Disaster Recovery: A Focus on the Essentials

Every organization contends with planning for the unthinkable, preparing for the occurrence of the what-if scenarios, threats of an increasingly connected business landscape.

What if systems are lost, not just downtime or a service incident, but incapacitated in a way that required resumption of services from another location? While not a new concept in principle, rapidly changing cloud, virtualization and platform capabilities can be confusing. For many organizations, these complexities are distractions from maintaining the essentials needed to perform critical recovery tasks. A 2016 survey from CloudEndure® identified that while 90 percent of respondents claimed they meet their Disaster Recovery (DR) goals, only 22 percent of organizations measure this capability. This means that the first time the remaining 68 percent of these organizations will find out if their DR actually works is when their systems are incapacitated. The increasing threat of cyberattack continues to drive up the probability that you will need to execute on your DR plan. Many organizations have reported being effected by malware and/or virus injections, and this trend will only increase in the health care space. Your last line of defense when dealing with the unthinkable should be your DR plan; therefore, it is essential to focus on developing a plan before it is needed. This paper provides an overview of the essential elements to be considered when evaluating DR posture and practices and provide guidance in the effective development and execution of your DR plan.

> ***Through 2020, integration work will account for 50% of the time and cost of building a digital platform.***
>
> ***-Gartner***

Disaster Recovery Integration Focus

Rapid advancements in technology are increasing the options for organizations to integrate and deploy their digital presence. With this increased potential, the complexity of systems grows as organizations take advantage of the commoditization of IT services to their benefit. This complexity, while efficient for product delivery, tends to cloud the interrelationships between supply chains, service providers and business associates. Based on business needs and resource capabilities rather than a tactical process perspective, successful DR planning and implementation is only successful if your service partners understand and practice DR implementation.

> ***"The insurers have probably some many different legacy systems bolted onto older systems…They may not be quite as synchronized as much as they should be"***
>
> ***- Ken Dort, Modern Healthcare***

The key risk of system integration and partnering on a critical digital platform is the technical capabilities of a prospective integration partner and their ability to execute within the context of your DR process. This key risk is often overlooked. Many organizations discover too late that their partner either does not practice appropriate DR process integration as part of their service delivery, or they only provide a one-size-fits-all approach that does not serve the needs of your organization and their specific DR approach.

Organizational focus on the essentials of DR across the integration management continuum, from service management through the security implementation, as part of the services procurement process, is vital to DR effectiveness. Selected partners must integrate DR through a holistic approach to business continuity to ensure an integrated digital platform and integrated services delivery. Figure 1 depicts a DR ecosystem integration model for a mature partner engagement.

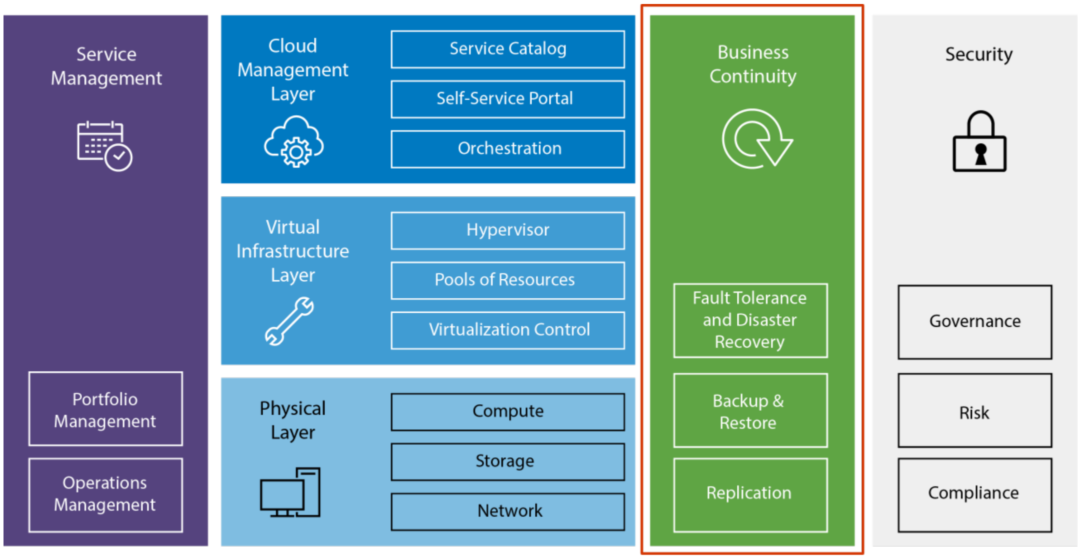


Figure 1. Disaster Recovery ecosystem integration model — mature DR partner engagement.

