

8 key reasons to consider off-site, online data backup

In today's information driven organisations, the costs to generate, keep available, manage and recover data are staggering. Many businesses today depend on 100 percent data availability to keep mission-critical functions operating. With the increasingly widespread reliance upon data, the costs of interrupted access to data or data losses could financially compromise an organisation and, in some cases, leave it no room to recover. The price of downtime is just too steep.

Despite the best efforts of IT teams everywhere, downtime occurs. As a result, data protection and business continuity planning have taken on increased visibility in businesses of every size.

With the ever increasing cost and complexity of managing internal storage systems (despite an overall trend of lower hardware prices), the continued growth and importance of corporate data, and a bevy of new regulatory requirements and technological threats, CIOs and CEOs are on high alert. This has created a rising sense of anxiety and vulnerability to the risk of data loss.

At the top of this list of fears is the devastating impact of downtime including financial and legal liability, lost revenue, irreparable customer

and investor confidence and lost productivity. As a result, today's CIOs and CEOs share a common goal of finding more reliable, more affordable ways to protect themselves and their company.

Fortunately, with the reach and capacity of today's networks, and advances in storage technologies, companies now have an option for data protection that was inaccessible to them just a few years ago highly efficient remote data backup and recovery using secure off-site facilities.

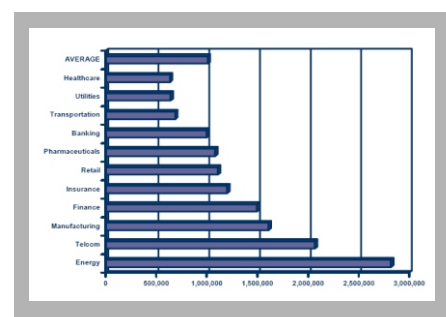
Using their existing networks, companies can now realize the benefits of highly reliable remote backups more cost-effectively than internal tape-based backups. Backups that used to take hours to internal tape systems now take minutes automatically to secure off-site storage facilities from servers, desktops and laptops anywhere across your multiple business offices.

Because the remote backups occur automatically, this approach also removes the human element from traditional data protection which, ironically, is the cause of most data loss. In turn, remote data protection avoids the time delays, human error, expense, and security risk of internal tape-based backup and restores.

To help you better understand the advantages of remote data

protection, we describe a number of reasons to outsource remote data protection.

1. Eliminate Impact of Downtime



According to a Meta Group study, the average downtime cost for businesses across all industries in the US is over \$1 million per hour. What's more, a recent study found that 94% of companies that suffered a catastrophic data loss would not survive beyond two years of business. In fact, 43% would never reopen their doors and 51% would close their doors within two years.

Despite this, it is estimated that only a fraction of businesses are fully prepared for the everyday disasters let alone the catastrophic disasters that can occur to their business or their data. Just a short time ago, spending on business continuity planning was less than five percent of IT budgets and fewer than 25 percent of large enterprises had invested in business continuity planning for e-

business processes. Analysts at the Gartner Group say within two years that figure is expected to rise to more than 60 percent. This sends a clear message to companies of every size of the importance and urgency of business continuity planning.

2. Protect Your Distributed and Mobile Enterprise

As businesses become more and more dispersed, so does their data. With the continual increase in the number of remote offices the complexity of protecting data across multiple locations has increased with little to no IT support or storage/backup experience.

IDC estimates that as much as 60% of corporate data resides unprotected on PC desktops and laptops. And the situation is only going to get worse. The number of workers using mobile devices and applications is predicted to increase significantly over the next few years. Gartner Group has predicted that in the near future 33% of new PCs shipped will be mobile. And, if a laptop is lost or stolen, Computer Security Institute estimates it costs an average of \$16,000 to replace data and proprietary information on these computers.

3. Ensure Regulatory Compliance

New UK and European regulations (Data Protection Act, Freedom of information Act Basel II etc) relating to documentation and corporate compliance have challenged organisations to protect, store, archive and make accessible every

bit and scrap of data that is generated within the business, from the monumental to the mundane.

In essence, every conversation, every email, every document, every process, every transaction and every action a company takes that has a paper trail (and even many that don't) needs to be captured, saved and made accessible.

4. Avert Disasters and Technological Threats

Acts of natural and man-made disaster are increasing pressure on IT organisations to more frequently backup data across multiple locations, increase security, and create contingency plans on a scale previously unthinkable.

