be to recreate some of this data if it were lost and how critical is it to recreate?
- Have you considered where and how you could have an offsite backup?
- If you accidentally delete a file, how quick and easy do you need it to be to restore that file?
- How much effort are you willing to put into making sure the backups happen? Will you be disciplined enough or would you be better off with more of a hands-off approach? How much time can you spare to make this happen per day and per week?
- How long could you be down without a working computer (or server)?
- How long could you be down without your data (or subset of it)?
- When things go down, do you have a list of contacts (not on your computers) to call to get it all back and running? (And this isn't the time to start shopping for a new phone or computer technician.)

## **Data backup options**

Now that you have put some thought into your needs, below you will find some of the backup solutions at your disposal. Again, this list doesn't cover all possible options, but it gives you an idea of the range of options, what they do for you, their pros and cons, and their approximate costs. You may actually want to implement more than one of these solutions for different scenarios and backup schedules. It is highly recommended to get a consultation from a professional in this area to make sure you choose the right solution and implement it correctly. It would probably take 1-3 hours for someone to review your situation, research options, and produce a quote.

Note: in the following table, amounts shown are for cost of hardware, software, and media. It does not include time or labor costs for setup or installation, nor does it include the ongoing cost of your time involved for doing the backups.

Option	Pros	Cons	Costs
CD-R/RW	Hardware and media are cheap. Portable (for taking copies offsite).	Less than 700 MB capacity. Requires user intervention. Single user. Slow.	under \$50 for drive + pennies for media
DVD-RW	Hardware and media are cheap. Portable (for taking copies offsite).	4 GB capacity (8 GB for dual-layer DVDs). Requires user intervention. Single user. Slow.	under \$70 for drive + dimes for media
ZIP drive	Hardware and media are moderately cheap. Portable (for taking copies offsite).	Disappearing technology. Very limited capacity (100-250 MB). Requires user intervention. Single user. Slow.	\$100 & up for drive + \$10 & up for media
USB or FireWire Desktop External Hard Drive	Fairly cheap, depending on size of drive. Lots of space (100 GB – 1 TB).	Not practical for offsite. Requires some user intervention. Single user. Slow.	\$100 & up
USB Flash drive (a.k.a. thumb drive)	Cheap. Portable. Easy to use. Good for manually backing up documents, Quickbooks files, photos.	So small they are easy to lose. Not secure. Requires user intervention. Single user. Slow.	\$20 & up (depending on capacity)
Online backup solution (e.g., Connected.com)	Fairly cheap, usually a monthly fee, based on space purchased. Automatic.	Requires fast Internet connection. Various plans with different space limitations. Slow. Single user. Restore options may be limited (all or none).	\$15/month & up
Tape Drive 4mm/DAT/DDS	Industry standard for backing up servers. Allows off-site storage, multiple restore points, incremental backups. Able to back up entire server. Automated except for swapping tapes.	Not cheap. Can be complicated to set up and monitor. Requires special hardware and software. Limited portability. Slow to restore.	\$800 & up for hardware + \$30 & up for media (each tape, reusable)
Backup software (e.g., Handy Backup, Platinum Backup, Backup Exec)	More options and easier to use than Windows built-in backup solution. Can set up backup schedule with rules. Better than manual drag & drop to backup location.	Add-on cost for most of the above hardware solutions.	\$30-\$200
Built-in backup features of programs (e.g., Quickbooks)	Built-in solution should make it easy to make sure the right stuff gets backed up. Can back up to a back up folder (good in case of corrupt files or user error) or external drive (network, USB).	Limited to just the data for that program.	None
Network storage device (network-addressable hard drive, e.g., SNAP Server)	Completely separate data server. Automated duplication of critical data possible. Easy set-up. No user intervention unless there's a problem.	Not cheap. Not portable for offsite safety.	\$400 & up
Cross-machine backups (one machine backs up another's data and vice versa)	Cheap, if you have the disk space.	Not portable (no offsite).	None (if use existing machines)

## Systems continuity options

The list above shows several options for making sure you don't lose your data. But you also must consider how long you can handle if your system(s) go down. If you need your business to keep running without any or minimal interruption, you will want to make further investments to make this happen. Even something as simple as a power outage can cost you hundreds or thousands of dollars. Here are just a few types of interruptions and possible solutions to help gracefully recover from them.

