

Backup and recovery are cornerstones for anyone building a data protection structure. From the earliest days of computing, setting aside a recoverable second copy of essential business data has made the difference between a business' survival and its painful death. This is by no means an anecdotal consideration, and the inconvenience of lost data is the most trivial element of the equation. Studies by the University of Texas and the United States Small Business Administration assert that 93% of companies that sustain a loss of critical data go out of business within two years. No competent IT manager will assume that kind of risk. But, too frequently, businesses don't talk about making a backup copy of critical data until a disaster strikes. At that point, it may well be too late.

The data center cannot be the sole repository of mission-critical and business-critical data. It is vulnerable to threats from within and without. Natural disasters like Hurricane Katrina or man-made catastrophes like the WTC attack make extreme and showy examples. Less showy and more mundane examples include fire or water damage, human I/O errors, and malicious attacks by viruses, worms or other malware. Modernly, off-site backups are less a convenience and more a necessity. In an effort to promote continued education in this consistently vital area, Backup Data Now, LLC a provider of off-site backup and recovery solutions offers 5 worthwhile tips regarding off-site backup and recovery.

#### 1. Plan, plan, plan.

The IT professional has an ethical mandate to safeguard the data with which he is entrusted. It is essential to secure data survivability, and is by no means an off-hand consideration. The kinds of different plans for disaster recovery and business continuity are legion, but in this context, the key planning consideration is a profound understanding of the data being managed. The question to be answered is: What data needs to be protected with off-site backup and recovery tools? You must decide whether it is necessary to protect your operating system, word processing software, spreadsheet makers or similar applications programs. If you no longer have the original CDs, backup will be vital to re-installation. The records you keep should have priority. Records are data objects that have either legal or business consequences should they be lost. These would include databases, with key customer contact and ordering records as well as inventory control materials. Financial software data files, such as essential spreadsheets for accounting and human resources, need that layer of off-site protection. E-mail is a more and more important source of business records, and needs to be kept safe for both legal and operational transactions. Documents, including memorandum, work product text files, and other intellectual property should be kept under the umbrella.

#### 2. Adhere to a schedule.

Your data is only as secure as your last backup. Data important enough to be sent off-site needs to be protected on a predictable, repeatable schedule. When your hard drive crashes and there has been no backup in 4 weeks, that time frame is your window of vulnerability. Backup on a daily basis is commonplace, and is scheduled within a backup window that will not impact the ordinary daily operations

and transactions of the network.

### 3. Off-site storage concerns.

Transmitting data off-site requires a software solution that provides reliable and repeatable performance. Additionally, data that is going beyond your firewall should be encrypted against external inspection. Key databases with sensitive client identity information, billing records, tax records and payroll are favorite targets for network snoopers, identity thieves or greedy information brokers. The stronger the encryption method, the more likely it is that data raiders will give up and seek less cautious prey. The only eyes that should see sensitive company data are its users.

### 4. Vendor Selection.

Selecting an offline backup software vendor can make the difference between an easy deployment and a nightmarish experience. At no time in your infrastructure development should you be more risk-adverse than in purchasing your off-site backup provider. The vendor needs to be experienced, brand-new players are untested, and untested solutions are too great a risk for the data your business survives on. They need to provide sound pre-sales consulting advice and excellent after-sales support. Off-site backup is nothing new, and established vendors can show a history of deployments covering a wide range of infrastructures and backup/recovery strategies.

### 5. Test, test, test.

In an ideal world, there would never be a need to restore data from an off-site backup repository. But in the real world, both accidents and malicious conduct take place. The greatest mistake that disaster recovery planners continue to make is that they do not regularly test their plan. You need to have a comfort level that testifies to the reliability of the restore function in the event of catastrophic data loss. Just like backup, testing the restore function should be done on a regular, scheduled basis. Too many businesses have attempted to restore files only to find them unrecoverable. There is absolutely no replacement for regular testing of the backup and recovery subsystem.

Data is recognized as an important corporate asset that warrants safeguarding. Aside from the direct financial losses that can result from catastrophic data loss, there are indirect effects that range from loss of investor confidence to customer flight to competitors and lost opportunity costs. The drivers for protecting data are many: smooth corporate operations and transactions, compliance with an array of regulations (Federal, state and local), litigation support and much more. Business continuity, however, continues to claim primary share of mind when considering the assembly and deployment of an off-site backup and recovery operation. Businesses are now operating 24/7, depending on data traffic ranging from that original order to fulfillment and after-sale support of the customer. A well-planned, well-tested off-site backup and recovery infrastructure gets you back in business fast. The alternative doesn't bear considering.

Backup Data Now, LLC a leading offsite backup and recovery company, encompasses all the major and minor backup concerns of an organizations backup objectives. Recent contracts and partnerships with Backup Data Now and a broad spectrum of management software providers in the medical, dental and optical industries has paved the way for offsite backup as a trusted and viable way to secure a business's mission and business critical data.