Disaster Recovery Security Focus

On February 4, 2015, Anthem disclosed that criminal hackers had broken into its servers and stolen millions of records containing Personally Identifiable Information (PII). In addition, integrated partner health care organizations such as Amerigroup Corporation, CareMore Health, UniCare and HealthLink were victimized through this attack. Other health care insurers have since seen similar attacks to include large data hacks at CareFirst Health Plans, Excellus BlueCross BlueShield and Premera Blue Cross.

It is clear that health care insurers are being systematically targeted for cyber exploitation; this underscores a need to focus on selecting DR integration partners that manage risk to industry specifications, as essential to sound business practices.

Security Gone Wrong: A Mini Case Study on Third Party Integration Risk

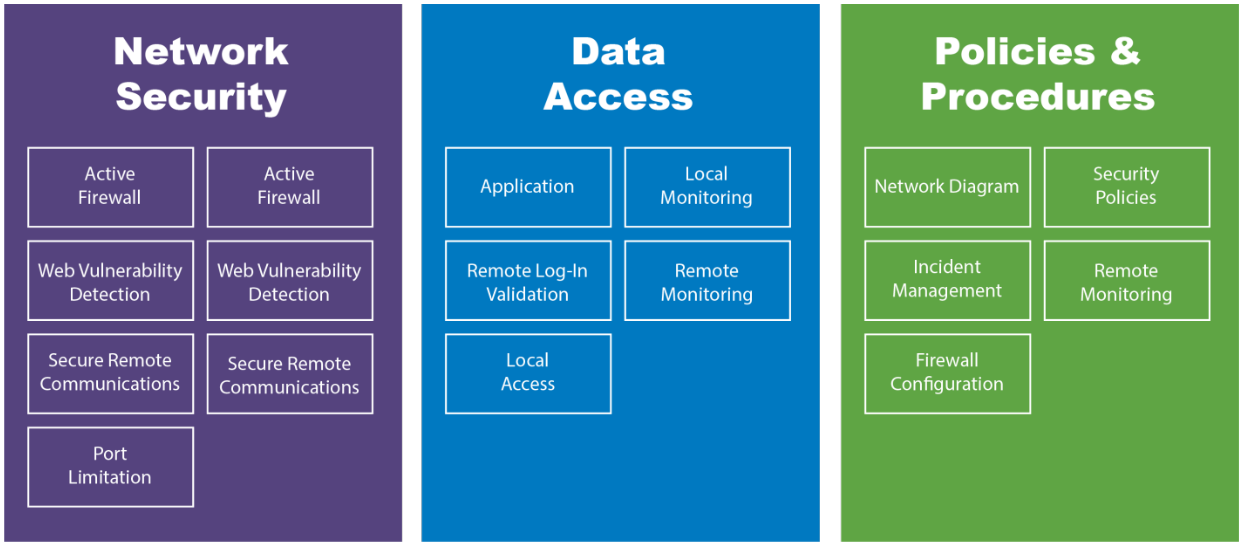
> ***"Top three requirements for an appropriate disaster recovery solution:***
> - ***Reliability of solution***
> - ***Speed to recovery***
> - ***Cost of solution"***
>
> ***-Fred Rowell, CDS CTO***

In 2013, Target Brands Inc. (Target) experienced a cyberattack that stole contact information from more than 60 million customers and more than 41 million payment card account numbers. In May 2017, the federal government ruled that the company must pay $18.5 million to 47 states and the District of Columbia to resolve state investigations into the cyberattack. The largest settlement ever for a data breach that pushed the total cost well beyond the fees Target incurred to diagnose and correct the breach and to notify customers. The investigation determined that the hackers gained access to Target's computer gateway by stealing credentials from the company's third-party air conditioning vendor. Once the hackers had access, they installed malware in the customer service database system and captured names, phone numbers, email addresses, payment card numbers, credit card verification codes and other sensitive data. According to a Soha Systems Inc. survey on third-party risk management, 63 percent of data breaches can be tracked directly or indirectly to access by third-party vendors. This highlights the risk of third-party vendors in a security loop.

Technical Security Considerations for DR Integration

As holders of private data, such as protected health information and personally identifiable information, health care organizations have a commitment to their customers, stakeholders and themselves to understand and evaluate risk within the environments for which they are responsible, to include their DR integration points. Any business case used to drive operational efficiencies through the integration of digital platforms needs to include holistic system security practices.

Organizational focus on the integration of security practices shown in Figure 2 must be part of the services procurement process, and selected partners need to demonstrate and measure security integration for all indicated DR functional service elements.



