

Article – Back-ups: A Quick Case Study

February 24, 2006

Concerto Networks of San Diego

Written by: Eric Rockwell

Back-ups: A Quick Case Study

How putting a system in place to protect your company's data can give you peace of mind and prevent possible loss, a detailed account of one client's experience

When it comes to those crucial back-up processes in our small businesses, it is a known fact that some or most of us just do not do it. That is right, most of us overlook the fact and underestimate the importance of regularly, daily backing up, to enable us to retrieve our work, in the event of catastrophic failure, viruses or other unforeseen, unfortunate incidents or occurrences, outside of our own control (or is it?).

From actually doing back-ups, checking it, verifying, testing, monitoring and/or even safely capturing and storing it, safeguarding even encrypting our data, files and records for security and safe storage – although it sounds logical and important, we again find ourselves simply not doing it.

There are also considerations regarding checking if you are in fact successfully backing up, and if so, if it is the same, correct, accurate and appropriate data, we should be dealing with. Most of us do not even stop to think about what it is that we are doing or not doing when it comes to backing up our work, files and data on a regular basis.

We will normally find out also, when it is too late and this can be a hugely expensive and costly oversight, negligent act – even if unintentional for the most part, or left up to someone else, a third party, or even worse just assuming somebody is taking care of it, or not doing it at all.

We want to be able to retrieve, restore, update and not lose any of our data, work or files, but when it comes to the daily discipline to actually follow through, check and verify the accuracy of our content and process – we again **SIMPLY DO NOT DO IT!**

It is critical to any home or business where there are computers and information involved, to regularly back-up, as well as ensure the backup processes and sequences are in fact working. We argue that just backing up is not enough either!

How about a good illustrative example of what we mean here?

Recently, we were contacted by an existing client, who we were providing a peripheral or affiliate Information Technology (IT) service to- remote e-mail and access through a portal. When they called on us, saying that they were running into some difficulty with capacity issues, at risk of losing information, and that the current vendor has been slightly non-responsive, dragging their feet, that the delay and wait for an upgrade was simply taking too long and that they wanted guaranteed results in an expedient fashion, from someone they trusted and knew could get it done quickly, affordably and reliably, they got our full attention.

Some background to the story is also important here. In this case, we are dealing with an 80-user office in the medical and health-care field, where the importance and security of data and personal information is a crucial element of the day-to-day practice. Critical items include the integrity and accuracy of relevant and updated information, critical for successful business operation, billing, treatment, claims and the like. So, imagine what would happen – heaven forbid, if they lost some of this data, access or entries into the database made over a couple of days or weeks, due to a failure in their own back-up processes and systems?

Article – Back-ups: A Quick Case Study

Well you guessed it – this did in fact happen. Here is their story.

When the call came in, our take on this task or project, was basically that it was a very routine maintenance upgrade. After being advised that they were in urgent need of an upgrade, as they were getting close to capacity, their main, only and third-party IT specialty vendor, who was on full-time retainer at the time, had been called, and advised of the situation and the potential risk of losing files, data and input, that they were facing. They were in desperate need of upgrades, fast.

They have been waiting at that point for a couple of days. The process dragged on for a couple of weeks, when they finally called on us again to now just get and install the new equipment as soon as possible. We placed the order, got it approved and processed within a day or two and got ready to install.

During our normal process, we always snap an image of the existing data, and do a back up, just in case and just to be proactive, prudent and safe. Needless to say, the discovery was made at that point, that there were some serious problems and issues here, way past available disk space. The network was not properly configured, it was a difficult situation and environment to work in, extremely messy was one of our technician's comments that stuck. In short, the hard-drive and with it, their database was corrupted.

Now the business was at real risk here and loss of productivity and work, not to mention the data and information in question, seemed imminent. The problem was complex, the crisis real .

A total of 80 employees could no longer access the database. Not only that, to make matters worse, they did not know when the last back up was done. Although an image was captured (they did have a process in place, that at least, was a plus), but the back up was not being done, not properly at least, and it was not being monitored either.

Another complicating issue was the fact that the back-up processes were set up in such a manner, that the system was actually backing up, onto itself. Normally, this would be considered an acceptable practice, for data would be retrieved, as long as the hard drive stayed intact and did not fail. The long and short of this – the vendor who actually was contracted and paid to monitor these and other processes, simply did not do it. At this point in our troubleshooting and discovery, **we found that there were no back-ups for over two weeks!**

The problems continued and worsened. At no point was the customer, ever made aware of the situation and any problems or back-up failures. There were no monitoring activities or notifications, of any sort and no one was really aware that the database information or back-up image was over two weeks old.

