

ByteVault Remote Backup

Protecting Your Greatest Asset

White Paper presented by:
IRIS Technology LLC
www.irisstechllc.com

Save your work!

The single most valuable asset of most businesses is not the inventory of products or services that they provide, or the process by which they deliver them. It isn't the hardware and machinery that they employ in their efforts. It is not even the building the business is housed in, nor the various holdings of the company. The most valuable asset, by far, of today's businesses – is data. Stored innocuously on multiple computer hard drives scattered throughout the enterprise, this data is the lifeblood coursing through the veins of a business entity. Without it, statistically speaking, these companies are simply dead. A comprehensive remote backup plan can dramatically shorten the downtime associated with data loss, and thereby lengthen the lifespan of most companies. Consider the integral role that computer data plays in the daily workflow of any business. Customer databases, electronic communications and distribution groups, forms, contracts, e-templates, online information stores, and other critical data are the virtual 'tools of the trades' being plied by today's companies. Just as many businesses decentralize their materials warehousing operations in order to maintain a backup supply in the event of unexpected loss or destruction of their primary stockpile, thousands of businesses are now turning to automated remote backup as a means of insuring their critical computer data. Paper copies of most correspondence and historical data are increasingly the exception rather than the rule. The 'paper mill' offices of the past now employ a series of electronic data stores of varying degrees of importance – and many businesses are still grievously exposed to the loss of these electronic resources.

What's the plan?

Processes for smoothing the transition and replacement of key personnel, infrastructure, and other components of a typical businesses workflow can be invaluable in a time of crisis. Items as basic as building evacuation plans, documented Sales and Marketing plans and established processes for replacing key materials and equipment can be used by new and existing employees to further the goals of the company even under extreme conditions. As important as one component in a star-performing division is, in many cases that component can be replaced rather quickly and according to established protocol. If a major piece of equipment ceases to function or a key player on a project team is suddenly out of the picture, contingency plans kick in and the transition process begins. While not always comfortable or even necessarily successful, the fact is that the plan, and at least a process outline, usually exists. Now consider the processes in place for the safekeeping, replacement and transition of computer data at most businesses. Many simply don't have a plan or a process in place to ensure the redundant availability or integrity of their critical business data. They are busy tending to business, working within whatever margin is comfortable or (perhaps more often) that is dictated to them by a typically lean and aggressive business plan. Especially at small-to-medium-sized (SMB) businesses, the concept of critical data loss and the implications of that loss are simply swept aside in many cases, to be dealt with 'later'. The pressures of making the sale, completing the process, or simply staying afloat in a competitive market frequently mean that time isn't allocated to consider and plan for this critical aspect of business insurance. Business continuity planning, for many businesses, appears only as dollars in a bank account - not as a critical data backup strategy.

The cost of Inaction

According to a widely-quoted National Archives and Records Administration article, some 93% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster. 50% of businesses that found themselves without data management for the same time period filed for bankruptcy immediately. It indicates that data backup should be among the primary considerations for small to medium businesses, regardless of cash on hand. While this statistic is shocking, it is echoed in a 'Cost of Downtime Survey' compiled by a leading industry magazine. An impressive 42% of respondents cited 72 hours downtime as the point at which they would consider the survival of their business 'threatened' due to loss of data access. Perhaps more telling is that all other respondents indicated an even shorter timeframe. With the regular release of statistics and findings similar to those above, business owners, insurance firms and risk management agencies continue to study the true costs of business downtime. Many are looking for trends in data loss by SMBs and are examining ways to limit opportunities for data loss in the business sector. The ultimate goal of the ongoing study and suggestions is twofold: to stem the loss of revenues that catastrophic data loss can entail for client organizations, and to establish best practices in data management for each business sector. Best practices for maintaining a backup copy of data usually include automated, secure, remote data backup. Most business insurance companies with clients located in hurricane zones cite data backup as a basic element of commercial hurricane preparedness, and this advice paid huge dividends for those who implemented a solution prior to the concentrated round of storms that struck the southeastern United States in the Fall of 2004. Industry figures show that most data loss occurs in two distinct exposure areas – systems or hardware malfunction, and human error. In fact, some industry estimates have these two areas accounting for 89% of all data loss in the business sector. This indicates that the vast majority of data loss events are not brought on not by external events such as natural disasters, but rather are caused by the very people and systems that create the data in the first place. Remote backup offsets some of this internal liability by storing complete, accurate data sets in a separate - perhaps less volatile - environment. By securely transmitting a copy of the quality data offsite and employing separate hardware, software, and network resources in the storage of that data, normal catastrophic hazards such as fire, flood, and windstorms are also somewhat neutralized.

The bottom line – Who's got *your* back?

Any business that depends on computer data needs to assess their vulnerability from a data-loss perspective. What would your clients' downtime be if they lost their critical electronic data stores? What would the interim manual processes look like? Who is responsible for restoring the data? How?

With the proliferation of high-speed connectivity, network resources at virtually any business are suitable for sending large amounts of data 'over the wire' to an offsite server for storage. Security protocols of the best remote backup software products, including tight encryption and compression of the data, shorten data transfer times and ensure absolute security-in-transit of even your most sensitive and valuable data. Unlike some legacy backup processes, the better remote backup software and services usually provide the ability to receive verification notices that the backup sessions completed successfully, and also include the ability to restore data quickly, without IT staff involvement. When compared to the painful and lengthy manual re-entry of lost data, which can take days (if not weeks or months!) to complete, remote data backup is a relatively low cost way of insuring that your client's data and business can be back online quickly after a catastrophe or other data loss event.



505 Dewey Street South • Eau Claire, WI • 54701
Tel (715) 514-1402 • Fax (715) 514-1463