

February 28, 2007

10 Reasons to Outsource Remote Data Protection

AccountingWEB.com

In today's information-driven organizations, 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 organization 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.

What began as a frenzy following the catastrophe of 9/11, has emerged into a very legitimate and ongoing business concern. Business Continuity has become a central theme in IT organizations, and every executive across the business needs to understand the importance of data protection and the risks of data loss.

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, here is a list of the top 10 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 is over \$1 million per hour. What's more, a recent study found that 94 percent of companies that suffered a catastrophic data loss would not survive beyond two years of business. In fact, 43 percent would never reopen their doors and 51 percent 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 rise of enterprise Remote Business Offices (RBOs), the complexity of protecting data across multiple locations has increased. About 80 percent of U.S. enterprise sites (about 1.5 million) are classified as remote or branch offices, with little to no IT support or storage/backup experience.

IDC estimates that as much as 60 percent 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 by 2006, 33 percent of new PCs shipped will be mobile. And, if a laptop is lost or stolen, Computer Security Institute estimates it costs an average of \$32,000 to replace data and proprietary information on these computers.

3. Ensure Regulatory Compliance

New federal regulations relating to documentation and corporate compliance have challenged organizations 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. Some regulations recommend backup facilities for data and operations 200 miles offsite.

4. Avert Disasters and Technological Threats

Acts of natural and man-made disaster are increasing pressure on IT organizations to more frequently backup data across multiple locations, increase security, and create contingency plans on a scale previously unthinkable. Prior to September 11, 2001, our definition of disaster had a decidedly different definition than it does now. And although planning for every contingency isn't necessary, planning for the magnitude of a 9-11 type of scenario is now common in today's business continuity planning.

However, data loss is more commonly a result of far less dramatic causes than those that caused 9-11. 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 organization. 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 percent 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 percent do not believe their data is adequately protected. An IDC survey found similarly discouraging results, where only 13 percent of users believe that their restores are 100 percent successful.

However, what's most alarming are actual statistics of failure rates of tape-based restores. An Enterprise Storage Group report cited a 60 percent 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 stock value and corporate brand.

7. Better Manage the Data Explosion

Over the last couple years, IT organizations 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 to IDC, the amount of new storage capacity installed each year is increasing almost 80 percent 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 organizations 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 percent of storage costs are for management and administration, with only 12 percent going to hardware and capital expenditures. At the same time, the total number of IT workers is increasing approximately 5 percent per year. With outsourced remote data protection, the traditional costs to provision and manage storage.

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 offsite 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 percent (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 percent 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 decentralized the organization 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.

9. Respond to Market Pressures

Customers are continually increasing their expectation from companies to keep historical activity on transactions, payments, collections, services and other data collected from multiple, geographically dispersed online and offline sources.

Whether you are a financial services company, a pharmacy or a department store, the age of information has not been overlooked by your customers. Today's demanding consumers are setting continually increasing demands on customer service organizations and sales organizations to have immediate access to incredible amounts of historical data to demonstrate how you value their business.

In addition, individual industries and supply chains have set new expectations from vendors and suppliers to have access to shared data for improved customer service. This includes creating matching data files that share financial, customer service and product and warranty information, as well as new communications systems that improve access to the right people.

10. Leverage Outsourcing Strategically

In the late 1990's with Y2K fears looming, many organizations out of necessity turned to outsourcers to complete time-critical projects. As these projects progressed and succeeded, these organizations became more comfortable with outsourcing as a means of augmenting their internal teams in times of overflow. As the U.S. market decline and recession of 2000 and 2001 sank in, this comfort level with outsourcing grew into dependence for many businesses when IT budgets tightened and internal staff were let go. Through these experiences, many businesses realized the efficiency and cost effectiveness of outsourcing, and have since begun looking at more and more ways to outsource non-core IT initiatives to outsourcers. In turn, outsourcing has become viewed as an integral, even strategic, way of making IT organizations more productive and less expensive.

© Copyright 2007 - AccountingWEB.com. All Rights Reserved