

Backup and Restore Strategies

How to identify the appropriate life insurance for your data

WHITE PAPER



At home, you safeguard against any incident to protect your family, your life, your property – everything that is valuable to you. You buy insurance to have peace of mind. But, what about your data? Data is the most valuable part of your company! Are they safeguarded? You should start thinking about protecting your data to get a tailored insurance which covers your requirements.

Analyzing your data

What are my requirements? At home, you might have insurance for different assets and some are more relevant than others. This also applies for your data. Some of them are business critical, others are accessed rarely. A question you should ask is: Where does my data reside, are they stored locally or are they stored in the Cloud? But the most important questions are: How long can I live without them? How much does it cost me?



Analyzing possible incidents

To find the right insurance for your data, you need to know about threats in your environment. Hardware failures are responsible for data loss and human errors are the second reason. Nowadays, data corruption due to virus and ransomware attacks ranges in the top three reasons for data loss. You should also analyze your area for possible incidents like floods, earthquakes or tornados. But also unforeseen events like fire or water damage.

Cost considerations

After analyzing your data and possible threats, you should look at the cost of possible data insurances. For example, Cloud might offer an affordable entry level price point, but cost increases dependent on capacity and retention time. Tape might be the most cost efficient solution for big data. Consider initial costs, but also perform a TCO analysis long term cost.



Checking your environment

We learned that selecting the right insurance is dependent on data importance and cost. In addition, you should consider your amount of data regardless of the size of your business. Finally, you should take a look at your IT environment. Does your business consist of laptop users or do you utilize servers? Do you operate physical or virtual environments or a mix? Do you have multiple locations or branches?

Choosing the right software

The first step to choosing the right insurance for your data is the selecting the appropriate backup software. According to your needs, you should ask some of the following questions:

- Does this backup software support my entire IT-environment?
(Physical, virtual, servers, desktops, branches, home office users, etc.)
- Does this backup software support multiple backup jobs?
(You can define separate jobs for more important and less important data)
- Can I perform backup copies to a second backup target?
(Have an additional backup copy on another media, removable media is preferred)
- Does this backup software support media rotation?
(With this, SOHOs and small SMBs are able to implement a full disaster protection strategy)
- Does this backup software support backup to the Cloud?
(Cloud is ideal for weekly and monthly backups as a supplement for local backups)

The 3-2-1 backup strategy

Whether your business is in the SMB environment or your company is a large enterprise, you should implement a 3-2-1 backup strategy, which means to create three copies to two different media of your data and store one copy off-site.

Almost all backup applications allow performing a copy job of the backup after the primary backup job is finished. You should plan to utilize two different media: one media for primary backup and another one as a secondary backup target. If one media fails, the other media is still available for recovery tasks. As a primary backup target, disk is the best choice. In addition, another copy should be stored on a removable media to place this copy off-site. This ensures being capable to accomplish a full data recovery in case of a disaster at the business site.

Media rotation

Especially for smaller environments with single server infrastructure, laptop users or single NAS implementations, media rotation is an ideal method to be fully protected against data loss due to a disaster. In this case, a single backup target with removable media, like RDX®, should be implemented. Using multiple media enables you to alternate the media after the backup has finished. Most backup applications allow ejecting the media when backup is complete.

Backup and NAS

Most NAS systems offer a built-in backup application which is able to perform a backup to an external device which is connected via USB3.0. In this case, RDX QuikStor™ is the ideal solution. In conjunction with media rotation, RDX offers full disaster protection with off-site storage capabilities.

If you use a NAS system as a backup device, you should also complete this solution by adding a secondary backup target. Use media like RDX or tape to overcome failures of the primary backup target.



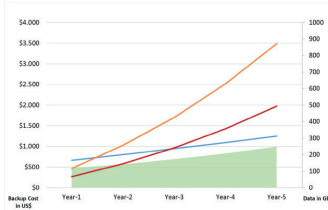
Backup and Cloud

Backup to Cloud is now more popular than ever. SMBs especially are using this option to protect their data in the public Cloud. The advantage is that backups will be stored off-site and will be available even in case of a disaster at the primary location. Users can implement the off-site part of the 3-2-1 backup strategy. But, you should not only rely on Cloud backup alone. If you have a total breakdown, your network might be broken too. In addition, you should take a look at your bandwidth. Is your network strong enough to get your data back?



Furthermore, you should take a look at the cost of a backup to Cloud solution. Many Cloud providers attract with low entry level fees. This might be less expensive as the deployment of a local hardware-based solution.

But if data is growing, the price increases rapidly and you will reach the breakeven point pretty fast. Also accessing data is charged by most Cloud providers. These costs must be included in your TCO calculation as well.



