Computer Data Recovery

Table of Contents

A Safer Way to Recover Damaged Partitions

Repairing damaged partitions on is a risky business. Even if you use the best toolkit and are absolutely sure in what you are doing, you are still risking your files shall something go wrong. Changes made to the damaged partition are irreversible; it is just too easy to overwrite an important system structure that holds vital information about your disk, files and data. Bottom line: it's good to backup before performing data recovery. But is this really the best way to do it?

There is a different approach to do data recovery that is even safer. No need to backup and restore during the recovery. Instead of making a backup copy of corrupted data, you can simply take a binary snapshot of the partition being repaired, and attempt the recovery with different settings as many times as you need on this snapshot instead of the actual disk.

SoftAmbulance Partition Doctor by http://softambulance.com/ is one of a few data recovery tools that allow recovering a virtual image of a damaged hard drive instead of repairing the hard drive directly. The data recovery tool lets you create a binary image of the damaged hard drive, and works with the binary image instead of the real thing. The binary image is a big file stored on another hard disk, CD, DVD or other media. The technology is similar to making an .iso image of a CD or DVD disc, only SoftAmbulance Partition Doctor extends it to partitions or even entire disks.

The hard drive copy may be virtual, but any data you save from it is for real. SoftAmbulance Partition Doctor can recover your files, documents and other data from the binary image and put it on a healthy media. After that, you can attempt fixing the damaged system structures of the corrupted hard drivewithout taking any risk at all. Any modifications will be performed on the virtual image.

Don't rush the recovery. Don't take the risk of losing or corrupting your data. Create a virtual snapshot of the hard drive being repaired, and work on that snapshot instead of accessing the corrupted hard drive. This procedure keeps your original data safe, and ensures the highest level of safety during the recovery process.

SoftAmbulance Partition Doctor recovers files from damaged and corrupted disks and partitions and fixes damaged hard drives. The disk recovery product supports all 32-bit versions of Windows, and recovers FAT and NTFS formatted hard disks, memory cards, CD and DVD media, and USB flash drives. The evaluation version is available for free at http://softambulance.com/

Can USB Data Recovery Be Recovered?

When you store important information on a USB device, you take the chance of losing that information. Losing data on a USB can be kind of a mystery, but there are companies out there that can help you get that data back. These companies use engineering that can recover your lost data over ninety six percent of the time. These companies can even recover data that has been stored on a damaged USB device. So when you find yourself in a situation where you have lost valuable information you should not assume that this data can not be retrieved.

There are some companies that specialize in repairing damaged USB memory devices. In the process of retrieving your data, companies can also repair your device. Types of the problems they can repair broken solders, loose plugs, and broken internal connections. Some of the devices that they can fix are USB ports, USB sticks, USB drives, USB thumb drive, and Flash memory devices. These companies use a type of recovery called a jump drive recovery. They can recover any files from any type of USB drive or memory stick. Sometimes the chips inside the devices will be damaged, but don't fret; there are some companies that can fix that problem too.

So the conclusion on USB data recovery is that just because information seems to have disappeared, doesn't mean that it is lost forever. There are companies that can find and retrieve lost data on a damaged or removed USB device. In the process of finding data, the problems that caused the data to go missing in the first place will be fixed. This is helpful because it insures that it won't happen again. There are programs out there that can help you retrieve your data by yourself, but the problem might be bigger than you know, so you should always seek professional help. There could be problems inside your device that prevent your device from working properly.

Clean Room Data Recovery - What's Its Significance?

Clean rooms are rooms that have been designed to reduce the level of particulates in the air like dust aand airborne microbes. Clean room construction employs filters extensively. Outside air is filtered to prevent dust entering the room. Filters and processes will be in place inside the room to remove internally generated contaminants during production and working areas are often further filtered locally such as laminar flow bench.

Staff would usually have to enter clean rooms through airlocks and wear protective gear while working inside the rooms.

There are different "classes" of clean rooms, with each class limiting permissible different numbers of particles per cubic meter, as well as the maximum sizes particles. Thus a Class 1 clean room is one where the number of particles should not exceed 1000 particles per cubic meter.

Clean rooms are used extensively in the pharmaceutical, semiconductor manufacturing and biotech industries. Data recovery centres typically use a Class 100 clean room that has an allowance of 100,000 particles per cubic meter (compared to 35 million particles per cubic meter in a normal room).

