

Bullet-proof Your Data without Breaking the Bank

Highlights of [keepproving.biz](http://www.keepproving.biz) service

- A complete solution that is designed to reduce any server down time with the use of a specialized backup and virtual server appliance.
- Allows near real-time backups and data points - as frequent as every 15 minutes.
- Offers offsite storage at an affordable cost.
- Provides a low-cost, no-headache, speedy disaster recovery process.
- Data is encrypted so it is not accessible to anyone without the passkey, either on the [keepproving.biz](http://www.keepproving.biz) storage server at your site or at the remote storage facility.
- Eliminates the cost and time of managing on-site tape backup. We monitor and manage the entire process.
- All costs - frequent on-site backups, on-site virtual server, remote storage, disaster recovery in the event of disaster and 24x7 management of the entire process - are bundled at a price that is usually significantly lower than the overall cost of buying and managing tape backup.

Executive Summary

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. This white paper evaluates the scope of BCP for smaller companies, by examining their challenges, range of existing solutions and their drawbacks. We’ll also discuss how we have overcome commonly faced challenges to offer the most comprehensive solution in the marketplace.

Business Continuity Planning for Small and Medium Size Businesses

BCP is the blueprint for how businesses plan to survive everything from local equipment failure to large-scale disaster. Data-oriented BCP, an indispensable component of

business planning regardless of organization size, poses a number of challenges. Smaller businesses generally lack the in-house IT resources to achieve the demanding planning, technical and process requirements listed below. Therefore, many SMBs either neglect to implement any data-oriented business continuity plan, or they approach data backup and recovery in a sporadic, rudimentary fashion that fails to conform to the best practices of BCP.

Evaluate the risks of *not* having a plan in place

- Understand Regulatory Compliance requirements in your industry. Regulations such as the Healthcare Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act, the Gramm-Leach-Bliley Act (GLBA) and other state and federal regulations.
- Understand how to mitigate the risk of losing vital business data, such as customer records.
- Be aware of the environmental hazards that the business infrastructure is exposed to due to your geographical location.
- Estimate time it would take to build the business back if disaster strikes without having any BCP in place.
- Understand ROI for having a BCP in place.

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

- Identify what data to back up.
- Identify how frequently to back up, related costs and ROI.
- 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 understand, design, implement and keep a BCP running 24/7 and are available to get your business back in action after disaster strikes.

Traditional Solution vs. Emerging Technology

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 The Gartner Group 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."²

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."³

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.

Analyst Jon Oltsik of Enterprise Strategy Group also points out that tape is seldom encrypted, compounding the destructive impact of tape theft: "Very few people encrypt backup tapes, which means that they rely on the security of the backup and off-site rotation process."⁴ Magnetic tape encryption, unlike disk encryption, has historically been too costly for all but large enterprises: "Encryption of any data that is leaving the security of the data center, in transit, has always been an option, unfortunately, a very expensive option," explains Clipper Group.⁵

Disk offers not only lower cost encryption but other advantages as well. In contrast to tape, "disks are more durable, last longer, withstand more overwriting and you don't need to clean any heads," according to Rinku Tyagi of PCQuest. Additionally, "When it comes to backing up using disks, they are easier to manage. Disk backup systems include management tools, often browser-based, for you to easily configure settings and check status from anywhere."⁶

HP enumerates other advantages of disk storage, noting that “Data is backed up to disk much faster than tape, which translates to less impact on production server availability. Disk is also a more reliable media than tape and less prone to error, which translates to fewer failed recoveries.”⁷ Clipper Group believes that the superior speed of disk storage is an enduring advantage: “High performance disk will always be the choice for online applications that require fast access.”⁸

While disk offers advantages over tape, it is not a panacea. After installing disk technology, companies will still be responsible for monitoring and managing backup processes, encrypting and safeguarding backed up onsite and offsite data, restoring data to new hardware, and other functions. Without implementing a layer of governance over disk-based data backup, these companies court the danger of failed backups and delayed restoration of data, thereby jeopardizing their chances of successful recovery from major data loss.

Smaller companies unable or unwilling to invest in the human expertise and infrastructure support systems necessary for data-oriented BCP can leverage our data backup and recovery solution, which removes cost and complexity burdens from your staff.

A Complete Solution that addresses all of your BCP Needs

keepgoing.biz incorporates industry-leading backup, encryption and virtualization technologies that were previously unavailable or unaffordable for small and medium businesses.

Near Real-Time Backups

Our “Incremental Forever” methodology captures all changes to the initial image in increments of 15 minutes. The “Incremental Forever” technology not only backs up recent datasets but also allows end users to reconstruct the state of their data as it stood at the end of various 15-minute restoration points. This level of forensic and auditable data recovery may satisfy various regulatory requirements (such as HIPAA and GLBA) for data retention and data record reconstruction, and also serves stakeholders such as supply chain planners, warehouse analysts, auditors, and legal counsel.

On-site Virtual Server

If any of your servers fail, our server virtualization technology embedded in the **keepgoing.biz** storage server allows your servers and applications to be restored and rebooted within two hours. While you may sometimes have to endure a wait of several days to receive replacement servers or server components from vendors, your **keepgoing.biz** storage server can have your business up and running within a couple of hours. The **keepgoing.biz** storage

server multitasks so that, even while functioning as a virtual server, it will continue to back up data from your other physical servers as well as from the temporary virtual server instance. Our technology thus allows you to remain in business without any significant loss of data backup, server functionality, or application downtime.

