Protecting critical business data

Just like major corporations, small and medium enterprises (SME's) are increasingly reliant on the critical data stored on their servers. Limited resources and vulnerability to interruptions put small and midsize businesses at higher risk, and relying on native backup for a small business server can leave gaps in the disaster recovery plan.

While native backup for Windows Small Business Server provides a small measure of protection, periodic tape backup can leave small businesses vulnerable to data and time loss in quantities they cannot afford. The key to getting back on track quickly is a comprehensive disaster recovery plan, including fast access to an up-to-the-minute copy of your data.

Reliance on Data

It doesn't matter if you are a million pound firm or a twenty-person regional service provider, more likely than not you depend on your data for day-to-day operations. Recent events such as terrorist attacks, rolling blackouts, complex viruses and devastating natural disasters remind us how vulnerable our critical electronic data can be. Studies show small and medium enterprises (SME's) aren't doing much to protect themselves from data loss.

Small business management is not typically focused on what might be viewed as 'hypothetical' disaster scenarios. Not only have the risks changed, the culture of doing business has also changed. New factors that increase the impact of lost data include the exponential growth of critical data generated every day, customer expectations that services resume rapidly after a business disruption and the increasing need to access data almost around the clock.

Today's data protection challenges pose substantial risks to companies of all sizes, but they pose the greatest risk to small and midsize businesses. (SME's) often don't have the staff or budget for acceptable disaster recovery and there is often no recovery plan, no recovery site, or the recovery site is not far enough away to protect the primary site in case of a natural disaster. (SME's) typically have their critical data all on one server. If the server goes down, most offices have to get that server running and fully restored right away, or face costly consequences. (SME's) in regulated industries are also subject to the same data availability and data protection requirements as large corporations but without the budgets necessary to meet the requirements. Finally, cash flow disruptions are often fatal for (SME's).

Relying on normal backup medium to cover all of the bases in an emergency or disaster may leave a business vulnerable to potentially crippling gaps in protection. Tape and disk-based backup can only restore data to the point of the last good backup, which was most likely the night before; any data created since the last good backup will be lost. If the most recent backup was incomplete or corrupted, then you're forced to use the next most recent backup and lose even more data. Backup recovery time can also be below a business's recovery time objectives since the data must be restored from the proprietary backup medium to disk before it can be utilised.

Here we provide six tips for a small business approach to protecting critical data. These tips can help defend against crippling downtime and data loss.

1.) People, policies and priorities first

Consider having the right people, policies and procedures in place before turning attention to technology strategy. Designate one individual in the company as the data protection owner who is responsible for getting management buy- in, documenting the processes, investigating the options, and directing testing and training. The data protection owner should form a group to determine what the most critical information to the business is.

This small group should include those individuals whose input will ensure that the most critical business information is protected. In a small business, this may be just the owner or the executive staff. In a midsize business, a manager from each function is probably most appropriate. The data protection owner should identify any relevant regulations that affect the company's data protection priorities. Next, the group should define the critical applications.

Given the limited resources in most small and midsize businesses, initially narrow your focus to the one or two core applications where an inability to access key information can quickly start to cost you money, such as your e-commerce site, customer database or e- mail system. By focusing on protecting just one or two critical applications, your data protection goals will be more attainable.

2.) Get the data out of the building

It is extremely important to get your data out of the building and out of harm's way. The ideal offsite location is distant geographically so it remains unaffected by large-scale disasters, such as flooding or fire. Consider what the most likely threats are to your place of business.

Is it local power failure?
How far away would you need to store the data to be on a different local power supply?
Is it a Buncefield type fire or flooding?
Is it most likely to be server failures?
Think about what could be done for more rapid recovery of the production machine. Think creatively about how you can cost-effectively backup the data remotely.

3.) Calculate the costs of downtime

For your peers to appreciate the gravity of the problem, you may need to estimate the downtime costs for employees, suppliers and customers if they can't access critical information. The following method provides a simple way to estimate the average cost per hour of downtime.

