WHY OFFSITE BACKUP COPIES MATTER…

Most organizations today have adopted what is known as the 3-2-1 backup strategy. A part of that strategy includes managing offsite backup copies. Maintaining offsite backup copies isn't a new concept, but has it changed and are new market dynamics, policies, or laws making it easier to safeguard an organization's data?

What is the 3-2-1 rule for backup copies?

The rule is that an organization should maintain three copies of data, leverage two different types of media to store the data and ensure one copy of the data is offsite. The three copies of data include the production or primary copy with essentially 2 other copies where one of them is remote or offsite. The concept is to ensure a point of failure such as a ransomware attack, natural disaster, system failure, or human error doesn't affect an organization's ability to maintain their business continuity and recovery capabilities.

Why offsite backup copies?

Remote copies of data, stored offsite or in the cloud, have become a cornerstone of modern storage strategies, enabling enterprises to safeguard information while maintaining operational continuity. Tape backups are still being leveraged as a separate media and for remote backup purposes, so establishing the capability to manage backups on disk, cloud, and tape are essential. Challenges with ransomware and cyber-attacks have become a new normal and regulatory compliance demands are continuously growing as a result, changing the requirements for remote copies.

1. **Business Continuity and Disaster Recovery (BC/DR)**
Remote copies ensure that in the event of a local system failure, data corruption, or site-level disaster, a secondary source of information is readily available. Recovery times improve significantly when remote copies are maintained with synchronous or asynchronous replication, supporting strict recovery time objectives (RTOs) and recovery point objectives (RPOs).

2. **Ransomware and Cybersecurity Protection**
With cyberattacks targeting primary storage systems, encryption and remote immutable copies act as a secure layer of defense. By isolating data in a different physical or logical environment, organizations can recover quickly without paying ransom or risking extended downtime.

3. **Regulatory Compliance and Data Governance**
Many industries, including healthcare, finance, and government, require secure offsite copies for auditability and compliance. Remote copies provide verifiable evidence of data integrity, retention, and availability.

TEL (631) 777-5188 · FAX (631) 501-7633 · falconstor.com · rev 08262025

WHY OFFSITE BACKUP COPIES MATTER…

4. Flexibility Across Hybrid and Multi-Cloud Environments
Remote storage copies are not limited to physical offsite data centers. Today, cloud platforms offer cost-efficient, scalable options for creating secondary data copies. Organizations can balance performance, cost, and risk by maintaining copies across hybrid infrastructures.

5. Operational Efficiency
Remote copies enable more than just recovery. They can be leveraged for testing, development, and analytics without impacting production workloads. This creates a dual value proposition—protection and productivity—from the same data investments.

Regulatory Compliance Demands

New challenges, new laws and policies are driving the continued adoption of offsite backup storage. Here are just a few that demand offsite backup copies.

- **DORA (Digital Operational Resilience Act)**
  DORA has been enforced in the EU for financial institutions to be more vigilant in terms of their security measures and ransomware attacks. The ruling includes enforcing financial institutions in the EU to ensure one copy of data is remote from the source.
- **PCI DSS (Payment Card Industry Data Security Standard)**
  The Payment Card Industry Security Standard Council (PCI SCC) was formulated by the major credit card companies and has strict requirements about the storage of payment transaction data globally. PCI DSS requires that all businesses that accept, store, or transmit payment card information must abide to including offsite backup copies of payment information data.
- **HIPAA (Health Insurance Portability and Accountability Act)**
  For the healthcare industry, HIPAA sets a U.S. national standard to protect medical records and other personal health information. HIPAA mandates the storing of protected health information (PHI) to be in at an offsite physical location from the primary site to ensure data is always accessible, even in the event of a disaster.
- **SOX (Sarbanes-Oxley Act)**
  SOX was formulated in the U.S. to protect investors by improving the accuracy and reliability of publicly traded company disclosures. SOX requires financial data to be secured and recoverable in the event of a data loss by implementing offsite data backups to recover data for audit purposes.

FALCONSTOR

WHY OFFSITE BACKUP COPIES MATTER…

- **Cybersecurity insurance**
  With the rise in ransomware and cyber-attacks, many companies are investing in cybersecurity insurance. As part of the basic qualification process for coverage, the cybersecurity insurance policies require offsite backup storage.

Best Practices for Offsite Copies

Regulatory compliance demands can continue to change, as well as advancements in security to ensure your data is protected. Best practices for remote copies include some key steps in ensuring optimized data protection practices for remote copies.

Geographic Separation
Disaster recovery best practices include ensuring remote copies are stored in a location far enough to protect against regional disasters. Larger enterprises tend to even ensure protection storing off-site copies in two different locations regionally far enough from where the primary data resides.

Automation
Use modern storage solutions with built-in replication and orchestration for consistency and reduced manual errors. Built in replication capabilities helps to ensure for the quickest recovery capabilities. For added protection, one-to many replication capabilities enable added protection leveraging multiple recovery duplicate sources.

Security
To address ransomware and cyber security threats, protect remote copies with encryption, access controls, and immutability. Encryption needs to be in place for data in motion and at rest. Immutability helps to ensure no changes can be made to saved data.

Regular Testing
Validate that remote copies can be restored quickly and accurately to maintain confidence in recovery. Regular testing of disaster recovery capabilities is key in ensuring all systems are operating with the ability to recover whenever a problem may occur.

Why FalconStor StorSafe?

FalconStor StorSafe for offsite backups can ensure that data is recovered quickly in the event of a disaster, protect against ransomware and cyber-attacks, and help organizations meet regulatory compliance policies.

Disaster recovery
Replicate workloads from on-prem to cloud or from one region in the cloud to another region to recover rapidly in the event of a disaster. One- to-many replication provides extended protection for managing multiple remote sites, leveraging multiple clouds, disk or tape.

FALCONSTOR

WHY OFFSITE BACKUP COPIES MATTER…

Ransomware protection
StorSafe encrypts data in motion and at rest using AES-256 with StorSafe managed keys for best-in-class security. StorSafe leverages Write-Once-Read-Many (WORM) virtual tapes to ensure data cannot be overwritten. Integration with IBM COS provides immutable backup capabilities.

Regulatory compliance
Offsite protection has no limitation on capacity. For offsite protection, FalconStor StorSafe provides the choice of physical tape, cloud object storage, or a twin copy of StorSafe running at a remote site where data is replicated continuously. Maintaining offsite copies of data helps organization meet regulatory and cyber insurance compliance.

No changes to existing backup and recovery processes
FalconStor StorSafe works with all major leading backup and recovery products, working complementary to provide optimized data protection.

SUPPORT AND SERVICES

For the latest information on our certification support visit
https://www.falconstor.com/support/certification-matrix/

Contact FalconStor: https://www.falconstor.com/contact/
FalconStor reseller: https://www.falconstor.com/partners/all/

FALCONSTOR