Why Use Clean Rooms for Data Recovery?

Clean rooms are used for data recovery to prevent dust, electro static discharges and such disturbances. These kinds of precautions become necessary because even microscopic dust particles can damage the image on the drive platters, and make data recovery difficult.

With each generation of disks, data is packed more and more densely on the disk platters. It is thus increasingly important that data recovery be attempted in exceptionally clean rooms.

Drive manufacturers usually specify that their product guarantee will become void if the drive is opened by anybody other than themselves, or their authorized agents. And typically, one of the conditions they impose on authorized agents is that the disks be opened in clean rooms meeting specified standards.

Thus clean rooms are necessary for data recovery on both performance and product warranty considerations.

Clean Room Data Recovery

Disk drives are opened only in clean rooms and kept there until the recovery is complete and the drive is closed. All devices are also protected against electro-static discharge, physical shocks, temperature fluctuations and electrical disturbances.

Staff wear special clothing while working in the rooms and particle density is constantly monitored using particle counters. A typical objective of clean room data recovery centers is to maintain Class 10 conditions during production.

Data storage media are getting packed with data more and more densely with each new generation of drives. It is thus extremely important to attempt data recovery in exceptionally dust free rooms.

These days, clean room data recovery uses Class 100 clean rooms where the number of particles is reduced by some 350 times compared to normally prevailing particle density.

Clean room data recovery centers actually aim to achieve even higher levels of dust free conditions during production operations. Even minute specks of dust on the drive platters can damage the image on the media, and make data recovery even more difficult, if not impossible.

Colocation Hosting

Colocation hosting wherein multiple customers locate network, server and storage gear and interconnects to a volley of telecommunications and various other network service provider thus minimizes the complexity and cost. Have a dedicated hosting right away and enjoy complete freedom.

Data centers should be monitored 24-7. Your systems should be housed in a state-of-the-art data center, with redundant air cooling and filtering systems, designed to operate even in the event of a power failure. Data centers should be located and built to withstand natural disasters, and other emergencies. Don’t you want to safeguard your data centre too. Evaluate your business's power, cooling and security

requirements and design a solution that meets your need and scales to allow you to adapt in the future. Appropriate to businesses both large and small, co-location is a highly flexible, cost-effective and best practice solution to ensuring your business' IT service uptime.

Be one among the world's leading players or excel them with secure and well managed colocation. Colocation pricing queries can be dealt with our online professionals with just a click or a phone call. Have a single rack or a dedicated private suite, your servers and core systems need to be housed in a secure, well managed, and environmentally controlled environment. Sometimes the server is hosted with one and the other provides the Internet connectivity. Here, there are issues with cross-connection fees, which can complicate the matter. The host must be able to provide uninterrupted connectivity without any major hiccups.

Colocation hosting can offer reliable power with clean, uninterruptible power, through a combination of multiple power grids, generators, and best-of-breed maintenance practices. Colocation facilities manage their climate with two kinds of dedicated cooling systems, chillers and CRAC units. Chillers are systems of pipes which circulate chilled water throughout the server rooms. CRAC units (computer room air-conditioning units) are targets air conditioners which never shut off. Servers generate enough heat to overheat a several-thousand square foot room in only a few minutes; by continuously cycling, CRAC units prevent heat buildup in server rooms.

- Single rack to full private suite options
- Fully complemented value-added connectivity and managed service solutions
- Have high bandwidth on-net network connectivity to tier one carrier backbones for Internet access and private network connectivity
- Ensuring maximum security and uptime

Compact Flash Memory and Data Recovery

Flash memory gets its name due to its microchip arrangement in such a way, that its section of memory cells gets erased in a single action or "Flash".

Both NOR and NAND Flash memory were invented by Dr. Fujio Masuoka from Toshiba in 1984.The name 'Flash' was suggested because the erasure process of the memory contents reminds a flash of a camera, and it's name was coined to express how much faster it could be erased "in a flash". Dr. Masuoka presented the invention at the International Electron Devices Meeting (IEDM) held in San Jose, California in 1984 and Intel recognizes the potentiality of the invention and introduced the first commercial NOR type flash chip in 1988, with long erase and write times.

