Why your current disaster recovery strategy may not cover compliance

Written by:
Chris Patterson, Sr. Director, Product Management
Introduction

Implementing a reliable business continuity and disaster recovery plan (BCDR) is an important milestone in any organization’s IT strategy. While major aspects of business continuity—such as recovery point objectives (RPOs), recovery time objectives (RTOs) and service level agreements (SLAs)—are factored in when developing BCDR plans, compliance requirements associated with individual industry verticals are often not given enough importance. Regulatory frameworks like PCI, GDPR, HIPAA/HITECH have associated BCDR standards among various industries that should be followed to ensure compliance.

A linear approach to business continuity planning could lead to non-compliance complications and, eventually, a collapse of the company in the long run. This white paper will focus on the major compliance issues that organizations need to be aware of when developing a well-rounded BCDR strategy.
Chapter 1: Business drivers Influencing BCDR strategy

An organization’s disaster recovery strategy is determined by the long-term business goals of a company as well as variables like customer SLAs, business geography, data availability targets, security, and compliance. The following is a brief explanation of those factors.

Service level agreements

Service interruptions can have disastrous consequences for organizations. There are often financial penalties when SLAs are not met. Downtime is unacceptable and erodes hard-earned customer loyalty.

Geography of business

When data is being accessed from around the world, the location of data storage and management teams in the event of disaster is critical, because many organizations are bound by compliance regulations to store data within specific geographic regions, and a specific minimum distance away from the primary data site. Cloud-based Disaster Recovery-as-a-Service (DRaaS) providers address this challenge to a large extent.

Data availability targets

Two factors determine the RTO and RPO of a business continuity and data recovery strategy: the duration for which an organization can afford for data to be unavailable without critical business impact, and the maximum acceptable data loss. When selecting a service provider or a tool for DR, these are considered the most critical of the core criteria.

Security

When data is stored for disaster recovery in an offsite location, security should be ensured at all levels. This is achieved by managing authorized access at the management layer and data encryption mechanisms at the data layer. It’s the responsibility of the cloud service provider to make sure that customer data is safe while being transported for disaster recovery needs.
Chapter 2: Compliance standards and disaster recovery

Compliance standards for each industry apply to the DR strategy as well. For example, if your compliance standards mandate that data should be encrypted at-rest, the same standards apply for production data as well as data stored offsite or in the Cloud. Following is an overview of the main regulatory frameworks that organizations must take into account when crafting a disaster recovery plan:

**HIPAA**

The U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA) focuses on the privacy and security of a patient’s healthcare information. Two primary requirements of the security rules include secure access, and a contingency plan to ensure continued availability for electronic protected health information (ePHI) in case of a disaster.

**GDPR**

The European Union’s General Data Protection Regulation (GDPR) focuses on the data privacy of EU residents and goes into effect on May 25, 2018. The regulations cover production data as well as disaster recovery systems. The GDPR requires that personal data be encrypted. It also emphasizes the importance of ensuring confidentiality, integrity, availability, and resiliency for processing systems. The GDPR defines stringent rules for data transferred outside EU region:

“A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection.”

Two key HIPAA requirements to consider – secure access and a contingency plan.
To remain GDPR-compliant: Encrypt client data and ensure processing systems are confidential, have high integrity and are always available and resilient.

These guidelines are laid out in Chapter 5 of the GDPR and should be given careful consideration when planning an offsite storage location for DR.

**PCI DSS**

The Payment Card Industry Data Security Standards (PCI DSS) define the technical and operational requirements for payment cardholder data security. PCI standard 12.10.1 highlights the need for an incident response plan in the event of a data breach and mandates that a data backup, business continuity and disaster recovery process must be implemented. PCI standard 9.5.1 states that any backup data should be stored securely in an offsite location. These standards are key considerations when developing a DR strategy for PCI compliance.

**FedRAMP**

The Federal Risk and Authorization Management Program (FedRAMP) is a directive framework to be followed by U.S. federal agencies for secure cloud consumption. FEDRAMP emphasizes the importance of contingency planning and the requirement for DR planning for hosted services in cloud.

**SOX**

The Sarbanes-Oxley Act of 2002 (SOX) lays out guidelines to protect the public from fraudulent enterprise practices. SOX includes regulations regarding data retention of audit information for no less than seven years.
Chapter 3: Missing links in disaster recovery plans

Compliance standards for production environments are usually diligently followed by IT teams. However, when it comes to disaster recovery environments, not much thought is given beyond creating a baseline backup/DR strategy. The nuances of DR contained in regulatory frameworks are often overlooked. If neglected, this could eventually result in non-compliance and even severe financial penalties in some cases. Let’s review some of these missing links.

Security at-rest

Data layer security is a basic standard for production data. When this data is shipped to an offsite location, data layer protection is equally important. In DR plans that involve the shipping of data to offsite locations, physical media security and at-rest encryption is often not given due importance, even though all major compliance standards require this.

Security in-transit

Data in transit is susceptible to being intercepted by cyber criminals. Real-time data contains valuable information like certificates, encryption keys and personally-identifiable information. In production environments data is transferred in secure channels to eliminate this risk. However, in systems that use near real-time replication for lower RTOs and RPOs, the risk of data interception is higher if secure transfer is not implemented in the data transmission channel.

