Downtime is real. It’s not a question of if, but when the business will lose data. Moreover, it is very costly. It is not a surprise that 40 percent of all businesses close their doors permanently after a disaster or major data loss. With the increasing growth of data, it is important to have a continuous review of how it is protected and managed in order to improve your capability in recovering from business interruption.

Ensuring your organization can resume operating in case of a disaster, and deploying a solution that incorporates a local and cloud component that provides the recovery assurances are essential to all of the organizations in any scale. X10 Networks can help you to architect the appropriate plan for your business and get the backup and business continuity solutions that you need.

Developing and maintaining a complete Disaster Recovery (DR) strategy for your business is very critical. It needs operational planning and the right technology to get things right and X10 Networks can guide you throughout this entire process, from start to finish.

We strongly believe that the key to having a workable DR strategy begins with defining how much downtime the business will allow for each application on service. The following step would be finding a solution that matches those requirements.

The DR Assessment is a fast and reliable way in assessing your existing environment and capabilities. It also determines the following steps that are required to improve your disaster recovery capability.

Questions for consideration:
- Are you presently meeting your backup service levels?
- When was the last time you tested your backup and DR processes?
- When will you exhaust your existing backup storage capacity?
- Do you have a cloud strategy of your backup data for its long-term retention?

Deliverables:
- Improvement plan that can be executed with no further investment
- Suggested options for the architecture improvement of your data management and backup solution
**BACKUP REQUIREMENT ASSESSMENT AND REVIEW OF CURRENT BACKUP STRATEGY**

- Understanding customer requirements for business continuity from both legal and practical perspectives.
- Gathering information on mission-critical workloads, possible sources of downtime, implemented backup strategies, and restore point and time objectives.

**ASSESSMENT OF EXISTING IMPLEMENTED BACKUP SOLUTIONS**

- Evaluation of existing implemented disaster recovery software and, understanding it’s functionality to the business continuity requirements.
- Providing recommendations according to available budget, required functionality and available market offerings.

**ASSESSING BACKUP INFRASTRUCTURE**

Virtual or Physical machine backup and recovery is an I/O intensive task, meaning production workloads may suffer if the backup infrastructure is under provisioned or misconfigured. Infrastructure bottlenecks may affect backup and restore times as well as disrupt the production.

**ASSESSING BACKUP STORAGE**

Backup storage is an important part of the backup infrastructure and deserves a closer look. Lower end home NAS devices or other general consumer electronics are sometimes used to store business data because of the affordability of such products. Cheap storage, however, may not be reliable under I/O intensive workloads and may lead to backup file and backup metadata corruption.

Restore point objectives and restore time objectives dictate what type of storage is more suitable for a specific disaster recovery scenario. Deduplication appliances, Linear Tape-open devices, Directly Attached Storage, Network Attached Storage, S3 compatible Object Storage may be chosen depending on required RTOs and RPOs.

**BACKUP RESTORABILITY TESTING**

It is crucial to conduct periodical test restores for required workloads as there are many reasons successful backups in some rare cases may still lead to unsuccessful restores: backup file corruption, backup storage malfunction, pre-existing machine file system corruption, malware caused operating system files corruption and in some "unicorn jumping over the rainbow" scenarios backup software bugs.

**OFFSITE AND AIR-GAPPED BACKUP CONFIGURATION**

3-2-1 backup rule is commonly implemented for business critical data, the rule recommends three copies of backup files to be created, where two of the copies are stored on different storage media types, one of the storage media may be air gapped, and one copy is kept offsite.
INSTANT VM RECOVERY

Entire VM restores can take time depending on the restore scenario making the end user wait for the machine to become available. Instant VM recovery allows the VM to be accessed immediately in a matter of seconds running directly from the backup file. This VM can be later migrated to the production during the off hours.

SITE REPLICAATION AND TEST FAILOVER

Workloads can be replicated to a DR site and be available at a stand-by. In case of a disaster recovery scenario the available machines can be failed over to the DR site providing continued availability to the end user, once the production site is restored, changes made to the VMs on the DR can be failed back and the operations can be resumed as normal.

CLOUD BACKUP AND CLOUD REPLICATION

Small businesses may not have access to an offsite location or to an entire DR site, in this case a small fee can be paid to a contract for renting the right amount of storage processing resources to host offsite backups or replicas.

AUTOMATED BACKUP/REPLICA TESTING IN ISOLATED VIRTUAL LABS

Manual backup/replica restorability tests are often overlooked as these tasks can be time consuming for the staff and resource intensive for the live environment. Automating backup restorability testing is the solution that allows IT administrators to focus on other tasks, while allowing automation to perform the actual backup restorability tests during the off hours, when the live environment is not heavily used by the end users.

GRANULAR ITEM RECOVERY TESTING

Restoring an entire VM is a resource intensive task and not often required as most of the time users might only need a single item to be restored whether it’s a file, an email, an Active Directory item or an SQL database. It is important to take into consideration the backup software functionality to avoid staging operations overheads.

BACKUP FOR CLOUD WORKLOADS

Veeam Backup for AWS is a solution developed for protection and disaster recovery tasks for Amazon Elastic Compute Cloud (Amazon EC2) environments.

With Veeam Backup for AWS, you can create image-level backups of EC2 instances and keep them in Amazon Simple Storage Service (Amazon S3) for high availability, cost-effective and long-term storage. In addition to image-level backups, you can protect your data by creating and maintaining a chain of cloud-native snapshots of EC2 instances.

DISASTER RECOVERY ORCHESTRATION

Meet disaster recovery compliance requirements - generate and automatically update documentation for DR procedures to eliminate the problem of outdated DR plans.

Automate DR procedures - create workloads that orchestrate failover and restore operations for Veeam Backup & Replication backups and replicas.

Prove recoverability - build test schedules to automate verification of failover and restore plans, with isolated and low-impact testing of VM backups, replicas and applications they run.