

Backup and Disaster Recovery Services

How much can you afford to lose?



Genesis Systems Consulting, Inc. provides industry leading solutions for disaster recovery services and planning processes. From policy development to recovery testing Genesis can provide the necessary solutions to assure safe and timely recovery of all your information assets regardless of location. All these capabilities assure you that Genesis can be your Business Continuity Plan (BCP).

BCP's are only for the big guys

A recent study discovered that, of companies experiencing a “major loss” of computer records, 43 percent never reopened, 51 percent closed within two years of the loss, and a mere 6 percent survived over the long-term¹. For small and medium-sized businesses (SMB's) in particular, these statistics suggest the necessity of crafting a Business Continuity Planning (BCP) strategy grounded in a robust data backup and recovery solution.

Unlike enterprises, many smaller companies cannot afford optimal in-house strategies and solutions in service of BCP. These companies are consequently at an elevated risk of being put out of business due to any major loss of data. Loss of data could mean emails lost, accounting data lost, patient or client files lost, company records lost, client legal records or orders lost and so on.

A Business Continuity Plan is the blueprint for how businesses plan to survive everything from local equipment failure to a global disaster. A data-oriented BCP, an indispensable component of business planning regardless of organization

size, poses the following challenges. Smaller businesses generally lack the in-house IT resources to achieve these demanding planning, technical and process requirements. Therefore, many SMB's either neglect to implement any data-oriented business continuity plan or else approach data backup and recovery in a sporadic, rudimentary fashion that fails to conform to the best practices of this process. Additionally, the following risks exist for organizations that do not have a plan in place:

- Non-compliance with Regulatory requirements in your industry. Regulations such as the Healthcare Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) and other laws-state and federal.
- Undervaluing the loss of vital business data, such as customer records.
- The risk of not considering all of the environmental hazards that the business infrastructure is exposed to due to your geographical location.
- Underestimating the time it would take to build the business back if disaster strikes without having any plan in place.
- Understanding return on investment for having a BCP in place.

The Challenges

The following bullet points summarize the technical and operational challenges that all organizations must deal with when determining

the right business continuity plans. We feel that our solutions alleviate these challenges.

Technical Challenges:

- Identify the lowest-cost, highest-performance data backup medium (tape or disk) based solution and keeping abreast with the latest and greatest in the industry.
- Ensure that all backed-up data is encrypted and otherwise safeguarded from theft.
- Ensure that backed-up data can be restored to different kinds of hardware.
- Ensure that data backup continues even during active recovery phases.

Operational Challenges:

- Identifying what data to back up.
- Identifying how frequently to back up, related backup and recovery costs and return on investments.
- Retain the ability to recover not only the most recent data, but also data from older time horizons, such as past quarters and years.
- Retain the ability to monitor and manage the integrity of ongoing data backup processes so that backup failures can be diagnosed and remedied before adversely impacting the BCP lifecycle.
- The need to hire staff who understands, can design, implement and keep a BCP running 24/7, and be available to get business back in action after disaster strikes.

But I already have backup tapes

Implementing a data-oriented BCP strategy first requires designation of a specific data storage medium. Magnetic tape and disks are the two leading media for data backup storage. While magnetic tape is currently dominant, analyst Dave Russell of Gartner believes that “Recovery will move to online disk-based storage in the future. This will cause a major shift in the backup market during the next four to five years.”ⁱⁱ

Smaller companies in particular will benefit from the shift as recent advances in design and manufacturing lower the total cost of disk-based storage in terms of storage per bit. Falling prices, combined with the various performance advantages that storage industry analysts cite, render disk increasingly attractive. Gartner Group highlights the suitability of disk for these organizations by explaining that, “The need for high-performance online recovery of data, combined with the availability of low-cost disk arrays, has influenced enterprises and small and midsize businesses to adopt a disk-based approach for backup and recovery.”ⁱⁱⁱ

Tape, in contrast to disk, is physically delicate and easily compromised by environmental factors such as heat, humidity, and magnetic interference. Moreover, tape cartridges must be replaced frequently (every 6-12 months). Tape’s innate sensitivity contributes to high failure rates, with analysts estimating that anywhere from 42 to 71 percent of tape restores fail. Even when magnetic tape backups are successful, tapes themselves are subject to loss or theft, and may be in the possession of an employee or vendor unable to reach a recovery site. Thus, even when physical backup and restoration processes succeed, tape may not prove to be as timely and appropriate a

medium for data storage as disk. Time is a crucial consideration because each hour of server, application, and network downtime endured until data restoration comes at a high cost, especially to smaller businesses.

Data Privacy and Protection

Data Encryption

Backup images are encrypted using a 256-bit AES encryption technology. Data is encrypted before it leaves your server with an encryption key that only we maintain. The data is then encrypted again for its transit over the Internet. Files are then stored, in encrypted form, on multiple servers in high security facilities. Because of the encryption, no personnel at either facility can access your data. Genesis will provide the Company with a copy of the encryption key in addition to maintaining a copy for ourselves. Finally, the backup software communicates with the remote servers using SSL (Secure Socket Layers) technology. As a result, the online backup of data is encrypted twice. It is encrypted at all times using the 256-bit AES encryption, and it is encrypted again while it's being sent over the Internet.

Off-Site Remote Storage

Significant offsite storage is available with each bundled solution, however, additional offsite storage is available by the Gigabyte. Storage is provided at two high availability data centers. One on the East Coast and another in the West Coast. The backup images are stored at a data center on a Storage Area Network (SAN) Server at the primary facility, and then replicated to the same system at the secondary facility.

Connectivity to each center is provided by multiple telecommunication providers with automatic failover capabilities. The facilities provide two fiber optic network drops for the backbone and provide full physical security at each facility including security cameras, key card and biometric access. The network is secured with high-end redundant, automatic failover firewalls. Fire suppression and environmental controls are provided. Additionally, automatic back up power is provided by on site generators. Verification tests are done to point out any data corruption in the images that are backed up and replicated. In the event this occurs, our team will take the steps necessary to fix the corruption or re-image a completely new image should the corruption be irreparable.

ⁱ Cummings, Maeve; Haag, Stephen; and McCubbrey, Donald. 2003. *Management information systems for the information age*. http://highered.mcgraw-hill.com/sites/0072935863/information_center_view0/.

ⁱⁱ Russell, Dave. 2007. *Recovery will move to disk-based, manager of managers approach by 2011*. Gartner Group. <http://www.gartner.com>.

ⁱⁱⁱ Russell, Dave. 2007. *Recovery will move to disk-based, manager of managers approach by 2011*. Gartner Group. <http://www.gartner.com>.