Planning for the Worst: Disaster Recovery Strategies to Preserve Your Data

Elio Grieco
grieco@egx.com
602-688-4014

1. What is your data worth? DR (Disaster Recovery) planning starts with assessing requirements.
- What types of data do you have?
- How much data can you afford to lose? What would it cost to replace?
- Backing up is always cheaper than disk recovery, a few hundred dollars vs. well into the thousands.

2. Failure modes and threat models: How does data disappear?
- In DR planning faith and optimism are best avoided. Always plan for the worst possible scenario.
- Storage system failures: all drives fail sooner or later…usually sooner.
- Environmental factors: fires, floods, earthquakes, tornados, hurricanes, lightning, riots, etc.
- Threat models: physical theft, system intrusion, denial of service (especially CryptoLocker), etc.

3. Backup principles
- Never go proprietary! The point of backups is to keep your data available. The more obscure the format, the harder it is to access your data later. Open and standard are the key.
- Rule of 3: If your data is not in at least 3 places it doesn't exist. The more important the data, the more copies should exist.
- Geographic distribution: the more distance between copies, the better protection against environmental factors and physical theft.

4. Backup techniques: pros and cons
- Copying files allows for fine grained backup.
- Cloning disks allows for instant recovery after a disaster by booting from the disk's clone.
- It doesn't count if it's not automated! Computers don't forget to backup, you will.
- Encryption: Keeps your data safe from prying eyes, but remember the key!
- Data integrity assurance: If it's really important, checksum it and have multiple copies.

5. Data storage options
Online: Data can be accessed instantly but is vulnerable to a system compromise.
Nearline: Data can be accessed quickly (minutes or less), potentially still vulnerable to compromise.
Offline: Can take hours to days to access, but is immune to online attack scenarios.
- **CD/DVD** (offline, nearline) Great for archival and offsite storage, cheap, usually write once (protects from accidental overwrite and malicious attacks like CryptoLocker). Good data lifetime.
- **M-Disc** (offline, nearline) Somewhat more expensive than DVD but otherwise similar. Outstanding data lifetime, ~1,000 years in accelerated testing.
- **Hard Drive** (all) The most economical way to backup. Ok data lifetime.
- **Flash Drive** (all) Very portable. Good data lifetime.
- **RAID** (online, nearline) Ideal for protecting from disk failures and storing lots of data. Excellent data lifetime if maintained and powered.

6. Restoration and recovery
- Test your strategy or you don't have backups. There's nothing worse than trying to restore from a backup only to find that you can't get your data back.
- Recovery windows: When do you need your data? Instant recovery, or hours to days?
- Partial vs. full recovery: Restore just a few files vs. an entire computer.
- Recovery time is usually proportional to the amount of data you need back, plan accordingly.
- Disk cloning can provide almost instant recovery.
- RAID can do live recovery if a disk fails.
- Choose a strategy to match the disaster: don't simply restore systems after a security breach.

7. The "Cloud" (aka hosted services)
- You need to trust the provider with your data or encrypt the data before storing it. If they tell you "we encrypt your data…" it doesn't count as encryption.
- Cloud backups offer massive equipment and geographic redundancy by professionals.
- How good are your professionals? Companies make mistakes too. Have alternate copies.
- Cloud backup is a service not a product. You have to keep paying to keep your data.
- Modern computing is only a few decades old. How long will your backup provider be around?