Availability

High availability is built into production systems by design in order to ensure multiple copies will be made available by underlying redundant systems. An example is Patient Health Information (PHI), which should always be available to meet HIPAA compliance. However, the same goes for disaster recovery systems too. The DR solution should be reliable enough to restore data quickly in the event of disaster, and have built-in resiliency for the stored data.

Location

Standards like GDPR place particular emphasis on the location of stored data. The data being sent to an offsite or a cloud location for disaster recovery purposes should also be considered for compliance along with production data.

Access control

All compliance standards dictate a stringent access control mechanism for data to avoid unauthorized access, especially for sensitive personal information. These controls should be implemented with same diligence for data that is replicated and moved to a DR site.

Full compliance with your DR means data must be:

- Secure in-transit and at-rest
- Available easily and quickly
- Stored offsite
- Restricted from unauthorized access
Chapter 4: Bridging the gaps

When planning your disaster recovery strategy, organizations should be sure that all controls for live production systems and data are also applied to DR systems as well, to ensure compliance. Depending on the compliance standard that is being targeted, all applicable control metrics should be considered for disaster recovery platforms and data, along with production systems.

A checklist to ensure you’re covering your DR needs:

- Select a DR solution that provides end-to-end encryption, e.g. for data at-rest and data in-transit. It is prudent to select a solution that provides out-of-the-box encryption capabilities, so organizations don’t have to spend additional time and effort.
- Create a well-defined process for the management of data encryption keys in line with data protection compliance guidelines. Implement a logging mechanism to audit the use of key and data retrieval.
- Implement data and management plan access control mechanisms to ensure that only authorized personnel have access to the disaster recovery data. This ensures protection of PII and ePHI assets for HIPAA and GDPR compliance.
- Use a DR tool that supports audit trails of failovers for documentation purposes.
- When selecting DRaaS providers, check for the SLAs that will take care of the disaster recover solution availability. If using on-premises DR solutions, review the architecture to ensure that high availability is built into the solution.
- Select a vendor that can store multiple copies of disaster recovery data in multiple locations for resiliency. However, organizations aiming for GDPR compliance must ensure that the data is not being replicated to regions outside the EU.
- Regularly test and document to ensure resiliency and availability. This is relevant for all compliance standards, especially GDPR, which emphasizes confidentiality, integrity and availability of data. HIPAA compliance also requires periodic testing and revision of contingency plans.
- FedRAMP regulations apply to cloud-hosted environments, and therefore it makes more sense to consider cloud-based disaster recovery solutions.
- Cloud storage is a reliable way to comply with the offsite data storage requirements of PCI/DSS & FedRAMP. Data transfer and storage should be secure. In case of cloud-native environments, data should be replicated and stored in a different region or geography.
- Data recovery solutions should ideally support long-term data retention with inexpensive storage options. Cloud-based DRaaS vendors have an advantage because they leverage less expensive cloud storage and can offer long-term data storage at incredibly low pay-as-you-go rates. This will help organizations targeting long-term audit data retention for SOX compliance.
Chapter 5: Leveraging MCSPs for disaster recovery

Compliance standards should be considered as a major factor in selecting the right disaster recovery solution vendor. Defining a DR strategy and setting up the solution demands diligent planning and execution. That’s why it’s worthwhile to leverage the services of a Managed Cloud Service Provider (MCSP) with proven expertise in DRaaS implementation.

To help you meet your organization’s compliance requirements, Navisite provides enterprise-class DRaaS services such as:

- A heterogeneous support model where virtual machines and applications can be replicated between on-premises and off-premises DR sites.
- Managed offsite backup and shared backup services.
- Enterprise-class, financially-backed and industry-leading SLAs that fit your compliance standards.
- Flexibility to choose between hot site, warm site and cold site DR models. This choice depends on the RPOs, RTOs, and availability targets defined by compliance standards.
- Customers can adopt a hot site disaster recovery model for fastest recovery, because it ensures near real-time replication and failover capabilities. It helps to achieve the strict availability targets of standards like HIPAA.
- Compliance controls are factored in at every stage of development; implementation is performed by expert engineers.
- Secure data centers for DR meet strict requirements for data integrity, confidentiality and privacy requirements.

A managed cloud service provider (MCSP) is a great way to more easily meet your DR concerns and compliance requirements, by offloading those responsibilities to an organization always on top of requirements.
Summary

The key considerations in designing a secure and compliant infrastructure depends on factors such as encryption, access control, secure data transfer and storage, availability, and resiliency at both production and DR system layers. If your organization needs to comply with leading regulatory frameworks, it is important that both production and DR systems meet the criteria.

There are many advantages of using an experienced service provider like Navisite for a data recovery solution. Using Navisite will help ensure that the intricacies of compliance standards will be part of your DR strategy and not overlooked. Visit our website to learn more about business continuity and disaster recovery with Navisite, or call us at (888) 298-8222.

Learn how Navisite can help your organization collaborate more efficiently and productively at www.navisite.com/collaboration