Photographers
Image Storage and Backup Workflow

Chase Jarvis is a well-known worldwide commercial photographer and videographer, who completes hundreds of large photo and video projects per year, at tens of thousands of dollars per job, for multi-national companies. He and his team use a massive, complex and comprehensive backup process, which is excessive for any individual photographer or small company. All information he gives below is scalable to suit any photographers need, from commercial large operations to one person pro, to hobbyist. Below are simple concepts and practices to consider.

Image storage and Backup is an essential part of any photographer's toolkit. We live in a digital photography world, images are no longer usually kept in photo albums and film negative strips. We are therefore reliant on our digital tools to store, find and use images. We need to consider the means of keeping this data safe and available for when and where we need it. In our ongoing desire to inform and assist our membership, we provide this document to stimulate thought, regarding your own storage and backup solution. KPAC

- STORAGE AND BACKUP THEORY:

1. Make your work ORGANIZED. You should be able to easily navigate, save, and locate files in an organized folder structure. For starters, I recommend what's commonly called reverse-date naming, combined with some convenient, recognizable text. For example;

- Let's say I shot images for an Apple campaign today, June 22, 2010, on my labeled #1 Nikon D3s camera, I rename the images: Date_Client_Camera_Setup_Shot Set (location/model detail/environment created). eg: 20100622_Apple_1_Beach_Surfer … or similar and folder them referencing that info as such.

- Make it organized. That goes for files, folders and overall folder structure. Be sure to AVOID folder names like 'new pictures', or 'yesterdays party'. Be as specific as you can.

2. Choose the right STORAGE MEDIUM. Use portable, external hard drives, and perhaps even RAID storage at your home, office or studio to store your work.

- I do not use DVDs or CDs. I find that research incomplete and flawed, even so called archive quality. They are not worth the risk.

- We use hard drives, a lot of them. We use G-Tech. They make great, affordable drives in a range of sizes, from 256G to full enterprise quality multi Tb RAIDs. G-Tech is our choice, but you can feel reasonably comfortable using most any name brand hard drive. As a general rule, if you can afford it, purchase more storage than you think you'll need. Stick to manufacturers who have a long history making hard drives. Discount, knock off's or 'in house brand' hard drives from big box stores carry a risk not worth taking.

3. Keep a CLEAN COPY OF THE ORIGINAL RAW DATA. Before uploading your images into some proprietary viewing software like Lightroom, I recommend copying the original data to a sacred place, in a sound file structure, where it's never altered. I strongly recommend this is a separate drive from your computer's hard drive, and separate from your daily system backup. This also needs to be stored somewhere safe, but I will talk about that in a minute.

You can upload from your camera card again, and copy images onto your computer's hard drive, or into your preferred viewing or editing software for manipulation, client output or reference ONLY AFTER you have a clean unaltered copy saved, and somewhere safe. This means if something happens to your computer hard drive, you will always have the RAW files. As well, a client 2 years later might call and ask for that shot from a previous job, but with a different post process, in which case you will need that unaltered RAW file. RAW files are the lifeblood, not processed files. As well, as software improves over the years, you may want or need to reopen and reprocess images with a particular software upgrade. If you start with your unaltered RAW file, you will not need to consider any existing sidecar files, in essence, you can start fresh.

4. Make it REDUNDANT. In order for your backup protocol to be effective, it's absolutely crucial that your files be in at least two different locations as soon after creating the images as possible. Creating two copies of the original data is the most important step in backing up data. However unlikely, hard drives and memory cards do FAIL. Don't subject yourself to having only one copy of your precious photos or videos. It's not worth it.

5. Keep them SEPARATE. Remember why you keep originals of your will in the bank's safe-deposit box and copies at home? This is a similar concept. Now that you've got two separate copies, on separate drives, with the exact same data on them, do your best to keep them separated. Try keeping one at home and one at the office, or maybe one at your house/office and one at your moms. This is the most far-reaching component of the backup protocol and protects you from the more extreme events like theft or fire. Statistically, it's unlikely that this will happen, however it's the best way to truly protect yourself from catastrophic loss.

6. Use DILIGENCE. A backup strategy is only effective if you can maintain it. Even if you're not a pro photographer, keeping extra copies of your files according to a well-organized, established protocol will help keep your precious files safe for a long time. Be sure to actually do your daily or weekly backup, or however you have it set up. A backup system is only as good as the diligence that is put into it.

