**Why is it important to have a backup system in place that works closely with cyber security framework?**

The purpose of the backup is to create a copy of data that can be recovered in the event of a primary data failure. Primary data failures can be the result of hardware or software failure, data corruption, or a human-caused event, such as a malicious attack (virus or malware), or accidental deletion of data.

**5 Steps For Creating a Backup Strategy**

1. **Define your backup needs**

When creating a backup strategy, consider the following factors to ensure your company’s unique needs are covered:

* Risk
* Infrastructure
* **Frequency**
* **Compliance**
* **Storage**

1. **Budget for your backup plan**

Since not all backup services cost the same, develop a budget before committing to a solution. By doing this, you can determine how much the company is willing to spend on a backup solution and whether it will be a capital or operating expense.

1. **Choose a data backup vendor**

While it’s possible for your organization to implement a backup solution without assistance, a third-party backup vendor can help ensure you implement it correctly and effectively.

1. **Implement your data backup plan**

After choosing a backup platform, consider what role your company has to play in implementing the strategy. Vendors take considerably different approaches to helping new customers successfully adopt and deploy their solutions**.**

1. **Test your data backup plan**

Once you’ve outlined and defined a backup plan, you need to test it to verify that it works. One way to do this would be to simulate a data loss (where data is deleted) and a data corruption (where data is updated).