

# How NAS Data Actually Gets Lost

Even With RAID – 5 Real Scenarios + What Actually Protects You

## WHAT RAID ACTUALLY PROTECTS

SCENARIO	RAID HELPS?
Single drive hardware failure	YES
Drive failure mid-rebuild (2nd drive)	RAID 6 only
Ransomware / file encryption	NO
Accidental file deletion	NO
Controller / NAS hardware failure	NO
Fire, flood, theft	NO
Bit rot / silent data corruption	ZFS/btrfs only
User error (wrong format, overwrite)	NO
Software/firmware bug data corruption	NO

⚠ RAID is uptime insurance, not data insurance.

## 5 REAL DATA LOSS SCENARIOS

- Ransomware**  
 Encrypts every mounted share. RAID replicates the encrypted data across all drives instantly.  
 Fix: air-gapped off-site backup + versioning
- Second Drive Fails During Rebuild**  
 RAID 5 is fully vulnerable during the rebuild window (12–36 hrs). Any second failure = total loss.  
 Fix: RAID 6, or a hot spare
- NAS Controller Dies**  
 Proprietary RAID metadata may make drives unreadable in a different enclosure or brand.  
 Fix: backup independent of NAS hardware
- Accidental Deletion / Overwrite**  
 Deleted files sync instantly to all drives and any connected cloud sync.  
 Fix: versioned snapshots + separate backup
- Theft or Physical Disaster**  
 NAS + all drives taken or destroyed together. No RAID level survives this.  
 Fix: off-site backup – cloud or USB rotation

## 3 THE 3-2-1 BACKUP RULE

**3**

COPIES OF YOUR DATA

**2**

DIFFERENT MEDIA TYPES

**1**

COPY STORED OFF-SITE

**Example:** NAS (live) + external USB (local) + Backblaze B2 (cloud)

**NAS counts as 1 copy** – even with RAID 6, it is one logical copy.

**Cloud sync ≠ backup** – Dropbox/OneDrive propagate deletions instantly.

## BACKUP PLANNING CHECKLIST

- Off-site backup destination chosen  
 Backblaze B2, Wasabi, or USB drive kept off-site
- Backup schedule set (daily minimum for active data)
- Versioning enabled – how many versions retained?  
 Minimum 30 days to catch ransomware incubation
- Restore tested – actually recovered a file  
 Untested backups are not backups
- Drive failure risk assessed:  
[needtoknowit.com.au/tools/drive-failure-risk/](https://needtoknowit.com.au/tools/drive-failure-risk/)
- Backup capacity sized:  
[needtoknowit.com.au/tools/backup-calculator/](https://needtoknowit.com.au/tools/backup-calculator/)



### MORE FREE NAS PLANNING TOOLS

[needtoknowit.com.au/tools](https://needtoknowit.com.au/tools) – RAID Calculator · Drive Failure Risk · Backup Calculator  
 Power Calculator · NAS Sizing Wizard · Transfer Speed Estimator · UPS Runtime Estimator

Need to Know IT  
 Independent Australian storage guidance  
[needtoknowit.com.au](https://needtoknowit.com.au)