Flash memory is a form of non-volatile memory that can be electrically erased and rewrite, which means that it does not need power to maintain the data stored in the chip. In addition, flash memory offers fast read access times and better shock resistance than hard disks. These characteristics explain the popularity of flash memory for applications such as storage on battery-powered devices.

Flash memory is advance from of EEPROM (Electrically-Erasable Programmable Read-Only Memory) that allows multiple memory locations to be erased or written in one programming operation. Unlike an EPROM (Electrically Programmable Read-Only Memory) an EEPROM can be programmed and erased multiple times electrically. Normal EEPROM only allows one location at a time to be erased or written, meaning that flash can operate at higher effective speeds when the systems using; it read and write to different locations at the same time.

Referring to the type of logic gate used in each storage cell, Flash memory is built in two varieties and named as, NOR flash and NAND flash.

Flash memory stores one bit of information in an array of transistors, called "cells", however recent flash memory devices referred as multi-level cell devices, can store more than 1 bit per cell depending on amount of electrons placed on the Floating Gate of a cell. NOR flash cell looks similar to semiconductor device like transistors, but it has two gates. First one is the control gate (CG) and the second one is a floating gate (FG) that is shield or insulated all around by an oxide layer. Because the FG is secluded by its shield oxide layer, electrons placed on it get trapped and data is stored within. On the other hand NAND Flash uses tunnel injection for writing and tunnel release for erasing.

NOR flash that was developed by Intel in 1988 with unique feature of long erase and write times and its endurance of erase cycles ranges from 10,000 to 100,000 makes it suitable for storage of program code that needs to be infrequently updated, like in digital camera and PDAs. Though, later cards demand moved towards the cheaper NAND flash; NOR-based flash is hitherto the source of all the removable media.

Followed in 1989 Samsung and Toshiba form NAND flash with higher density, lower cost per bit then NOR Flash with faster erase and write times, but it only allows sequence data access, not random like NOR Flash, which makes NAND Flash suitable for mass storage device such as memory cards. SmartMedia was first NAND-based removable media and numerous others are behind like MMC, Secure Digital, xD-Picture Cards and Memory Stick. Flash memory is frequently used to hold control code such as the basic input/output system (BIOS) in a computer. When BIOS needs to be changed (rewritten), the flash memory can be written to in block rather than byte sizes, making it simple to update.

On the other hand, flash memory is not practical to random access memory (RAM) as RAM needs to be addressable at the byte (not the block) level. Thus, it is used more as a hard drive than as a RAM. Because of this particular uniqueness, it is utilized with specifically-designed file systems which extend writes over the media and deal with the long erase times of NOR flash blocks. JFFS was the first file systems, outdated by JFFS2. Then YAFFS was released in 2003, dealing specifically with NAND flash, and JFFS2 was updated to support NAND flash too. Still, in practice most follows old FAT file system for compatibility purposes.

Although it can be read or write a byte at a time in a random access fashion, limitation of flash memory is, it must be erased a "block" at a time. Starting with a freshly erased block, any byte within that block can be programmed. However, once a byte has been programmed, it cannot be changed again until the entire block is erased. In other words, flash memory (specifically NOR flash) offers random-access read and programming operations, but cannot offer random-access rewrite or erase operations.

This effect is partially offset by some chip firmware or file system drivers by counting the writes and dynamically remapping the blocks in order to spread the write operations between the sectors, or by write verification and remapping to spare sectors in case of write failure.

Due to wear and tear on the insulating oxide layer around the charge storage mechanism, all types of flash memory erode after a certain number of erase functions ranging from 100,000 to 1,000,000, but it can be read an unlimited number of times. Flash Card is easily rewritable memory and overwrites without warning with a high probability of data being overwritten and hence lost.

In spite of all these clear advantages, worse may occur due to system failure, battery failure, accidental erasure, re-format, power surges, faulty electronics and corruption caused by hardware breakdown or software malfunctions; as a result your data could be lost and damaged.

Flash Memory Data Recovery is the process of restoring data from primary storage media when it cannot be accessed normally. Flash memory data recovery is a flash memory file recovery service that restores all corrupted and deleted photographs even if a memory card was re-formatted. This can be due to physical damage or logical damage to the storage device. Data even from damage flash memory can be recovered, and more than 90% of lost data can be restored.

Companies Must Be Prepared For Data Storage and Backup Compliance

Companies must account and deal for new legislation governing how information is stored on IT systems.