Backup to Cloud is a good solution for keeping data copies off-site. Backup to Cloud protects your data against any event which could happen at your data center. In addition, Cloud protects your data against virus and

ransomware attacks. Cloud should be used for weekly and monthly backups. It can also be used for daily backups as a supplement for local backups. Local backups ensure full restore capabilities even if the network connection to the Cloud has failed. If network bandwidth is a problem, local backups allow fast restores and enable you to be back on business much earlier.

Think about restore, then plan your backup

Before you plan your backup strategy, you should think about the importance of your data. As already mentioned, data should be analyzed according to the importance of your business. You should ask the following questions:

- What is the maximum downtime my business can tolerate?
- What is the maximum amount of data loss my business can tolerate?
- Which data do I need first?
- Which data can be restored afterward?

Local backups ensure fast restores and reduce business downtime. Local backups should be done to disk, like SnapServer® or RDX. In case of RDX, you should label your media to pick the right cartridge in case of a restore. The local backup should also include the system information and applications.

According to the maximum amount of data loss your business can tolerate, you might setup an hourly or bi-hourly backup schedule. At the end of the business day, a copy of the entire backup should be stored on a second media like NEO® tape products or Cloud. The restore of your important data will run much faster as you don't recover the whole company information at once. In this case, your business is up and running much faster and outage cost will be reduced dramatically. Less important data and applications can be restored afterwards.

Business continuity

In many cases, companies cannot afford any downtime. Whether they provide their total IT infrastructure over the private Cloud to their employees and 3rd parties or if they offer online services to their customers, every minute of downtime might cost thousands of dollars. In worst case, these companies won't be able to recover from this downtime.

These companies should think about implementing a business continuity solution by deploying a second disk system at a remote location, either inside or outside their campus. As an ideal solution, SnapServer is recommended. SnapServer features SnapECR (Encrypted Continuous Replication) a replication feature which continuously copies data to the second SnapServer at the remote location. SnapECR is a byte level incremental replication with bandwidth throttling and encryption. This ensures fast data transfers without impacting network bandwidth.

Use cases and recommendations

SOHO and small SMBs

Most SOHO or small SMB environments don't perform backups at all. They are not aware that losing data might result in losing business. Windows and Mac users can benefit from backup applications built in the operating system. Windows Backup and Time Machine offer scheduled backups to removable disk like RDX QuikStor with the capability of media rotation for full disaster protection with off-site storage.



NAS users should utilize the integrated backup app of their systems. Most NAS vendors offer scheduled backups to RDX QuikStor with media rotation.

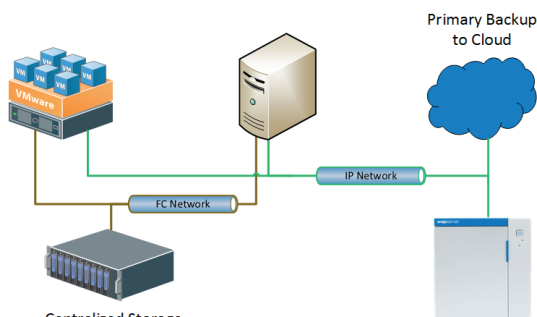
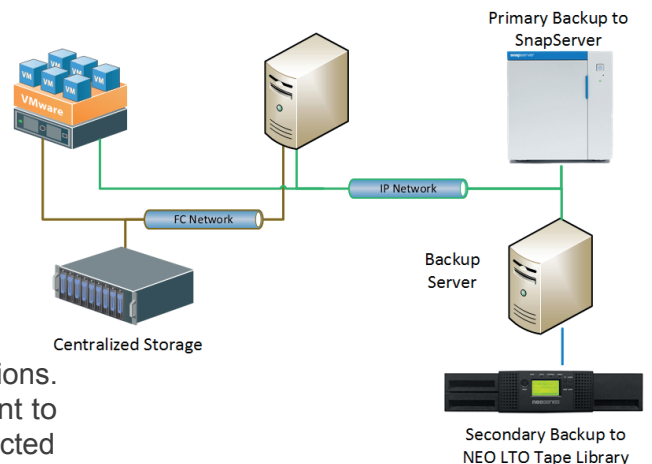
Midrange to large SMBs

Most SMBs only use one backup target which is mainly disk. To implement 3-2-1 backup strategy, they should implement a secondary backup to tape or Cloud. The primary backup to SnapServer ensures fast backups and restores.

A secondary backup to removable media like RDX or NEO tape automation products ensures full disaster protection with off-site storage.