Network Security

Active Firewall

Active Firewall

Web Vulnerability Detection

Web Vulnerability Detection

Secure Remote Communications

Secure Remote Communications

Port Limitation

Data Access

Application

Local Monitoring

Remote Log-In Validation

Remote Monitoring

Local Access

Policies & Procedures

Network Diagram

Security Policies

Incident Management

Remote Monitoring

Firewall Configuration

Figure 2. Disaster Recovery Ecosystem Technical Security Integration Touch Points for a Mature DR Partner Engagement.

Compliance Security Considerations for DR Integration

In the health care industry, potential DR partners must understand the health care specific requirements that drive business for integration into your compliance practice. Companion Data Services, LLC (CDS) maintains a robust health care system security and compliance practice that responds to or aligns with these compliance frameworks for an integrated DR Service Delivery approach and adheres to:

- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Federal Information Security Management Act (FISMA)
- International Organization for Standardization (ISO) 9001:2015
- Federal Risk and Authorization Management Program (FedRAMP) Ready
- Uptime Institute Tier III
- Payment Card Industry (PCI) Compliance

DR Technology Focus

Every company has unique characteristics and IT architecture. Therefore a one-size-fits-all approach will leave gaps in DR posture that are difficult or impossible to reconcile. When choosing a technology strategy for recovery, you must first tier or rank digital platform groups to identify these essential elements:

- Specific technology dependencies
- Required recovery service levels
- Associated downtime cost

Organizational focus on these elements ensures that DR addresses the needs of each application stack tier in alignment with the associated business value. Selecting a DR integration partner becomes more straightforward once these digital platform groups are ranked and defined.

Compatible Technology Stack: Mind the Platform/Services Gap

The DR technology landscape has grown in complexity due to requirements of handling multiple and overlapping technical services. A major factor that ensures DR success is a clear understanding of the scope of the technology stack under consideration for sharing with or management by a DR integration partner. While virtual Windows and UNIX® platformed DR services are an important element of many hosted digital platform solutions, the whole technology stack must be looked at including critical mainframe application integrations. The ability to wrap integrated systems services across the stack is a key consideration in selecting a DR integration provider. Figure 3 details the applicable technology stacks and associated service delivery wrappers essential to an effective DR approach.

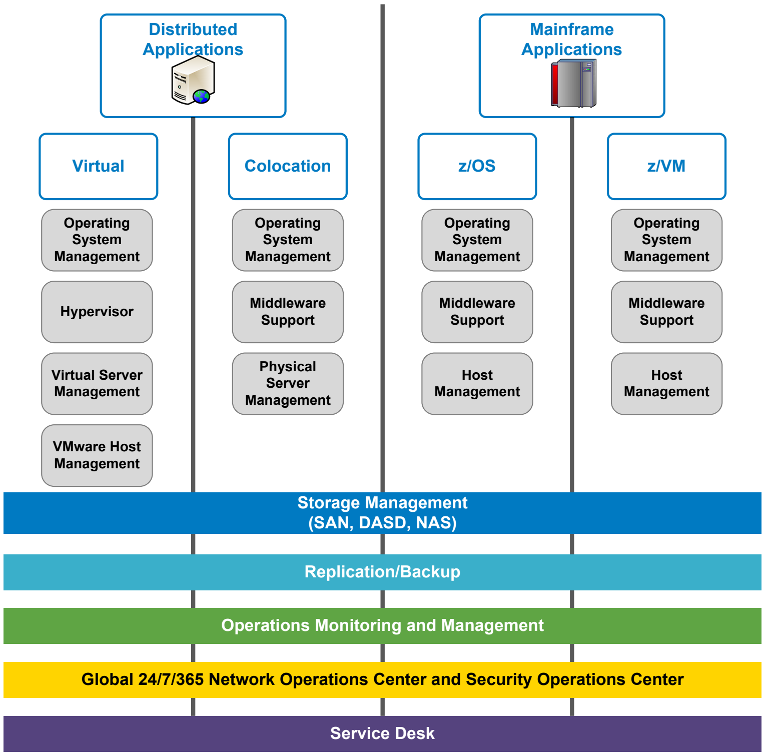
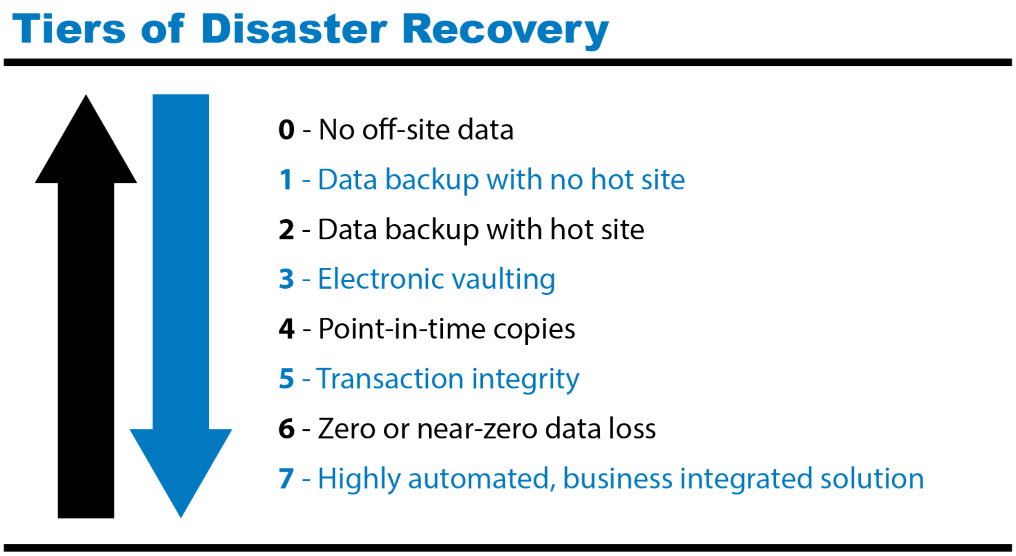