Cost Per Occurrence = (T1 + T2) x (Hr + Lr)

T1 = Time / Length of Downtime.
T2 = Time since the last backup.
Hr = Hourly Rate of Personnel (Calculate by monthly expenditure per department divided by the number of work hours.)
Lr = Lost Revenue per Hour (A good rule is to look at profitability over three months and divide it by the number of work hours.)

Next, define the recovery objectives for your applications. The best way to quantify your objectives is with a Recovery Time and Recovery Point for each application.

The Recovery Time for an application is simply the goal for how quickly you need to have that application's information restored. For example, perhaps 4 hours, 8 hours, or next business day is tolerable for e-mail systems.

The Recovery Point for an application is the goal for how much data you can afford to lose since the last backup. Is it 2 minutes worth, 20 minutes or 2 hours?

Then estimate the costs to achieve these two objectives for each application.

Finally, understand and agree your downtime cost estimates and required Recovery Time and Point goals. Once this is done it's easier for everyone to agree on the data protection strategy and budget. For example, if you can get the business owner or executive team's agreement that the company's downtime costs are approximately £50,000 per year, they are more likely to agree that £25,000 is an appropriate data protection budget.

4.) Think beyond tape

Once you have established how quickly you need to recover key applications, how much data you can afford to lose and your budget, you can select the appropriate technology solution. Like many (SME's), you are likely to discover that traditional backup technology won't be enough for critical applications because of the propensity for failure and the long time to recover your data before you can access it again. For (SME's) whose critical applications run at multiple remote locations, the quality and consistency of on-site tape backup is also an issue.

Few companies of any size have technical experts in every location who can clean and maintain tapes, ensure that they are properly backing up the site data, and execute a recovery when needed. (SME's) face a conundrum: tape backup systems are inexpensive and fairly reliable, but they offer poor Recovery Times for critical applications, and they are usually ineffective for remote locations. Hardware mirroring technology, which uses remote copy technology to provide synchronous mirroring between two sites, offers excellent Recovery Point of data, but it is prohibitively expensive for (SME's) to buy and manage.

Plus, it is less than ideal for backing up remote locations which often have low-bandwidth connections and hardware mirroring requires large dedicated bandwidth between sites. Solutions based on asynchronous software-based replication can achieve the acceptable excellent Recovery Point of data for critical applications without the cost and complexity of the synchronous replication approach. With software-based replication, only the bytes that change are replicated.

When compared with synchronous replication solutions, this approach offers lower load on the production servers, faster updates and the ability to send replication updates across low-bandwidth Internet networks. Software-based replication solutions also provide application and server fail-over for excellent Recovery Time, so your users can continue working within minutes of a failure.

5.) Make it easy for users to restore themselves

Most (SME's) don't have the IT resources to respond to individual requests to restore files. Fortunately, solutions like Microsoft's Windows Storage Server 2003 make it easy for users to restore files themselves. Windows Storage Server 2003 can be configured to take a snapshot of the data on a server twice a day, for example. Should a user delete or make unwanted permanent changes to a document, they can simply select the file from any snapshot by right clicking on the file, selecting "Properties", viewing all the versions of the file and selecting the one they want.

6.) Make sure you really can restore

It's important to make sure you have thought through how to restore your critical applications quickly, either locally or at a different location. Do you have fast access to all of the components you need to recover? What are the specific steps needed to restore a failed server? What would you do if you had to move the company's operations and employees to another location?

REMEMBER!!

Like major corporations, (SME's) are increasingly reliant on the critical data stored on their servers. However, limited resources and vulnerability to interruptions put small and midsize businesses at higher risk. In the past, small and midsize businesses had could only try to cope with this greater level of risk, but no longer.

Plus, relying on native backup for your small business server can put your hard-earned success at risk, and statistics show that a large percentage of small businesses who endure a disaster are not able to reopen. While native backup for Small Business Server provides a small measure of protection, periodic tape backup can leave you vulnerable to massive amounts of lost data and time in a disastrous event. The key to getting back on track quickly is a comprehensive Business Continuity Plan, including fast access to an up-to-the-minute copy of your data.