Companies should not rely on backup to Cloud implementations. A supplemental backup to SnapServer or RDX is important to

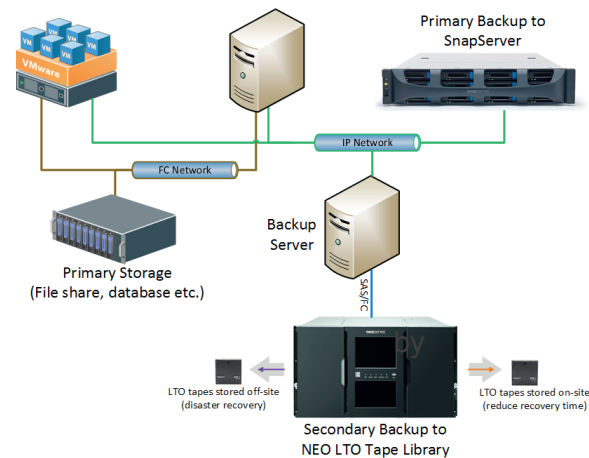
be protected against network breakdowns and slow network bandwidth. Important business data should reside on a local backup device to speed up restore operations and back to business.



RDX QuikStation™ is the ideal device for virtual environments. It provides easy integration with iSCSI connectivity. So VMs can utilize their own RDX device for individual applications. Multiple operational modes allow backup to disk and backup to removable disk/tape in one system.

Enterprises

Also larger companies should think about their data protection environment in terms of restore. What is the maximum business downtime they can afford? They



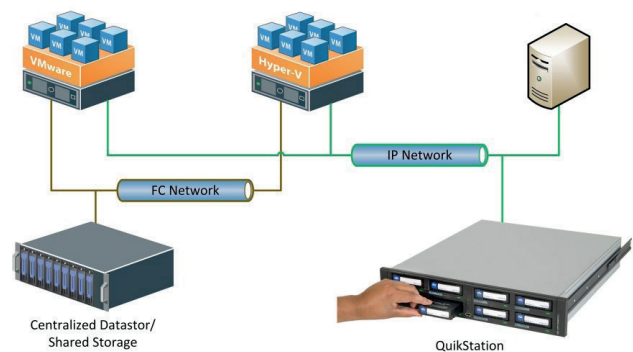
locations and offers data availability in case of a disaster at the primary location.

Conclusion

Business data is the crown jewel of a company. Losing data will result in losing business. Before you start to implement a backup solution, you should analyze your data, your IT and your natural environment. You should consider all incidents which could happen, including human errors, hardware failures, virus and ransomware attacks as well as natural disasters. Get an idea on which data must be recovered first in case of a disaster. This will shorten downtime and bring you back to business much faster.

Implement the 3-2-1 backup strategy to be protected against hardware failures and malware intrusion. If your company is a SOHO or small SMB, use media rotation. Watch cost and availability especially if you have deployed a backup to cloud solution.

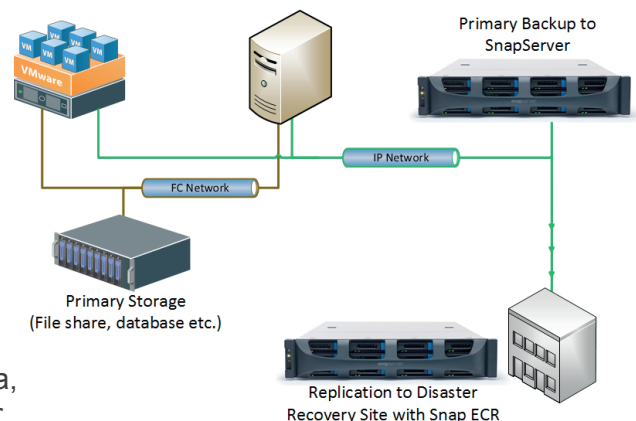
Last, but not least, perform restore tests.



should consider the 3-2-1 backup strategy.

Primary backup to SnapServer ensures fast backups and restores and are available at different capacity points with non-disruptive extension via DynamicRAID functionality. Secondary backup to NEO LTO tape libraries ensures full disaster protection with off-site storage.

Most enterprises have to provide 24/7 data and application availability. In this case, business continuity must be ensured implementing a secondary data center. SnapECR provides continuous replication between remote



Sales and support for Overland-Tandberg products and solutions are available in over 90 countries. Contact us today at sales@overlandstorage.com or sales@tandbergdata.com

©2017 Sphere 3D. All trademarks and registered trademarks are the property of their respective owners. The information contained herein is subject to change without notice and is provided "as is" without warranty of any kind. Sphere 3D shall not be liable for technical or editorial errors or omissions contained herein.

WP_v2_may10_2017