The EU is shortly to adopt many of the recommendations on corporate governance set out by the Sarbanes-Oxley Act in the US, UK firms are to be expected to deal with and manage explicit guidelines on how to store email and other documents on their IT systems. IT managers should consider the necessary procedures and technologies needed for compliance now, in order ensure technology is able to deal with the new legislation.

Regulations regarding data storage at the moment are fairly lax, but there will be a huge increase in the amount of data than must be held over the next 18 months to two years.

Email archiving, the increased use of expencive write-once read-many media, information lifecycle management and content-aware storage as a few of the technologies which firms should consider for the future, though in some cases companies will simply need to improve the way they manage existing systems.

It is anticipated that new legislations will demand that an organizations' archiving solutions must guarantee that the information they hold has not been changed, and keep it for a specific period of time before automatically deleting it.

A survey of 493 companies in the UK has shown that compliance with regulations has a high or fairly significant impact on the data storage strategies of 87% of the organisations surveyed. Back-up and recovery was also very important to the data protection strategy of 93% of organisations.

78% of organisations future storage strategy is set to include Disk-to-Disk-to-Tape technology. This may be due to the highly affordable and flexible nature of this new technology. For example, recent deployments of disk-to-disk-to-tape (D2D2T) solutions by various companies have, on average, reduced the backup window by more than 70%, from fifteen hours to less than four, yielding significant time and cost savings in tape management.

Interestingly, product features were far more important than the brand of the product, with 82% of organisations making a decision based on product features. When it came to the decision of choosing a specialist storage supplier or a general IT provider for storage solutions there was a very slight preference for specialised storage suppliers (51%) over general IT providers (49%).

This survey shows that compliance with regulations is a key driver in companies' storage security policy and that we are likely to see more companies deploying Disk to Disk to Tape technology in the future.

All the above is fine if you are a corporate, you have an annual IT budget of J500,000 and numerous members of staff who can plan and complete such a system. Is it very easy to talk about SANs, NAS's Virtual Tape Libaries. Organisations of this nature already have a very stable and flexible infrastructure, where it is comparably easier to implement such a system.

What about the 1000's of smaller companies such as solicitors, accountants, medical practices and manufactures etc, which may have only 2 servers on site, but still have the same reliance on data and have to adhere to the same legislations? Backup to tape is an option, however, there is an upfront cost and a requirement for a trusted member of staff to take the tapes off site every night and store in a safe place. Can you guarantee your backup has worked, and do you really trust your long term data on magnetic media? Another option is to archive your data onto optical devices, however the cost is even more prohibitive than tape and you still need to take the disk offsite.

No doubt your data is growing quickly; recently enforced legislations makes sure of this, so why not employ a backup and archival solution which has no upfront cost, is fully automated, secure and regardless of disaster will ensure your data is always available, Offsite Backup.

Computer Data Backups: Test Now or Cry Later

If you're like most small business owners, your computer data backups are one of those things that you rarely pay attention to. Computer data backups are kind of like flossing your teeth and eating low-fat, high-fiber foods... everyone knows what they're supposed to do... but how many REALLY do these things religiously?!?

Unfortunately when it comes to your computer data backups however, complacency can be very dangerous. Of course, it's always a good idea to have a local computer service company that you can rely on for advice on selecting and maintaining your computer data backups. But, unless you're prepared to put a full-time PC support person on your company's payroll, it's really important that you get some basic understanding of the major issues with computer data backups.

So here's a compilation of some really crucial tips on computer data backups that I've put together, after nearly 15 years of helping small businesses protect their valuable computer data files.

Test your computer data backups regularly and monitor their log files.

To be effective, computer data backups must be highly automated to ensure that jobs are launched consistently and correctly, but your computer data backup system also needs to be watched over diligently to make sure it continues to function reliably.

Unfortunately, monitoring the computer data backup system generally isn't a priority until something goes wrong. By then it's too late.... Like the article title says, “Test Now or Cry Later!”

People have a strong tendency with a computer data backup system to set it and forget it. Automation clearly has many benefits, but a totally hands-off approach can be very dangerous if no one is overseeing your computer data backup process.

