Cyber tips: **Backup policies**

Questions about a businesses network backups are common. But what does a good backup policy include and why can it make or break a businesses capability to bounce back from a cyber incident?

Data is the most valuable part of a computer system and may be irreplaceable if lost to a ransomware attack or a hardware failure, or if it becomes corrupted. The following tips will assist you planning and preparing a backup policy for an incident in case the worst happens.

What is a backup policy?

A backup policy is a well-thought-out plan to mitigate against data loss that could happen due to a ransomware attack, hardware failure, data corruption, or some other detrimental event. If implemented well, it can help an organisation to return to business as usual more quickly and easily.

The complexity of the backup policy will depend on the size of the organisation, the number of applications and databases it uses, and the quantity of data that requires backing up. It will also depend on company policy and regulatory obligations applicable to the organisation.

How do I implement backup policy best practice?

1. Identify your most critical data and plan accordingly
   By identifying the most critical data to your business, resources can be allocated to ensure that this data is protected and prioritized. Backups can be tailored to that particular data accordingly.

2. Take frequent backups
   If you have mission-critical data, then attention should be paid to the frequency of the backups that are taken.

3. Use the 3-2-1 approach to backups
   Create three copies of your data in addition to the original file, using two different backup media types stored locally and one copy stored remotely offsite.

   Backups should be isolated or air-gapped from the network when not actively backing up data. Backup media should never be permanently connected physically or over the network.

4. **Practice versioning data**
Backups should contain old versions of your data, not just current versions of files backed up most recently. This is important in case of file corruption or ransomware that may be lurking in current data backups.

5. **Periodically test the integrity of your backups**
Data should be checked regularly to ensure that it is accessible and readable.

Why are backups so crucial and what happens if they fail?

We recommend this level of diligence because backed up data can be recovered from if you suffer a cyber incident. Reducing the business downtime, the need to pay a ransom and the time it takes to get back up and running.

But even with the best intentions, back-ups can sometimes fail. Whether they're not pulling the right data, at the right intervals or at all, there are cases where recovering from backups does fail. This is where having a cyber insurance policy that offers data **recreation** is key. It covers the costs to recreate any data lost in a cyber incident if your backups fail. A lot of coverage will stop at data recovery, but at CFC we go the extra mile to help rebuild lost data.

Other considerations for your backup policy

- Data should be encrypted when backed up. This will help prevent unauthorised access.
- Consider making your backups immutable, so they cannot be altered by you or the bad actors.
- Consider using remote storage. Cloud based storage can be a cost-effective option if managed correctly.
- Automate backups where possible. This will make the practice of backing up your data a part of everyday business.
- Consider the retention period for your backups. This is especially important if you are using cloud services to back up your data. Cloud data storage costs can mount up so determine a sensible length of time for storage in your backup policy, considering legal and regulatory obligations.
- Consider your data retention policy. Do you actually need all the data that you are storing and backing up? Often data is stored unnecessarily adding an unnecessary cost and has additional security burdens if exposed.

Further information

+

- UK National Cyber Security Centre advice on backups can be found here.
- USA CISA advice can be found here.