However, data loss is more commonly a result of far less dramatic causes than a total disaster. According to a Wall Street Journal report, more than 83 percent of all critical data that is lost is due to some form of human error; 64 percent from mistakes and 19 percent from internal sabotage within an organisation. Losses from these everyday acts of negligence and violence can be just as catastrophic to a business as a natural or man-made disaster.

An additional driver for data protection is from technological threats such as security breaches by hackers. According to iQ Magazine, 150,000 break-ins occur each year. In addition, a CIO and PriceWaterhouseCoopers study cited 29 percent of security breaches in the last 12 months resulted in the compromise or

loss of stored data. The question is how confident are you that your data is really protected from hackers, or 100% recoverable from accidental loss?

5. Limit Reliance on untested Tape Backups

Ironically, with traditional tape-based backup approaches, when most businesses need to restore data from a backup, the odds are not great that they will be able to recover their data. According to Enterprise Research Group, 50% do not believe their data is adequately protected. An IDC survey found similarly discouraging results, where only 13% of users believe that their restores are 100% successful.

However, what's most alarming are actual statistics of failure rates of tape-based restores. An Enterprise Storage Group report cited a 60% failure rate for traditional tape media and backups which demonstrates how infrequently actual restores from tape are tested.

6. Reduce Financial and Legal Exposure

New financial, legal and civil pressures are forcing companies to collect and store information to protect their key executives and the interests of their shareholders. In many cases, corporate executives and officers now have personal, financial and criminal exposure for not properly backing up and protecting company data. Several very visible court proceedings

relating to insider trading, inappropriate accounting practices, health and safety compliance, and employee actions have demonstrated the importance of documentation to separate the innocent from the guilty. Without accessible documentation, legal proceedings can tie up significant amounts of executive and board time accrue large financial costs and put a strain on share value and corporate brand.

7. Better Manage the Data Explosion

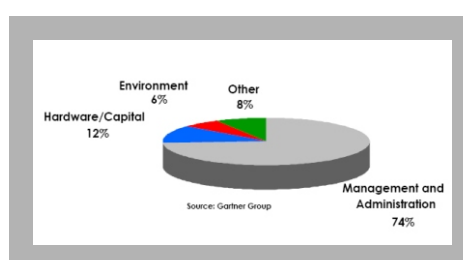
Over the last few years, IT organisations have been under tremendous pressure to deploy and manage increasingly large and complex data protection and storage environments to accommodate the explosion of corporate information.

According IDC, the amount of new storage capacity installed each year is increasing almost 80% annually. With this growth has come an equally dramatic rise in the complexity and cost associated with managing storage environments for this data. Numerous new hardware, software and networking products and standards have emerged in response to this, but still few organisations have managed to solve the problem.

More importantly, Gartner Group estimates that the cost of managing data protection and storage is five to seven times the cost of purchasing the hardware. More specifically, more than 74% of storage costs are for management and administration,

with only 12% going to hardware and capital expenditures. At the same time, the total number of IT workers is increasing approximately 5% per year. With outsourced remote data protection, the traditional costs to provision and manage storage hardware and software for backup and recovery are virtually eliminated.

8. Remote Backups Protect More Data, More Efficiently



For years, many data protection and business continuance plans have relied on internal staff to backup data to tape in-house, then physically transport the tapes off-site to a backup data center. In this scenario, IT managers backed up databases, files, or data sets after business hours and moved copies to remote storage archives via shipment of removable media (e.g., magnetic tape or optical disks). This created extended periods where important data is not protected until the next backup cycle, slowed recovery times (tapes must be physically transported to and from remote sites), increased the risk of damage to tape media that prevents recovering data, and ultimately resulted in inconsistent ability to recover due to uncertainties in the quality of specific backups...where failure rates can approach 60% (Enterprise Storage Group),

For the most critical information in transaction intensive applications, IT managers have had the option of replicating (mirroring) data to disaster recovery sites via very expensive high-speed network links. However, this has been highly expensive, not only for the storage infrastructure, but also the network (often 50% of ongoing costs). As a consequence, companies protected only the most mission-critical applications with this type of solution, leaving the vast majority of data unprotected.