- SOME STORAGE AND BACKUP SPECIFICS:

'ON LOCATION' SITE PORTION OF THE SOLUTION: At our location shoots, the camera card is instantly loaded via a laptop to 2 separate, small daisy chained 256G hard drives. That's actually at the beach, up the mountain or at a studio. More or larger drives are used in the case of video, but they are always twinned so there are two copies of every RAW image or second of raw video. The camera card is not yet deleted or reformatted, in case the briefcase falls into a Norwegian crevasse, or hijacked on the subway. Redundancy begins immediately. If the location is within range of the home office, the hard drives are taken home and copied to the server (detailed below). These drives and the camera cards are not transported together in the same bag.

If the location is further away, the hotel is set up as a remote office, and the data is transferred to two 2TB drives, which are stored overnight in two different rooms. Once it's confirmed that the data is good on these drives, the camera cards and small drives can be cleaned for the next day. After the shoot, these 2TB hard drives are returned to the home office and loaded onto the server. If possible the drives take different flights, and we have actually courier shipped a third drive home on critical shoots when separate flights cannot be arraigned.

HOME OFFICE STUDIO PORTION OF THE SOLUTION: This is where the size of our company will seem out of line with your operation, but read this info and adapt it for your needs, if it works for you.

Our studio runs a network of many computers linked together at a hub which speaks directly to a central file serving computer. This "server" can be any computer really, in our case it's 2 Apple X Server. The server's job is to retrieve files for the rest of the computers or work stations, on the network. This server's external hard drive is the focus of this section. In your case, this might be just a single drive, or a small RAID solution.

In our case, we upload all our data onto G-Speed FC-XL Raids by G-Tech. This is a giant hard drive (64TB) that has written data seamlessly over a number of different drives in an array. This is fancy terminology that basically means that the drives (32 x 2TB independent external drives) all sync together to act like one drive, but in reality they're separate drives arranged in such a way that if one drive fails, the server can identify it and, upon replacing the defunct drive, re-create data that was on the dead drive. It circumvents the horror of all your data living on a single bulk hard drive and failing. By spreading the data over several drives, you're minimizing your risks. If one drive fails, you're covered; and theoretically, multiple separate drives are far less likely to die at the same time. Redundancy is the key. Whether you've got an enterprise quality solution, or even just a two hard drives daisy-chained together, make it redundant.

OFF SITE BACKUP PORTION OF THE SOLUTION: Now, the RAID takes care of any on-site single drive failures. You're backed up at the studio. But what about a fire, earthquake or M16 toting Sasquatch with a hate on for hard drives? What if the studio, 64TB RAID and all, is destroyed? If you are professional or an advanced amateur, you should have at least one copy of your data at a secure location off site. In our case, we use raided G-Speed 8TB drives for all data. We do NOT recommend DVD's or CD's. The data for all jobs gets put directly onto these G-Speeds and gets archived off-site. Thus, we're backed up in case of drive failure AND in case of a catastrophe. Generally speaking, we're betting, as all backup systems do, that our redundancy measures will outperform even the most disastrous situations that occur.

What does this mean to you? Well, you have a backup hard drive at your mom's with the RAW files on it. That's hidden gold, not to be played with or used except to update the backup with more RAW files. This section suggests having another hard drive to back up your 'server', which has your RAW files and working, editing and client output files, as well as business and client contracts and communication files. I recommend running a separate, independent external backup on your 'server' or computer. This would be the backup that all computer techs say, we should all have on our home computer, but few do. This backup is your business, it's your livelihood. The other one at moms is for your images, see the difference? Just like your image backup, the 'business' backup should not be stored in the same place as your computer, but you will need to access it easily so maintaining the backup isn't a pain. Anywhere above flood level, protected from freezing, overheating and should be dry. Think of a neighbour you trust, hard drives can be password protected.

We at the studio have a more elaborate setup, due to many workstations and the volume of work. Let me detail what we do next.

STUDIO "LIVEWORK" BACKUP: Remember all our images exist in their original, unaltered state on the RAIDs and off site. But what about client work, adjusted image drafts, delivered images, post production in progress, invoices, production docs, etc, and all the other data that gets changed or updated on a day to day, "trickle" basis? We call this our LIVE (rhymes with hive) WORK and it's handled in a slightly different manner.

