Data is your company's most precious asset in today's tech-driven environment. Whether you're storing customer information, inputting financial data, or accessing proprietary documentation—nearly all business functions flow through digital datasets.

Although your company may take precautionary steps to protect digital assets—your organization may still be at risk.

Loss of data by way of crashes or breaches can wreak havoc on internal systems. Failure to have sufficient protection strategies in place may result in substantial financial losses along with consumer frustration. Creating a viable data backup system is crucial for protecting valuable business interests.

Data backup is the process of creating accessible data copies for use in the event of breach or loss. Surprisingly, 29% of businesses have absolutely no data backup plans currently in place. Creating a data backup strategy can protect your business by helping to recover or restore data that has been lost or corrupted.

Here's the top 5 items that should be addressed when it comes to data backup strategy.

1) Verify Data Backups

Data backups should be routinely scheduled on a regular basis. Whether it be daily, weekly, or monthly—having a consistent schedule helps build continuity and provides peace of mind. The problem is backups sometimes fail resulting in data corruption and incomplete files. Verification measures must be taken to ensure backups have been successfully completed and fully executed.

Companies should be persistent in making sure data backups contain the most up-to-date information. Verifications should be done on a consistent basis within regularly scheduled timeframes. Conducting restore tests after every backup can ensure that all data has been securely copied and validated.

Extra care should be taken when dealing with large software updates or newly installed patches. New versions of software or security updates can cause compatibility issues that result in backup failure. Verifying data backups ensures your company's most up-to-date information is protected in the event of a potential crisis.

2) Monitoring with Automated Reporting

Keeping valuable data secure is critical to maintaining professional sanity. However, it's not enough to assume all backup jobs have been successfully completed. Monitoring backups with the use of automated reporting can eliminate the need for logging into systems daily.

These data reports should clearly outline how much data was backed up along with other pertinent information. Reports should be scheduled on a regular basis and

provided to company stakeholders as needed. Any failures should be noted and addressed immediately so that the proper corrective steps can be taken.

3) Properly Organize Backup Jobs

Organizations should not backup all their data simultaneously. Backup jobs should be separated in a clearly defined, rational manner. Properly organizing data allows for increased control over backup jobs and a higher rate of success.

Backups should be logically grouped together by department or business needs. All applications similar in nature should be ran together concurrently. Segmentation allows processes to run more efficiently while prioritizing critical data.

Setting up files in an organized manner allows users to easily manage backup jobs for increased focus on areas most crucial to the business.

4) Understanding Retention Requirements

Backup retention policies dictate how long data files are stored and maintained. Depending upon the needs of your company, some data must be readily available for weeks, months, or years at a time. Obtaining a clear understanding of your company's data retention requirements is critical to maintaining a successful data backup strategy.

Many organizations are subject to regulatory requirements or compliance standards that must be met (e.g. PCI, HIPAA, DoD, etc). These companies must follow specific policies when it comes to retaining data over a certain period of time. Failure to adhere to these regulatory bodies could result in fines, penalties, or permanent business closure.

Having a clear understanding of storage requirements allows businesses to better utilize data backup strategy. Longer retention periods may require additional storage capabilities. Not all data is subject to the same retention requirements so it's important to identify which policies may affect your business. Doing so can help avoid any potential lapses in data backups occurring from insufficient storage.

5) Data Backup Diversification

Diversification is key when it comes to data storage needs. Copies of data should be sent to multiple locations as an offsite insurance policy in times of emergency. Supplemental data backups can protect businesses if anything happens to primary data sources.

Storing data in various locations can help safeguard the interests of your business in times of catastrophe. Protecting data files at all times is a non-negotiable requirement for allowing business operations to flow uninterrupted.

More than one backup source should be maintained to increase data protective measures. Consider using combinations of hard drives, tape drives, and cloud-based backups that can keep you secured under all scenarios. Like they always say, “Never put all your eggs in one basket.”