Test and Then Test Again: VERY Important with Computer Data Backup Systems

With any newly installed computer data backup system, don't assume everything works correctly right out of the box. Even more important, don't take for granted that your backup system will continue working indefinitely. You need periodically to restore some folders and files from your backup media to validate that your computer data backup system still works.

If your automated computer data backup routine is configured to include a verify run with each backup job, testing a sample restore job monthly should be adequate. However, if you have an extremely low tolerance for risk, you may want to simulate a sample restore job once a week.

The Hazard of Moving Parts and Open Design with Computer Backup Systems

Why do you need to take these precautions if you're purchasing a reliable, business-class computer data backup system to start with? Typically, a tape drive or other backup device is one of the few components in a PC or server that still have moving parts.

As a result, it's more prone to mechanical failure. In addition, because a backup device generally is open, as opposed to the sealed design of a hard drive, it's easy for the inside of the computer data backup system device to attract a significant dust buildup in a relatively short period of time.

Sample Restore Jobs and Cleaning Tape Heads of Computer Data Backup Systems

Testing a tape for a sample restore job is also a great time to clean the heads of the backup drive if your backup system requires this kind of maintenance.

Restoring a few hundred megabytes (MB) of data to a scratch directory and running a head-cleaning tape should take no more than 15 to 30 minutes.

When running a test restore job, always restore the data to an alternate server folder path, so as not to disrupt the use of any shared folders.

Building a Computer System Backup and Restore Procedure Checklist

In times of crisis, the most crucial issue becomes how quickly you can get the data back onto your system, undamaged. So, as you build your computer data backup system, be sure to document your test procedures into handy checklists.

This documentation also can be great for cross-training and crucial for avoiding panic during an emergency. Be sure you have a hard copy of this documentation next to your system and stored off-site with your backup media.

Watching the Log Files of Your Computer Data Backup System

In addition to running test restore jobs, you must inspect your computer data backup system log files daily. When the backup system is first installed, take time to get familiar with the way log files look when everything is working. This way, if something goes awry, you'll be better prepared to pinpoint the nature of the problem immediately.

As network operating system (NOS) suites and backup software have become more sophisticated, it's now possible to monitor backup system log files remotely and more proactively. In most cases, the backup system log files are just plain text (.txt) files.

Many third-party tools and utilities, as well as those included with Microsoft BackOffice Small Business Server (SBS) and Microsoft BackOffice Server, can automatically e-mail or fax a backup system log file at a preconfigured time.

Automatically and Remotely Monitoring Tape Backup Log Files

Many computer consultants have their small business clients' log files automatically e-mailed to them daily, so the consultants proactively can watch out for potential problems with the computer data backup system.

However, don't think this proactive monitoring is limited to professional consultants. If your company has one or more branch offices you support from a centralized location, you also can use a similar method to monitor backup system health in remote locations.

For greater flexibility, you can set up an e-mail alias so the computer data backup system log file automatically is sent to you, your second-in-command and perhaps an external computer consultant - so you are all kept in the loop. Also, this way, monitoring continues even when you're out of the office or on vacation.

The Bottom Line

If your small business depends greatly on its computer systems, backing up your data is not optional... and it is not something that can be casually brushed to the back burner.

Use the computer data backup tips in the articles to help you become a more IT-aware small business owner. And remember, when it comes to computer data backups, "Test Now or Cry Later". The choice is yours.

Computer Hard Drive Recovery – Should We Have An External Back Up?

Technology has certainly come a long way in the past few decades. Gone are the huge contraptions that used to characterize computers. Nowadays, you can easily purchase a notebook computer that weighs in at less than 6 pounds. However, one thing hasn’t changed. Hard drives still occasionally crash and frustrated users are left trying to figure out just how to do hard drive data recovery on their own.

Hard drives aren’t perfect, although they’re amazing examples of mechanical engineering. Physical damage can easily occur since these disks are spinning at such high speeds. The smallest interference while in use can cause damage in certain areas. Various features have been put into place to reduce the likelihood of a critical hard drive failure, but these are not 100% effective. Sadly, physical damage isn't the only reason why you may need to attempt hard drive data recovery. Many people accidentally wipe out their hard drives because they're not sure what they're doing.