It still lives (in a separate partition) on our RAID, and thus has built-in, on-site redundancy, but to remedy the off-site portion of the equation we use Apple's Time Machine software to write a copy of this portion of our data onto two hard drives that are in rotation, while one is on-site backing up the data every night, the other

is offsite, secure. Then, every 7 days, we swap out the drives. What this accomplishes is important and is based on the same basic principle of redundancy that we use for storing our raw photo data. If the studio gets firebombed, then we still have all our raw, untouched data offsite and also all our LIVEWORK offsite … the most we'd be out in such a catastrophe is 7 days of image editing.

Also, we backup each and every workstation in our studio with its own, separate hard drive using Apple's Time Machine. It writes a backup of your computer every hour for 24 hours and every day until the drive is full. As a rule of thumb, the size of the Time Machine drive should be twice the size of your computer's hard drive. These backups are important if you have a computer hard drive failure OR if you errantly delete a file. Time Machine has a nifty interface where you can go back into various earlier 'snap shots' of your hard drive and find that file you accidentally deleted. Don't rely on this as a strategy for saving data, but in a pinch this can be a life saver.

- THE CONCEPT:

One word – redundancy. Both what we do, and what we have suggested for you, follows a few hard rules, which I will phrase as you might use them, assuming your operation is smaller than ours.

-Your RAW files come from your camera, are renamed and follow a folder structure that ensures you will find any image, and are copied onto 2 external hard drives. Do not delete the camera cards until you have confirmed that the image exists in these two physically separate places. This is the moment redundancy begins.

-One of these is your personal drive with just RAW images, update it as much as you think you should, keeping in mind how much you are willing to lose if your home/office collapses due to asteroid impact. Store this drive somewhere else, take it to moms.

-Now you import your images from the other hard drive to your computer hard drive and work your images, fulfill client needs and generally do what we do, day to day as photographers. At your work station, you have a RAW backup, and your working files on the computer drive.

-Now we need to back up your computer, onto third drive. I know you're thinking "3 drives, you're kidding". Think about it, at work you have a hard drive with your RAW files that you need to access for various jobs, and a computer needing a working backup for day to day operations. If you set up your work station backup as we have, using a product like Apple's Time Machine software, it updates every hour. This means that;
1) It spins a lot. If it also the drive you keep all your files on and work on thru the day, the risk of drive failure is higher.
2) A continuous backup like this doesn't really allow for regular file access, your computer might run slower. A separate drive for office backup means a safer backup and better operation of your computer.

In a one photographer operation, you might think you could use the RAW drive at the office as your once daily backup if you really want to, but remember in the real world, you're probably not going to make it to moms to update that drive as often, which means this drive will likely be spinning with the working backup and fresh job RAW files. The more you use a drive, the more likely a failure could occur. If you delegate a backup drive for this job alone, your RAW drive won't work as hard, and you won't accidently damage or remove RAW files. In addition, anytime you leave the office with a backup hard drive, there is an increased risk of damage or theft. Do you really want your entire RAW catalogue out there on that drive?
A back up file is only unpackable by the software that created it.

This 'server' or working computer backup only drive should be stored off site if you are a professional (ie: take it home from the office, or take it to the office, whatever works), and backup routines should occur regularly. I'm going to suggest daily, but that might not be what you feel you need. Think of it this way;
How much of your daily work can you lose and still operate?
How many days of post work are you willing to redo?
We have a backup occur every night, on two rotating hard drives, with one stored in a bomb shelter for 7 days till it is rotated out. That's with our server operating, so if the backup fails, we can still work. If the server fails, we have last night's backup. If both fail because of a satellite crashes into the office, we lose 7 days of in office 'LIVEWORK', and 2 copies of the original RAW files still out there in storage.

You need to figure out what works for you. If you follow these basic rules, you will always have 2 copies of every piece of work, in two locations, except for work not yet backed up, plus your RAW files at moms.
You are bomb proof.

- THE WRAP UP:

You just read all that, and are thinking "3 drives, backup daily, weekly and a separate RAW backup to keep up with … too much … not gonna do it". I can't blame you. But if you are a professional, your livelihood and continued existence may depend on it. Imagine being hired to do a shoot for a major company that sinks large dollars into you and the location, model talent, art directors etc., or if you are a wedding shooter, and because of a leaky backup system, you lose every image in a drive crash. Not only can you be held liable for the costs of the shoot that you are not responsible for, but you will lose future work. A few hundred dollars now and the time spent to install a backup system into your routine, could be worth large.

If you are a hobbyist or amateur shooter, all of this is obviously way over the top, but consider a minimum of a RAW drive and an updateable backup drive on your computer, which you're supposed to have anyways. Your work is only good … if you still have it.