A Complete Image

We generate an image of all hard drive partitions via an agent, which is warehoused on the [keepgoing.biz](http://www.keepgoing.biz) storage server physically located at your location. The data is stored with 256-bit Advanced Encryption Standard (AES) encryption and is compressed, reaching efficiencies as high as 2:1. We employ a block-level, not file-level, backup, which means that data is captured at the level of 1s and 0s. Block level data is raw data which does not have a file structure imposed on it. Database applications such as Microsoft SQL Server and Microsoft Exchange Server transfer data in blocks. Block transfer is the most efficient way to write to disk and is much less prone to errors such as those that result from file-level backups. Additionally, block level backups are not affected by open files or open databases. The block-level image is an exact digital duplicate of the on-site server

Intuitive and Flexible Restoration

A good backup system should allow for quick and flexible restores. Our solution allows for recovery of files, folders, partitions, mailboxes/messages, and databases/tables using a quick and intuitive process. In case of a complete server failure we do support a bare metal restore to new hardware, even if the new hardware has a different configuration, hardware and drivers compared with the failed server. Our 15-minute incremental backups allow a restore to be done from any point in time, allowing for multiple versions of files, folders, messages/mailboxes, database/tables to be restored.

Secure Remote Storage

After imaging the servers to which it is attached, the [keepgoing.biz](http://www.keepgoing.biz) storage server then creates an independent encrypted tunnel and transmits the imaged data to a secure offsite location where it resides in 256-bit AES-encrypted, compressed format. That remote site then replicates again to an alternate data center, creating a total of three copies of the data in three geographically distinct regions. Since the data is encrypted and only you have the key, no one at either of the remote storage facilities has access to your data.

Transmitting data to a remote site is a key component of BCP. It guarantees that, in case of physical damage to the client's network or our on-site storage server, or even regional disaster, the data is safe in uncompromised locations. Encryption is an important step in the process of transmitting data between the [keepgoing.biz](http://www.keepgoing.biz) storage server and the remote sites, because it greatly reduces

the risk of data loss incidents that plague magnetic tape and prevents man-in-the-middle attacks during transmission. We employ the 256-bit AES algorithm because it has never been broken and is currently considered the gold standard of encryption techniques, rendering your transmitted data immune to theft.

Secure, Bandwidth Throttling Transfer

Transmission itself occurs over your Internet connection, and can easily be configured to minimize bandwidth consumption. Our [keeping.biz](http://www.keeping.biz) storage server leverages Adaptive Bandwidth Throttling, which only utilizes unused bandwidth or allows us to set an outbound limit. Our UDP-based smart transfer technology utilizes a host of innovative algorithms to speed up data transport and resume from failure. We can therefore exercise fine control over the data transmission processes.

24x7 Completely Managed Solution

Our 300-person Network Operations Center (NOC) monitors your [keeping.biz](http://www.keeping.biz) storage server and the attached servers 24/7. Failed processes generate immediate alerts to *our technical support staff*, who often remotely correct errors within minutes of receiving notification. In case of more serious on-site issues, we will conduct repairs at your site. If any [keeping.biz](http://www.keeping.biz) storage server is ever irreparably damaged or destroyed, we will overnight ship replacements - pre-loaded with all stored data - directly to your location.

Affordable Cost

We offer simple and straight-forward pricing that is all-inclusive of the complete backup and disaster recovery service - with no hidden costs. This means the [keeping.biz](http://www.keeping.biz) storage server, our “Incremental Forever” methodology, file restorations, file integrity checks, secure data transmission, remote storage, annual reviews with our technical staff, and 24/7 process monitoring are included in one monthly price.

Please contact us to discuss further how [keeping.biz](http://www.keeping.biz) can *keep your business going* by providing highly-effective and very affordable business continuity and data protection.

[keeping.biz](http://www.keeping.biz)

1930 Pendleton Drive

Garland, TX 75041

Telephone: 214-580-1940

www.keeping.biz

References

¹ 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/.

² Russell, Dave. 2007. *Recovery will move to disk-based, manager of managers approach by 2011*. Gartner Group. <http://www.gartner.com>.

³ Russell, Dave. 2007. *Recovery will move to disk-based, manager of managers approach by 2011*. Gartner Group. <http://www.gartner.com>.

⁴ Jon Oltsik, quoted in Shread, Paul. 2005. *Bank's tape loss puts spotlight on backup practices*. Internetnews.com. <http://www.internetnews.com/storage/article.php/3486036>.

⁵ Reine, David. 2007. *Security for small data centers—right-sizing tape encryption*. Clipper Group. <http://www.clipper.com/research/TCG2007036.pdf>.

⁶ Tyagi, Rinku. 2006. *What's for your backup: Disk or tape?* PCQuest. <http://www.pcquest.com/content/technology/2006/106092501.asp>.

⁷ HP. 2007. *HP proLiant dl100 g2 data protection storage server—questions & answers*. <http://h18006.www1.hp.com/products/storageworks/dl100g2dpstorageserver/qa.html#1>.

⁸ Reine, David. 2007. *Security for small data centers—right-sizing tape encryption*. Clipper Group. <http://www.clipper.com/research/TCG2007036.pdf>.