# MEETING NCSC GUIDELINES FOR DATA PROTECTION.

https://www.ncsc.gov.uk/blog-post/cloud-backup-options-for-mitigating-the-threat-of-ransomware

## 3:2:1 Guidelines

NCSC state that three copies of your companies data (one production, and two held in backup) should be held at all times.

### How can Cohesity & CDW support this?

Cohesity and CDW are able to provide a solution to best meet your organisation's requirements reducing cost and improving RTO (Recovery Time Objectives).

Cohesity can replicate to another location within the organisation either on Cohesity for rapid recovery or to a 3rd party NAS or Object repository either on-premises or to the public cloud of your choice e.g. Azure / AWS.

For organisations without a second location, CDW offers an As-A-Service based option.

## Automating Data Protection

NCSC states that critical data held for recovery must be protected regularly; the more frequently backups are taken, the easier and quicker it is to restore.

### How can Cohesity & CDW support this?

Traditional backup environments can be complex to manage with performance bottlenecks limiting how often backups can be taken.

Cohesity automates protection by discovering new workloads ensuring backups of critical data are always included.

Cohesity's unique technology distributes backups across the platform enabling more frequent backups and quicker recovery, with reduced data loss.

## Immutability

NCSC states one copy should be stored off-site and offline or be immutable by online means, ensuring your backup copies are protected from ransomware.

### How can Cohesity & CDW support this?

Backups stored on Cohesity are immutable providing an effective barrier against ransomware and its impact on your critical data.

Cohesity supports WORM (Write-Once-Read-Many) which ensures that even Administrators cannot delete or reduce backup retention where applied.

Legal Hold is also supported which enables a reactive method to lock in individual backups that may be needed for compliance purposes.

## Administrative Access Controls

NCSC guidelines state that there should be administrative access controls in place to control access to data.

### How can Cohesity & CDW support this?

Cohesity supports granular RBAC (Role Based Access Controls) which can limit both access and authorisation of the environment helped by Active Directory integration.

This could for example allow a user to create a new backup but not append one that exists.

Furthermore, Cohesity supports Multi-Factor Authentication to enhance security of the environment in the event of a compromised user account.

**For more information, contact Cohesity@uk.cdw.com**

COHESITY
PREMIER PARTNER

CDW® PEOPLE WHO GET IT®

OWNER: Partner Marketing
DATE: 15/09/2020 V1.0

CONFIDENTIAL SENSITIVE