If you do know a good deal about computers, and are not the one who messed up the hard drive in the first place, it may be possible for you to do your own hard drive data recovery. Keep in mind that to do this, you may need to fix your master boot record, or retrieve data from a physically damaged disk. If you can't do this, then you'll need to employ the services of a hard drive data recovery expert. Actually, if your system crashes and you don't actually recover data for a living, I'd suggest you go straight to a hard drive data recovery expert. One thing though…they're expensive. Come on, these guys are specialized in what they do. You didn't really expect that any hard drive data recovery expert would do it for free, did you?

You know what can really help you save money if your hard drive does crash? Backing up your data. It seems like such a sensible thing to do, doesn't it? Some users partition their hard drive. This makes it easy for you to do your hard drive data recovery because chances are only one partition will fail. If you've backed up your files, you can continue working or, better yet, you can save them to an external source and get a new hard drive. You should definitely invest in an external back up. Yes, it's an inconvenience to remember to back up important files, but at least you won't have to pay for a hard drive data recovery expert.

Consequences of Data Loss and Why Should Offsite Backup Be Used

There is a calculated trend in all business corporations and firms: when the enterprise is getting bigger, its support of data increases its complexity, volume and value. The larger your enterprise is, the more significant your data files become. The traditional tape backup can no longer produce in-depth data information about all the important features of your business. That's why many people get acknowledged to a more adequate file protection. A secure offsite backup system can be the possible solution. Business owners and offices managers have got it straight: if the business is to flourish, precise data information storage should be used.

Offsite backup systems offer something, which no other data store can do: they protect to the greatest extent all your files. But why should they do that, you may ask. Imagine you are a business owner. You have your own office computer, which is crammed up with all the valuable info. Well, what if the computer gets stolen, or a short-cut puts it out of practice? What will happen to your enterprise? If you are still

not convinced enough to the rational extent, let’s consider the following statistic data. 1 in every 4 computer users suffers a critical data loss every year. Last years over 500,000 were stolen. Disk and other hardware failures are so numerous that major disk and computer manufacturers/resellers are reducing their warranties to 12 months. Over 25% of data loss is a result of computer program errors, software viruses and natural disasters (factors completely out of your control). 50% of businesses that lose their data never open their doors again. Of those businesses that do manage to stay open, 90% end up failing within two years. Data loss will cost business an estimated J12 Billion this year.

Still not believing? Consider the following fact: computer experts say that once data is lost, it can no longer be recovered to the full. Some data that contains pieces of valuable information will be forever lost in the digital space, with no hope of getting it back. Disaster recovery planning (DV) often fails to extract the lost files in the similar way as they were before the disaster struck. This happens because of the various regulations and compliance, which occur during the recovery process.

Data loss can happen to anyone, no matter how good the tape protection system is. There is no tape backup that can comprise all the valuable information without omitting some precious stuff. Text documents, financial records, contact records, address books, email messages and databases that you have created on your computer or servers may disappear forever unless you take a serious action to prevent it. The lost files are hard to recover, and it takes a lot of precious time and nerve-racking to recover even to the approximate extent the ruined system as it was before the disaster. The value of data highly exceed the mere cost of your computer or server, as you have to pay a great amount of money for reproducing the whole information as it was before the crack down. So, the most reasonable thing to do, if you don’t want to spend a lot of money afterwards, is to re-ensure your system using secure online backups.

Even though that is the sacred truth, most people avoid taking backup precautions. They leave their data files unprotected, and thus expose their business on the danger of bankrupt. Why do people do it? Because of laziness, because they don’t want to spend additional money, or just because they think that would never happen to them. Is it so hard to take some pre-consideration and backup your data? Sooner or later, everyone gets a strike in their unprotected file systems. Then it is too late to split hairs over the lost information. You should better take the action in advance and construct a data backup system, so that your files are fully protected and your business is ensured.

Data Backup - Do you have a backup and data recovery plan in place

Data backup is rarely a part of a home computer user's or business IT administrator's plans, we all say it will never happen to me or my company, but in reality we are just mentally preparing for the time we lose our data. Its like trying to stop smoking, we all know we should do it but will find every excuse not to. So be honest with yourself and ask yourself the question, do you have a backup plan for your data, or more importantly, do you have a restore plan which will protect your business should something go wrong? All business leaders and owners will now tell you that computers are way past being a useful part of our lives, but now they are an absolute necessity. We acknowledge the data which resides on our computer infrastructure is the most important asset of any organization. I ask again, what would happen if you lost your data and what are you doing to protect it?