This discovery was made as we were getting ready to remove and install the new hard drives to complete the upgrade. As mentioned, we normally take a snap-shot image (back up), to move it to the new hard-drive, as part of our standard process and operating procedure. It is at this point that we found out that the image, files, data and critically important database, had been corrupted.

Upon restoration, it was our back up that was relied upon. This image was not really meant for back-up purposes, just for removal. We quickly discovered however, that our own image was also corrupted. Another problem was subsequently identified. During the imaging process, due to switches not being set up properly, there were now lost pockets of information. The image could not be verified it was corrupt. No recourse, no go. We could not successfully extract the database file. At this point one whole week worth of work was completely lost, gone, forever. For this amount of practitioners and 80 users, it translated into a huge loss and potential risk for the company. They lost in the vicinity of \$40,000 per day, for they had to go back in time, they have lost 7 days, using their new backups, trying to make sense of it all, the fall-out, the aftermath, the crisis, the chaos. They had to start rebuilding, did not have a good back up and no confidence in the retrieved or backed-up information.

Article – Back-ups: A Quick Case Study

Their system was now back online, but they were still facing an uphill battle. The cost of this back-up process not working properly, HUGE! Lessons learned. They thought they were covered, that back-ups were happening and being monitored, they received no reporting, notification or forewarning, **they simply just did not know...**

We backed-up pro-actively, checking and verifying, extracting pieces of data, making sure and not just counting on it to compile, complete or actually do it – we wanted to be sure, not leaving anything up to chance (we still are) and have had no reoccurrences or problems of this nature.

The biggest lesson of all here, is that backing up is good and necessary, but **just backing up is not enough** – this goes for imaging as well. These processes are not on autopilot, when taking an image or back-up and verifying the image every night - do not assume it is taken care of or rely on someone else or processes, to do this for you. Take the extra time and effort to verify, test restores. Ask yourself if your back-ups are done, being done, checked and verified. Test whether you can successfully restore from back ups for example. Taped back up is notoriously unreliable as in up to 50% of the time, a process might have been interrupted by something, back-up switching issues, blank or defective back-up tapes – we all know the pain! With no one checking it, there is no way of knowing. If the tapes are empty, corrupted or gone, you get situations like this one, where one critical database, worth in the vicinity of a quarter of a million dollars – not being back-ed up – they thought they were covered and clearly were not.

Our Solution: we advise clients to create a checklist of what to do on a monthly, weekly and even daily basis. The good news is, these pro-active back-up and monitoring processes are part of our wide range, scope and levels of professional IT services.

- **Basic monitoring**, which enables you to keep your current IT vendor. This service from us is simply just monitoring/reporting. It is an inexpensive monitor exchange – a good solution to have someone check and verify, hard disk size, patches, anti-spam, anti-virus, strategies and of course back-ups. We can send frequent reports on these and even specific directories, files or databases.
- **Monitoring and servicing – not repairing, or just notifying**. We can also step into this role with ease. You could ask yourself if your current IT vendor is doing what he should be doing. We offer third party – tracking, performance, reasons and diagnosis. This pro-active partnering, gives green and warning lights in a timely fashion, which translates into peace of mind from a customer perspective. If and when we do become aware of, or find a (potential) problem, we can alert, fix, repair, the full range and scope of services are available. We can ensure that everything is done.
- **We also confirm, check and verify, monitoring with a checklist**, which is part of our most advanced service niche offering. Most IT vendors, even the one-stop shop, responsible IT professional small businesses rely on, in managing themselves, take these processes for granted and we are accepting it is just happening. They might not have any tools to effectively monitor these processes.

We deal in peace of mind for process and outcome. If an IT issue is critical enough – that alone can trigger contact with the client, engineers on call, and even the call centre. We are aware at all times if a critical (server) hard drive just failed, e-mails, back up, virus and so on, might place your company at risk. We offer timely notification, we can potentially advise you instantly!

Also, remember, like with all technology, even if it is 99% accurate and taken care of, something can still slip – we propose that it should never take 7 days – maybe slipping for a day is acceptable and possible, but no-one can totally rebuild 7 days worth of data, work and input from 80 users from 'memory'. Just imagine 500 patients per day, 10,000 patients in the database... it becomes painful just thinking about it! Protect yourself, your data, your customers, and your business. Get peace of mind with placing your trust in a full-service, comprehensive, pro-active IT provider and partner to optimize your back-up processes and overall strategy, execution and success.

For more information on Concerto Networks and our solutions for your business, visit www.concertonetworks.com today.