Option	Pros	Cons	Cost
<b>Power</b>			
UPS (uninterruptible power supply, a.k.a. battery backup) and surge protector	Keeps systems running for short periods of power interruptions. Protects equipment from power surges. Allows you to save your data and shut down gracefully.	Don't last very long (but better than nothing!). Need for each PC and server, and possibly other equipment (VoIP phones, PBX system, POS system, modem, router, switch).	\$50 & up (depending on capacity)
Backup generator	Keeps systems running for longer periods.	Need electrical expertise to hook up and do switch over properly. Need external storage. Requires periodic testing.	\$750 & up (depending on size)
<b>Computer Systems</b>			
RAID1 disk array (mirrored drives) usually just for servers	Moderately priced. Data is safe and intact – complete duplication of hard drive. No user intervention unless there's a problem.	Inefficient use of space (2 drives but usable space of 1). Down time required to switch to mirrored drive when primary drive fails. Expertise required to recover data.	Cost of extra hard drive(s)
RAID 5 disk array (triplicate drive sets) usually just for servers	Moderately priced. Data intact and server keeps running when 1 drive fails. No user intervention unless there's a problem.	Requires special hardware. Difficult to recover data if machine dies and needs to be replaced.	\$400 & up for RAID controller card + cost of extra hard drives
Backup/redundant PC/software	All software and access to data available on more than one PC in case primary system fails. If you need multiple PCs to have the software anyway, no added cost.	Requires duplicate licenses of most software. More maintenance to keep additional software up-to-date.	Cost of PC plus software
Redundant system (alternate server(s) running onsite or offsite)	Complete copy of system available to switch over to quickly if primary server out of service for extended period.	Expensive to buy and maintain. Requires duplicates of hardware and all software. Switchover may not be automatic.	Cost of duplicate server plus maintenance (and possibly offsite fees)
Extended on-site warranty coverage	Usually provides on-site repair/replacement next day. No waiting for parts to ship.	Cost. Read the fine print, as not all things are covered under all circumstances. Beware: third-party warranties usually sub-par.	Varies by manufacturer
<b>Services</b>			
Backup internet service	If your primary ISP goes down, can switch to alternate service fairly easily.	Ongoing (monthly) expense.	\$15 & up per month (depending on speed)
Backup phone service	If your main phone service goes down (particularly with VoIP), have at least 1 alternate phone line	Ongoing (monthly) expense. Unless entire system is duplicated, backup service mainly for outgoing calls and maybe as a forwarded line for emergency (depending on your phone service options)	\$15 & up per month (depending on # lines and service options)
Backup MX records (if you host your own email)	Backup service queues up incoming mail until your server is back up and running so it isn't lost/bounced.	Ongoing (monthly or yearly) expense.	\$30 & up per year (e.g., through No-IP.com)
Backup web hosting (if you host your own web site)	Backup service allows alternate server to host web site until primary server is back up.	Ongoing (monthly or yearly) expense. Only recommended if your business depends on web site (e.g., online store front).	\$100 & up per year

## What else is there to think about?

We've talked about backup procedures and contingencies when things go wrong. What else is there to think about? First you need to document and test your solution. Writing it down will help you think more clearly about it and get it organized for when you need it. Then, once it is implemented, do a fire drill of sorts. Think of disaster scenarios and test your plan to see if it will work. Are the systems in place as planned? Can you actually recover data from one of your backups? Once in place, it should also be periodically reviewed to see if it is still the best solution. Your needs may have changed and the plans may need to be revised as a result.

Security is another area to think about. If you have sensitive client or employee data (financial or medical records, social security numbers, credit card numbers, etc.), are you protecting this data as required by law? Does your offsite backup plan entail having an employee bring unencrypted CDs home? Is your online backup secure? Are you handing over sensitive data if you send a machine out for repair? Many computer manufacturers (including Dell and HP) require you to return a defective hard drive that is under warranty if they send you a replacement. They will not provide a written guarantee that the data is destroyed properly.

And what about the security of your hardware? How easy would it be to steal your computers (either a break-in or inside job by a disgruntled employee)? We had a client who had their computers stolen and their only backup *was in the CD-RW drive*. What if an employee leaves the company? Can they still get into the building? Do they have remote access to the computers? Could they wipe out the data on the systems?

## Conclusion

We've presented just a sampling of solutions for disaster preparedness from a technical perspective. As you can see based on the data shown, as a general rule, the more convenient and robust the solution, the pricier it is. But losing your data and productivity could be a lot more costly. And the least expensive solution on paper may not be the least expensive overall if it takes many hours of your time a week to implement that you could be using to make money for your company. Plus, unless you are extremely diligent and manage to incorporate backing up your data into your routine, you'll likely do it for a couple of weeks and then stop. But only you can determine if you will be disciplined enough for a more hands-on solution.

So, are you convinced you should have a disaster recovery plan now? The name sounds so official and complicated, but when you break it down, it's really just making sure you are backing up your data, keeping good records, doing ongoing maintenance and checkups to fix or replace things before they break, and having an action plan in place so you'll be able to calmly handle the disaster, big or small, *when* it happens.

*About Geekz, Inc.*

*Geekz, Inc. is a Chicago-area computer consulting company that focuses on the unique computing, networking and application needs of residential clients, small businesses and branch offices of larger organizations. Geekz, Inc. helps clients meet their business objectives with scheduled maintenance plans, on-call computer support and emergency services.*