In short, the more decentralised the organisation becomes the less core company data is actually managed in the corporate data center. So if the objective behind business continuance is accessibility to data anywhere and at any time meeting these objectives is all but impossible with traditional approaches.

The Solution:

DSO offers businesses the fastest and most worry-free way to transition to outsourced remote backup and recovery to ISO 27001 security accredited off-site facilities.

Simplified...

d-stor is a fully-managed remote backup and recovery service for mission critical servers and applications. d-stor makes it fast and easy to protect company-wide data from corporate data centers to branch offices with remote data



protection of servers to duplicated, secure, highly available off-site locations.

i-stor protects your organisation's desktop and laptop computers, securely backing up users' data and computer settings via the Internet to secure locations. Users have the ability to restore files and settings in seconds on-line, but the backup policy can be generated, distributed and enforced centrally.



Both d-stor and i-stor use trusted, established infrastructure backup software at their heart, from CA and Symantec (Veritas); software which manages the data backup of many of the largest organisations in the world.

New Levels of Efficiency and Cost-Effectiveness

Using its efficient global single instancing and compression technologies DSO removes the major limitations of network-based data protection: backup performance, network bandwidth requirements, stored data volumes and restore performance. By moving unique chunks of data only once over your existing network connections, DSO dramatically reduces network traffic compared to traditional backup solutions. Backups that used to take hours can now be completed in minutes, requiring only a tiny fraction of the actual data on a server to be copied in order to protect it. As a result, DSO can provide the security

of a full backup every day and the ability to quickly restore a complete point-in-time copy of your data in one go without managing multiple incremental restores. You can even instantly restore a single file from any point-in-time copy. This helps you dramatically improve the quality and thoroughness of your data backups while significantly reducing time and administrator effort taken to restore.

On-Demand Service

DSO backup services support all of the major applications and operating systems including Windows, Unix, Linux, Novell, Solaris, Exchange, SQL and Oracle. DSO backup solutions include all the hardware, software, installation, provisioning, operational support, and usage based billing to reduce start-up times and eliminate start-up costs. This offers you a fast, cost-efficient and convenient way to increase your data protection level across all your branch offices and other remote locations while leveraging existing network connections.

In short, DSO delivers the confidence of service levels agreements with the advantage of minimal capital investment.

Tailored backup

Each client's backup requirements are different in terms of the number of copies of each file, directory or database, to the length of time information need to be retained and the frequency of backups. DSO backup services are highly granular, allowing the backup to be tailored to

the client's exact data storage requirements.

Backup Efficiency

Both i-stor and d-stor provides "block" level incremental backups. "Block-Level" backups means that only the changes to existing files, databases or email servers need be incrementally backed up, not a new copy of the whole file, whilst still allowing for full point-in-time restores. This, plus compression and "global single instancing" means that the amount of data transmitted and stored is kept to an absolute minimum. Global single instancing is a technology which identifies duplicated data within the whole of the distributed organisation, only storing one copy whilst allowing all authorised users access to restore it. For example, an internal email is sent to 10 people within the organisation. It has a 1MB attachment which each user saves to their user directory on the file server. The backup requirement is now 10MB, plus the original file from the sender. With Global Single Instancing, only the original file is backed-up, but each of the 11 individuals who have a copy of the file are authorized to restore it.

These measures ensure that the amount of data transmitted and stored is kept to an absolute minimum.

Security

DSO uses advanced technologies to provide the highest levels of security including:

- Strong, industry-tested authentication and access control for application, activity and data, for both administrators and users
- Encryption of data throughout the storage process.
- Data stored within ISO27001 security accredited off-site facilities.
- Eliminating possible impacts from intentional modification or deletion of data
- Infection-prevention
- Limit access to data by assigning different privilege levels to users

Managed Service

Daily reports are provided showing total amount of data stored, files backed up by server and department. Highlighting failed backups and full alerting.

Summary

With the rising costs and risks of downtime combined with the continually growing complexity of managing internal data protection solutions, DSO offers a convenient, reliable and secure off-site solution as part of your business continuity plan. No more wrestling with storage hardware, software and vendors to get the control and peace of mind that your data is safe and available when you need it.

Contact Us:

DSO Limited,
Adamson House,
Towers Business Park,
Wilmslow Road,
Didsbury, M20 2YY

Tel: 08700 621200
www.dsold.com