



Backup and Disaster Recovery

A CRITICAL ELEMENT

OF SMB SUCCESS



ROYATECH

The Technology You Need
To Grow Your Business



Over the past few years, seemingly all

verticals have experienced an increase in major unplanned data outages caused by a variety of catalysts, ranging from computer viruses and power failures to natural disasters and system administration errors. At the same time, small and medium-size businesses (SMBs) are utilizing information technology far more than ever before, with computer systems currently considered a critical component of their business. These trends bare out a need for solutions designed to back up digital information and, subsequently, to limit data loss, as well as to aid in the recovery of data. This White Paper will examine how Backup and Disaster Recovery (BDR) options based on a Managed Services platform fulfill such a need, as well as why they are of particular value to SMBs and how VARs can select the proper solution for their clients.

BDR Solutions, the SMB Enterprise and VARs

Whether it involves email, accounting data, patient or client files, company records or other documentation, major data loss can have a devastating effect on businesses of any size. In *Management Systems For the Information Age* (McGraw-Hill, 2003), authors Maeve Cummings, Stephen Haag and Donald McCubbrey cite a study whose results demonstrate a strong correlation between a significant loss of “computer records” and companies’ ability to survive going forward. Of companies that had experienced an incident of this type, 43% never reopened, and 51% closed within two years. A mere 6% of companies survived over the long term.

Moreover, even losses of lesser magnitude have the potential to cripple businesses, at least partially. In many cases a lack of access to mission-critical data renders it difficult if not impossible, for businesses to properly service customers, placing them at risk of losing market share to the competition. Adherence to regulations surrounding documentation and record-keeping becomes equally problematic.

Given these risks, most large companies spend between 2% and 4% of their IT budget on disaster recovery planning, with BDR solutions comprising a portion of their investment.

However, unlike large businesses, most SMBs can not afford to implement optimal in-house BDR strategies and solutions. Consequently, they remain at an even greater risk than their counterparts of being put out of business because of any major loss of data. A BDR solution delivered in a managed service - and hence, more affordable - format is the most viable antidote to such risk.

Meanwhile, for VARs that service the SMB market, since business owners, controllers and IT administrators are looking for a cost-effective solution that addresses their needs in this area, they gain access to many more new clients who are willing to discuss this. After selling the new clients on this Backup and Disaster Recovery solution, the solution providers can easily begin promoting their additional services. This could start with “remote server care” for the critical servers that are being backed up, and then move into network monitoring and management. Additionally, desktop management and asset tracking becomes a natural offshoot of these services. It’s a step-by-step approach that becomes a natural fit Ñ as long as the solution provider performs each step along the way.

Axis Microsystems, an IT Service Provider to SMBs, has sold 50% of its clients on the concept of Backup and Disaster Recovery; its aim is to have transitioned all customers to a managed BDR platform over the next few years, said Brett Jaffe, the company’s president.

“Managed BDR solutions are not only a great way to introduce managed services to our SMB accounts, but they are a lucrative annuity stream and source of recurring revenue on their own,” Jaffe noted.

Selecting A BDR Solution: Best Practices

While a Backup and Disaster Recovery solution is clearly a critical component of every company’s technology arsenal, Channel Partners must follow a strategic approach to selecting the appropriate product(s) to offer their customers. The following components should be considered:

- A solution that offers limited capabilities, and/or is poorly configured, will defeat the purpose of implementing a BDR solution.
- A viable BDR solution should cover all the computing platforms in the business that it is being utilized.
- The solution should provide protection for all data, whether that data resides on a servers, laptops or desktop computers.
- Off-site and on-site backups should occur at regular intervals to meet individual clients’ needs.
- Backups should occur rapidly and seamlessly to avoid interfering with server performance while the backup process is being executed.



- For best results, off-site backup should be provided at a hardened, secure data center, and that has a high level of physical security in place along with internet and power redundancy.
- Data should be secure on-site as well as off-site by using a high level of encryption. The encryption key should be kept in a secure location either by the end-client themselves, or their respective solution provider.
- The Backup and Disaster Recovery solution should restore server images to dissimilar hardware. This is essential, as it prevents VARs from being limited by the type of new server that will be installed.
- It's important to know the recovery time frame following a server crash or catastrophe. The procedure for rebounding after the latter two disasters must not be complex, but rather comprised of a few simple, straightforward steps.
- The end client should ensure that there are no hidden fees - the cost to maintain and manage the solution on a weekly, monthly, and annual basis - plus any labor expenditures - should be taken into consideration before signing a deal.
- The end clients should take into account the provider's availability. Are they being provided with coverage 24 hours per day, 365 days per year?

Case Study

BACK FROM THE BRINK

A regional, multi-site law firm in the Boston area was in need of a business continuity solution. The firm turned to Axis Microsystems, an IT Service Provider, for assistance.

Because of the firm's organizational structure, several remote sites derive email from a set of servers in the main office. Email is critical in nature, as the firm specializes in real-estate transactions and the timely conveyance of critical closing documents and contracts is a must.

"The firm had several solutions in place to address redundancy, including multiple failover Internet lines at each location," says Brett Jaffe, president, Axis Microsystems. "However, addressing email was a different issue since the firm did not have the budget to deploy and manage a clustered application."

Axis installed RoYaTech's backup disaster and recovery solution to provide the failover necessary in this situation, yielding the benefits of off-site backup and the ability for a quick disaster recovery.

Just three weeks after the solution was installed, a critical RAID controller error caused the firm's server to go down at 3:00 am. The Axis Network Operation Center was able to perform a quick diagnosis of the issue and remotely create a virtual server environment for the mail server in under 10 minutes on the RoYaTech NAS system. At 8:00 a.m., business began as usual; employees were unaware that their critical email systems were running in a virtual environment because of the hardware failure. Axis performed liaison services with the hardware manufacturer to replace the defective controller and, at 6:00 pm that evening, the virtual server was restored onto the new hardware with no downtime for the client and no loss of data.