

What Would Happen If You Were Hit by a Bus?

Disaster Preparedness Strategies for Independent Consultants

Carol J. Elkins, Senior Member, Rocky Mountain Chapter

Independent contractors working out of home or small offices don't have a corporate IT department backing up our computers every night. Nor do we have the luxury of office colleagues who would inherit our workload if we suddenly disappeared. Added to our solo-concerns are our clients' significant monetary investment in the work lying on our desks. What would happen to your business and your clients' businesses if you were suddenly disabled—or more colorfully stated—if you were suddenly hit by a bus?

As an independent consultant, I'm very aware of the disastrous consequences that a disabling event in my life would have on my clients. If I were "hit by a bus" so to speak, my clients' production schedules would be disrupted (costing them lost business); they wouldn't have access to their current files; they wouldn't know where to begin to find another writer to help pick up the pieces. I want my clients to depend on me completely for tech writing services; I like having all their eggs in my basket. However, I believe they bear a disproportionate share of risk in their loyalty to me.

To even out the burden of risk, I practice several methods of disaster preparedness to mitigate my clients' downtime in the event I'm hit by a bus. My disaster paranoia...umm preparedness...also serves a second, equally critical need: it reduces my personal loss of billable time if my home office burns to the ground or another untoward event occurs. Any disaster preparedness plan needs to provide a way to back up my computer contents and be able to quickly recover that content. In addition, the plan must ensure that someone else can manage my business in my absence. Let's look at each of these requirements more closely.

Backing Up as if Your Life Depends on It

I have had the unfortunate experience of having a total computer system failure at least once a year for the past five years. Each instance was caused not by lightning strikes or viruses, but simply by installing innocent applications, such as a font program, antivirus update, or scrolling mouse driver. Although those experiences could be fodder for another passionate article, what I learned from them (other than never to install any program on my computer that isn't essential) is that you can never have too many backups. Call me overcautious, but I always plan for the worst possible situation and, way too often, that's the one that occurs.

As a result of these bad experiences, I've also learned that it is not sufficient to simply back up the data in the My Computer folder. What about the data stored directly in the application folder, such as the Outlook .pst file; Eudora mailboxes; Quicken data, Framemaker .ini. etc.? And what about the applications themselves? My disaster recovery strategies always include backing up my system files and applications as well as my data.

My ability to work efficiently depends on my software maintaining its "look and feel" from one day to the next. If my main workstation crashes, it will take me at least 2 to 3 weeks to reload software, adjust all personal settings, recapture system favorites, cookies,

patches, plug-ins, etc. Tweak, tweak, tweak. Until I get everything functioning as it was pre-crash, I am not focused and my efficiency suffers. Therefore, the only time I want to reload all my software is when I buy a new computer. So far, I've been able to time my new purchase to coincide with installing the next new Windows OS, so I'm often installing new versions of my software anyway.

My office consists of three networked computers—my main workstation; a secondary workstation; and a test CPU that runs older operating systems. Here are the disasters I prepare for every night and the recovery strategies I've developed to thwart them. As you read, ask yourself how *you* would cope with each disaster.

Minor Disaster: I screw up a critical client data file (or my client wants to revert to a previous iteration of a project). Every night I back up critical client data to a second harddrive. Other good options for backup devices would be a ready-to-be-retired CPU or a rewritable CD or DVD. I make separate backups for Monday, Tuesday, Wednesday, etc. An inexpensive (\$30) and easy-to-manage software application called Synchronmagic (<http://www.gelosoft.com>) makes this an absolute breeze. I use the Windows scheduler to automatically start Synchronmagic every night at 5:05 pm. This little program has saved my life on more than one occasion.

Major Disaster: Total harddrive failure—the dreaded blue screen of death. When this happens, I can immediately boot to a second harddrive inside my main workstation that has all my applications, system files, registry entries, etc., as well as all data files. To accomplish this, I created an identical image of my main workstation on a bootable harddrive, and I update that image every night. Thus, if my main harddrive is fried, I experience no downtime, and the maximum amount of work I might lose is only what I've done that day. Dantz Retrospect (<http://www.dantz.com>) is the only software I've found that can create a duplicate image of my computer's operating system, application settings, and user preferences without using a compressed proprietary file. That last part is important: other backup programs, most notably Norton Ghost (<http://www.symantec.com>), can create a compressed image of a drive, but you must decompress it before you have a workable directory structure (as in Windows Explorer).

Major Disaster: Lightning strike that fries the main workstation (both harddrives) or the motherboard goes out. In preparation for this disaster, I again duplicate my entire system, but I duplicate it to a second computer. In the event my main workstation goes down, I am able to move to the secondary workstation and resume work, having lost only the work that I had completed that day. I use Dantz Retrospect to do this, too. While I'm working on the second computer and continuing to earn a living, I can have the first computer repaired and then reinstall its operating system, applications, and data at my convenience.