The reasons for data loss are endless, human intervention, hardware failure, software failure, natural disaster, loss, theft, we can go on, but we can be sure of one thing, as time goes by the list will get longer and longer.

Ever had anything stolen or lost anything before?

I have been in the IT industry for some 25 years now, and as you can imagine, I have heard some bizarre stories of how computers and servers have been stolen. Laptops stolen from back seats of cars (data lost), a colleague forgot he left his laptop on the roof of his car; problem is he realized when he was 160 miles down the road (lost data). My friend's office was broken in twice in two nights, first time resulted in loss of desktop computers and totally trashed alarm system (some data loss), and second night was to take the servers along with the backup device and media! Apparently the heavy stuff was stolen the second night as the thief's had more time due to the alarm not being repaired quickly enough (total data loss and company ceased trading within 8 months). Save yourself money; prevent data loss in the first place by implementing a data backup plan.

Hardware Failure

If you have managed to never lose your laptop or have you whole IT infrastructure stolen then well done, so now let's prepare ourselves for hardware failure. There are mainly only three mechanical parts within a laptop, computer or server; 1) hard drive, 2) backup drive 3) CD or DVD. Hard drives do fail and if it has not happen yet it will. Don't get me wrong, if you take a failed drive to an expert, they will probably get most of your data back (phew) but expect to pay in excess of J5000 for the pleasure (not phew). Save yourself money; prevent data loss in the first place by implementing a data backup plan.

Fire or Disaster (natural or not).

I live in the UK, it's a lovely place as we don't have issues with forest fires, earth quakes, and hurricanes etc. so there will never be any large natural disaster which will wipe out the majority of a city. This is what I thought until the Bunsfield oil refinery blew up and flattened everything within a 3 mile radius. There are a million and one reasons and scenarios I can give you illustrating why you should backup your business data. We all know the practice of data backup is nothing more than good common sense. Mission critical or sensitive data you don't want or can not afford to lose should be secured. PROTECT YOUR DATA! If you honestly think you do not need to backup your data because you will never lose it, please stop reading this article now and go and do something less boring.

Let's talk about the various ways of securing your data and other backup services. If you take the following on board you will be able to find the solution which will best suit you or your company.

Backup to CD solution.

To backup your file data to CD is easy, it may be time consuming to do this every night and you will have to be disciplined to put up to an hour aside to carry out this task every night. To backup data to a CD drive is not an automated process and we all know people get busy. Once you have backed your data to CD please always verify that the data is actually on the CD and then take it home with you. There is no point leaving it to be stolen or destroyed by fire along with your hardware.

Please do not us a CD to archive data (safe documents for a long time) as I would not expect this form of media to remain stable for more than 2 years.

Backing up to CD has many limitations but it is certainly better than not backing up your data at all.

RAID – Not backup but will protect your server disks.

All servers should be given every opportunity to stay alive, running a RAID configuration will help prevent data loss due to hard drive failure. If you have 3 drives running in a RAID 5 configuration, your server will tolerate a single drive failure. RAID will not protect you from fire, flood, theft or any other disaster waiting to happen, but does offer business continuity.

This solution doesn't usually protect you from theft as the extra hard drives for RAID storage are usually installed in your computer or in other equipment on site. It usually won't protect you from fire either so this method does have its limitations.

Secure Offsite Data Backup and Recovery via a third party organization.

Offsite Backup or Backing up via the Internet methods are usually associated with larger enterprise companies. In the past the high cost of high speed connectivity has been prohibitive to smaller companies.

This method of data backup is now become totally accepted and is gaining momentum around the globe. The main reason for such grown is because the price of high speed internet connections has greatly reduced, virtually every business and home is connected to the internet via a minimum 2MB pipe as a result it is now possible to backup high volumes of data to a secure offsite data centre.

For me, the best element of an offsite backup solution is not the high encryption security levels in place, the price or the purpose designed replicated infrastructure where your data is stored, but it is the fact that an offsite backup solution is a totally automated process. Set and forget, once you have set the software to backup your data at a certain time of every day you can just forget it and let it get on with its job of protecting your data.

If I controlled your backup process, I would implement all three of the options mentioned. A RAID system for business continuity, offsite backup to securely protect all my business data, and to enable a quick restore, a CD backup of just my mission critical data which will keep my business running.