KeyKare™ Protect

Service For Your Data

A key component of your Business Continuity Plan

KSI Keystone Solutions, Inc.

Executive Summary

An organization’s most important asset for success and continuity is **DATA**. Don’t believe it? Unplug your computers for one day or even for an hour or two and see what happens!

Protecting data is an essential duty of any organization’s executive. The technology to bullet proof data restoration and quickly restore operations in the event of any data loss is now available to all organizations using technology previously available only to very large organizations.

There are 5 essential practices to protect data and bullet proof data recovery:

1. Begin with the end in mind – be able to restore operations rapidly.
2. Backup data as close to the time it is created as possible.
3. Store the data locally.
4. Store the data in one or more remote and secure locations.
5. Automate the process and monitor it 24x7 to ensure bullet proof data recovery.

A recent study discovered that, of companies experiencing a “major loss” of computer records (**DATA**),:

- 43% of the companies ***never*** reopened
- 51% of the companies ***closed*** within two years of the loss
- ***only*** 6% of the companies survived over the long-term[1]

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 and range of existing solutions, including their drawbacks. We’ll also discuss how our KeyKare™ Protect Service overcomes 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 global 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 these demanding planning, technical, and process requirements. Therefore, many organizations either neglect to implement any data-oriented BCP or else approach data backup and recovery in a sporadic, rudimentary fashion that fails to conform to the best practices of BCP.

Risks of _not_ having a plan in place:

- Violation of regulatory compliance requirements in your industry or regulations such as the Healthcare Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and other similar laws, both state and federal.
- Loss of vital business data, such as customer records.
- Exposure to environmental hazards that affect the business infrastructure, due to physical and geographical location.
- Under estimation of the time to build the business back if disaster strikes without having any BCP in place.

Technical Challenges:

- Identify the lowest cost, highest performance data backup medium (tape or disk) based solution and keep abreast with the best practices and most reliable technology.
- 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 and related costs and ROI.
- Retain the ability to recover not only the most recent data, but also historical data.
- 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.
- Hire and retain staff that can understand, design, implement and keep a BCP running 24x7 and be available to get 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 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."[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 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 offsite 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]

Like tape, the ever popular removable disk suffers many of the same limitations and deficiencies, including physically delicate and easily compromised by environmental factors, subject to loss or theft and is generally not encrypted. Worse than tape, many are ready to connect and retrieve data without any special software – making a lost removable disk an extremely high security risk!

Disk offers not only lower cost encryption but also other advantages. 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 less 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 local 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.

Our KeyKare™ Protect Service provides a complete solution that addresses the full range of BCP needs.

Near Real-Time Backups:

The "Incremental Forever" methodology employed captures all changes to the initial image in increments of 15 minutes. The Incremental Forever technology not only backs up recent data, but also allows recovery of data to the state 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.

Local Virtual Server:

If any protected server fails, server virtualization technology embedded in the KeyKare™ Protect device allows the failed servers and applications to be restored quickly, often within 1 hour. With traditional tape backup, there is often a wait of several days to receive replacement servers from the manufacturer and restore the server, applications and data. The KeyKare™ Protect Service can have your business up and running rapidly. The KeyKare™ Protect device multitasks so that even while functioning as a virtual server, it can continue to back up data from other protected servers. The technology allows you to remain in business without significant loss of data backup, server functionality, or application downtime.

Benefits of the KeyKare™ Protect Service:

- ✓ Complete solution to reduce server down time.
- ✓ Near real-time backups as frequent as every 15 minutes.
- ✓ Local virtual server for catastrophic failures.
- ✓ Protects Windows Server 2008, 2003 and 2000.
- ✓ Quick and flexible restoration:
    - ✓ Folder
    - ✓ File
    - ✓ Microsoft SQL server databases
    - ✓ Microsoft Exchange databases
    - ✓ Microsoft Exchange mailboxes/messages
    - ✓ Bare metal restore to dissimilar hardware
- ✓ Offsite storage at an affordable cost.
- ✓ Secure local and offsite data:
    - ✓ 256-bit AES encryption
    - ✓ Only you have passkey
    - ✓ Offsite co-locations in Maryland & Denver
- ✓ Secure bandwidth throttling.
- ✓ Eliminates the cost and time of managing tape backup.
- ✓ Automated disk to disk processes eliminate the poor reliability of tape backup.
- ✓ All costs of frequent local backups, local virtual server, offsite storage, disaster recovery in the event of disaster and 24x7 management of the entire process are bundled at a price that is comparable to the overall cost of buying and managing tape backup.

Quick and Flexible Restoration:

A good backup system allows for quick and flexible restores. The KeyKare™ Protect Service allows for recovery of files, folders, partitions, Microsoft Exchange databases/mailboxes/messages, or Microsoft SQL databases using a quick and flexible process. In case of a complete server failure, the KeyKare™ Protect device supports a "bare metal restore" to new hardware which has a different configuration, hardware, and drivers as compared to the failed server. The 15-minute incremental based backup allows restores to be done from a specific point in time, allowing for multiple versions of files, folders, Microsoft Exchange databases/mailboxes/messages, or Microsoft SQL databases to be restored.

A Complete Image:

An image of all hard drive partitions on the protected servers is generated via an agent. The image is warehoused on the KeyKare™ Protect device physically located at your location. The data is stored AES-256 bit encrypted and compressed, reaching efficiencies as high as 2:1. Block-level, not file-level, backup is employed, which means that data is captured at the level of 1's and 0's. 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 local server.

Secure Remote Storage:

After imaging the servers to which it is attached, the KeyKare™ Protect device then creates an independent 256-bit encrypted tunnel and transmits the imaged data to a secure offsite location where it resides in an 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 has access at any of the remote storage facilities.

Transmitting data to a remote site is a key component of BCP. It guarantees that, in case of physical damage to your network or KeyKare™ Protect device, or even regional disaster, the data is safe in uncompromised locations. Encryption is an important step in the process of transmitting data between the KeyKare™ Protect device and the remote sites, because it greatly reduces the risk of data loss incidents that plague magnetic tape and removable disks and prevents man-in-the-middle attacks during transmission. The 256-bit Advanced Encryption Standard (AES) algorithm is employed and is currently considered the gold standard of encryption techniques to render 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. The KeyKare™ Protect device leverages Adaptive Bandwidth Throttling, which only utilizes unused bandwidth or provides for a predetermined outbound limit. The smart transfer technology utilizes a host of innovative algorithms to speed up data transport and resume from failure. Fine control can be exercised over the data imaging and transmission processes.

24x7 Completely Managed Solution:

The Network Operations Center (NOC) monitors the KeyKare™ Protect device 24x7. Failed processes generate alerts to *our engineers*, who often remotely correct errors within minutes of receiving notification. In case of more serious KeyKare™ Protect device issues, we will conduct repairs at your site. If any KeyKare™ Protect device is irreparably damaged or destroyed, at an additional cost we will overnight ship replacements – preloaded with all stored data – directly to your location of choice.

Affordable Cost:

We offer a pricing package that is inclusive of the complete backup and disaster recovery service for protected servers – with no hidden costs. All your costs are bundled and include use of the KeyKare™ Protect device, the Incremental Forever Methodology, file restorations, file integrity checks, secure data transmission and remote storage.

For more information, contact:

Keystone Solutions, Inc.
6901 Shawnee Msn Pkwy, Ste 215
Overland Park, KS 66202-4005
913-381-1012
www.ksi-usa.com

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