Major Disaster: Office burns down or is demolished in a flood, hurricane, or tornado. Every night, I use Norton Ghost to update a compressed file of my entire system that is stored on a swappable harddrive. I change this harddrive every month and put it in an off-site location. "Off-site" can be a safe deposit box or a friend's house. Online backup resources are also an off-site option, but most are too expensive to back up the contents of today's high-capacity harddrives. When I store an offsite

copy of my entire system, maximum loss of data is one month; maximum loss of applications is only what I've added since removing the previous swappable drive. As soon after the disaster as I can purchase a new computer, I simply restore the contents of the swappable drive and resume working and earning a living. As horrible as it is to think about losing a month's work, it would be far worse to lose all of the expensive software sitting in CD sleeves on my shelf. Yes, I could make backup CDs of every application, but I find it easier to do it all in one nightly backup to the swappable drive, thus capturing any interim releases, upgrades, and updates.

I know these sound like rather elaborate steps just to back up your computer, but unless you have a strategy for each of the disasters discussed above, you are leaving a huge hole in your professional defenses. You do have medical insurance and liability insurance, don't you? Consider these backup strategies just another form of insurance—continuity insurance. And don't forget to test your backup strategies. Run a simulation of each disaster. It will do you no good to learn *after* a disaster really happens that your plan didn't work.

Backing Up Yourself

Okay, so you've taken my advice thus far and made sure that your computer is thoroughly backed up and impervious to any natural disaster that might beset it. What if something happens to *you*? That proverbial bus might strike you, or you might suffer a sudden stroke or heart attack. Every day on the news you hear about serious injuries sustained in car accidents. None of those people thought it would happen to *them*! We know their family and friends are traumatized by the accident, but if the injured person is an independent consultant, who's going to tell the clients the bad news? Those clients shouldn't have to hear it on the 10 o'clock news report. And their business shouldn't be jeopardized by your being incapacitated.

Depending on the workflow between your office and your client, you can do a lot to help them feel more secure. You might already be giving them frequent updates of the project so that they have minimal backtracking to do while waiting to learn if you'll be back. It's always a good idea to “document what you document” so that your clients know the status of each project and where to find it. The easiest way to document what you do is to build it right into your documentation using author notes, conditional text, FrameMaker markers, or help topics that reside outside of the build directory. These notes will likely help you more often than your client, especially when you return to a project after several months or years of being away from it.

Another alternative is to create a production manual for each project. Often, you can demonstrate to your client the value of a production manual and include it as part of your deliverables, thus being paid to document how you do things. A production manual should include everything another person needs to know about how to reproduce the project, other than actually how to “write” it. You might want to include a style guide, too.

If for whatever reason you are incapable of being physically present in your business or of communicating to others what needs to be done in your absence, your client is going to wish there was a backup of *you* on their shelf. I believe that it is a good business practice

to ensure that there *is* a backup of you who is ready to come to your office and, however temporarily, sort through the chaos and ensure that your clients' immediate needs are met.

Your backup partner should be privy to such things as the passwords to your computers; a list of all your software licenses and their serial numbers; physical locations of hardcopy and electronic client files; contact information for each client; and simple instructions about what your backup needs to do to notify your clients of your disaster. These tasks can be performed by a family member or friend. You might choose to prepare written lists and procedures or keep the information in a hand-held device that you sync to someone else's equipment to keep them current.

If your client is truly dependent on your services and cannot function without a trained communications professional with equivalent skills, then you really need to *clone* yourself. This can be accomplished by entering into a cooperative agreement with either a trusted colleague or a staffing agency who can be the keeper of all procedures necessary to keep everything intact until your clients can put more permanent measures in place to pick up your workload. Minimally this should be captured in a letter of agreement that includes a noncompete clause and a clear understanding of what your clone is expected to provide immediately after your incapacitation and for a predefined duration thereafter. You might want to include a fee agreement to ensure that both your client and your backup understand any change in fees or billing structure from what you have been providing.

Regardless of whether it is your client, your backup partner, or your clone who is picking up the pieces of your disaster, everyone will benefit by having immediate access to a file entitled "What to Do if Your Independent Consultant Is Hit by a Bus." In this file, you need to tie everything together at a high level, letting the reader know, step by step, what to do to begin their recovery effort. Call so and so; this person needs to know this; the files are located here; this project is due next week. Let's hope they never have to read this file; but everyone will rest easier knowing that it's there.

Marketing Your Foresight

Your successful back up of your computers and yourself will set you apart from your competitors, and you can use this edge in your marketing. Your potential (and current) clients will clearly see that you make their best interests a priority. Disaster recovery has become a major topic in recent years and everyone's lives, and pocketbooks, have been affected by the measures that companies are taking to ensure they are protected.

I guarantee you that you will be the very first contractor your potential client has met who takes such measures to mitigate their risk. Rather than being afraid you're handing them an easy replacement for yourself if things go sour, you can demonstrate to your clients that this service is only part of the Total Customer Satisfaction package that you are committed to providing them. It will make a difference, I assure you, and they will be more willing to place all of their eggs in your technical communications basket. You will have demonstrated early in your relationship your commitment to their success as a company by making sure your company is never a liability to them.

Finally, make sure that your clients and potential clients know that you have a disaster recovery plan. Tout it on your Web site; describe it in your brochure; discuss it in client interviews; maybe even write a booklet. Set an example that other consultants will want to follow and may be required to follow once this standard of excellence catches on. In an era where customer support is as nebulous as quality service, our profession can stand out from other independent contractors by creating this small ripple in the way we do business. Who knows, it may grow into a tidal wave—the non-disaster kind.