



White Paper

“Bullet Proof Your Data”

CCS Business Solutions, Inc. **DRS** Solution

A State of the Art Data Backup and Disaster Recovery Solution

CCS Business Solutions, Inc.
4450 Belden Village Street NW
Canton, OH 44718
Toll-free Telephone: 888-456-3406
Local Telephone: 330.493.5600
Fax: 330.493.5611
drs@ccsnet.net
www.ccsnet.net

A State of the Art Data Backup and Disaster Recovery Solution that “bullet proofs” your data

Top 10 Highlights of the Service:

1. **Real-time Replication:** No longer backup once at night, potentially losing a full day’s worth of work if server crashes at 4:00 PM. DRS allows real-time backups written to our backups the moment the change hits disk.
2. **No Tapes:** Never worry about someone stealing your tapes again. Our DRS solution eliminates the cost and time of managing on-site tape backups. We monitor and manage the entire process. You don’t have to remember to pull tapes, securely store them somewhere, purchase initial inventory and then replace after 2-3 years, etc.
3. **24x7 monitoring:** We monitor 24x7 the backup jobs and automatically troubleshoot and fix any failed job (included in price). No more assuming that information on your tapes will restore correctly.
4. **No upfront hardware cost:** Only pay a monthly rental of the DRS appliance to CCS.
5. **Virtualization:** This is a complete solution that is designed to reduce any server down time. If you notify us that your server is down, CCS will virtualize your server on our DRS appliance. If you also elect to utilize CCS’ Net-Assure program, if any or all of your servers crash, a CCS technician will be immediately notified. The CCS technician will then bring up the latest backup of your server virtually on the DRS appliance so you are down only minutes instead of days.
6. **Proof of Concepts:** We will restore files and virtualize your servers (quarterly) in a test environment to always have the system ready in case of a disaster. This way you know your backups are valid instead of assuming something of worth is on your tapes.
7. **Bare-Metal Restores:** If your server crashes and it is at end-of-life, there is no need to put an old server that is the same model back in its place to perform a restore. We can restore to a newer model with our restores unlike any tape solution which requires the same server model back in place.

8. **Offsite encrypted data:** The solution offers offsite storage at an affordable cost. The Data is sent to an XO datacenter data redundancy. We employ the 256-bit Advanced Encryption Standard (AES) algorithm therefore your data is not accessible to anyone without the passkey, which only you have.
9. **Disaster Recovery:** Provides a low cost, speedy disaster recovery process.
10. **No hidden costs:** 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 comparable to 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 SMB’s 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 customer orders, emails, accounting data, patient or client files, company records, client legal records, etc. This white paper evaluates the scope of BCP for SMB’s, by examining their challenges, range of existing solutions and their drawbacks. We’ll also discuss how our solution 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 with everything from local equipment failure to global disaster. Data-oriented BCP, an indispensable component of business planning regardless of organization size, poses the following challenges: SMB’s generally lack the in-house IT resources to achieve these demanding planning, technical and process requirements. Therefore, many SMB’s 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.

Understanding the risks of not having a plan in place:

- Understanding Regulatory Compliance requirements in your industry. Regulations such as the Healthcare Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley and other laws- state and federal.
 - Understanding how to mitigate the risk of losing vital business data, such as customer records.
 - Being aware of the environmental hazards that the business infrastructure is exposed to due to your geographical location.
 - Estimating time it would take to build the business back if disaster strikes without having any BCP in place.
 - Understanding ROI for having a BCP in place.
- **Technical Challenges:**
 - Identify the lowest-cost, highest-performance data backup medium (tape or disk) 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 and 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. This will ensure backup failures can be diagnosed and remedied before adversely impacting the BCP lifecycle.
 - The need to hire staff who can understand, design, implement and keep a BCP running 24/7. The staff will also need to be available to get business back in action after a 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.”ⁱⁱ

SMB's 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. Analysts estimate 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 or they 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."^{iv} 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.^v

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."^{vi}

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."^{vii} 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."^{viii}

While disk offers advantages over tape, it is not a cure all. 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 they jeopardize their chances of successful recovery from major data loss.

SMB's 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. This removes cost and complexity burdens from your staff.

A Complete Solution that addresses all of your BCP Needs

Real-Time Backups: Our "Collapsing Incremental" methodology captures all changes to the initial image. The Collapsing Incremental 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 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. It 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 Network Attached Storage (NAS) allows customer servers and applications to be restored and rebooted in less than 30 minutes in most cases. As you may sometimes endure a wait of several days in order to receive replacement servers from vendors, your NAS can have your business up and running. The NAS multitasks so that, even while functioning as a virtual server, it can continue to back up data from other devices plugged into the NAS. 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 NAS device physically located at your location. The data is stored using AES-256 bit encryption and compressed. We employ a block-level, not file-level, backup, 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 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, 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 which has a different configuration, hardware and drivers as compared to the failed server. Our 15-minute incremental based backup allows restores 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 NAS 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. 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 the client's network or NAS, or even regional disaster, the data is safe in uncompromised locations. Encryption is an important step in the process of transmitting data between the NAS and the remote sites. 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 Advanced Encryption Standard (AES) algorithm because it has never been broken and is currently considered the gold standard of encryption techniques. It renders 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 NAS leverages 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 imaging and transmission processes.

24x7 Completely Managed Solution: Our 1,500-person Network Operations Center (NOC) monitors your NAS units and the attached servers 24/7. Failed processes generate immediate alerts to *our engineers*, who often remotely correct errors within minutes of receiving notification. In case of more serious NAS issues, we will conduct repairs at your site. If any NAS units are irreparably damaged or destroyed, at an additional cost we will ship overnight replacements—pre-loaded with all stored data—directly to your location.



Affordable Cost: We offer a pricing package that is all inclusive of the complete backup and disaster recovery service-with no hidden costs. All your costs are bundled and include the NAS, the Collapsing Incremental Methodology, file restorations, file integrity checks, secure data transmission and remote storage.

For further information, please contact CCS:

CCS Business Solutions, Inc.
4450 Belden Village Street NW
Canton, OH 44718
Toll-free Telephone: 888-456-3406
Local Telephone: 330.493.5600
Fax: 330.493.5611
drs@ccsnet.net
www.ccsnet.net

References

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>.

^{iv} 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>.

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

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

^{vii} HP. 2007. *HP proLiant dl100 g2 data protection storage server—questions & answers*. <http://h18006.www1.hp.com/products/storageworks/dl100g2dpstorage/qa.html#1>.

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