Distributed Applications
Mainframe Applications
Virtual
Colocation
z/OS
z/VM
Operating System Management
Operating System Management
Operating System Management
Operating System Management
Hypervisor
Middleware Support
Middleware Support
Middleware Support
Virtual Server Management
Physical Server Management
Host Management
Host Management
VMware Host Management
Storage Management (SAN, DASD, NAS)
Replication/Backup
Operations Monitoring and Management
Global 24/7/365 Network Operations Center and Security Operations Center
Service Desk

Figure 3. Disaster Recovery Technology Stacks and Associated Service Delivery Wrappers Essential to Effective DR.

Figure 4 shows the seven business application tiers of DR relative to cost versus availability.



Tiers of Disaster Recovery

0 - No off-site data

1 - Data backup with no hot site

2 - Data backup with hot site

3 - Electronic vaulting

4 - Point-in-time copies

5 - Transaction integrity

6 - Zero or near-zero data loss

7 - Highly automated, business integrated solution

Figure 4. Seven Tiers of Disaster Recovery Relative to Cost versus Availability

Cost Based RTO/RPO

In a recent survey by CloudEndure, 36 percent of organizations indicated that the cost of downtime exceeded $100,000 per day. One's own organizational mileage may vary. To clearly understand the business value of DR integration, the evaluation of cost versus availability must be determined. These values are typically represented in service level agreements as the Recovery Time Objective (RTO) and Recovery Point Objective (RPO). Successful DR partner integration hinges on the partner's ability to deliver diverse RTO/RPO service levels aligned with business application tiers. Another critical outcome is measurement of DR performance because "if you can't measure it, you can't manage it". Organizational focus must be on DR service levels to ensure effective and measureable DR outcomes are delivered at an appropriate cost point for the respective digital platforms.

Real World Testing Equals Measured Results

Thoroughly testing the DR integration plan is the only way to identify issues such as hard-coded IP addresses, host file entries, license file/key, configuration details and dependency on other applications/services and result in the need to update the DR plan to make it more robust. CDS performs audited DR testing on a regular basis. DR is audited during each exercise and results are fed back into DR planning to ensure a mature solution. While important, DR technology does not preclude the need for top-shelf planning, testing and continual improvement.

Conclusion

Evaluating DR posture relative to the capability of potential third-party partners is imperative. Changes in the DR landscape have opened up potential efficiencies, cost savings and increased capability that drive the business value of digital platforms. A clear focus on the essentials of DR will ensure a consistent and continuous view of potentially effective solutions. Done well, the result is a measured, cost appropriate and tested method to ensure that organizations can recover when the unthinkable happens.

The CDS Difference

As a partner in Disaster Recovery, CDS has a mature, stable, flexible and proven information services structure that supports innovative, end-to-end DR Services. Our services feature comprehensive physical, data and network security. And our solutions and services include traditional, virtual and cloud provisions for all aspects of technology for effective DR integration, from mainframe to distributed systems. Our cloud offerings and secure infrastructure managed services are unprecedented in the industry and include all disaster recovery capabilities to meet today's health care data protection requirements.

CDS Disaster Recovery Capabilities

- **Virtual/Cloud approaches**
- **Colocation**
- **Vendor agnostic technical solutions**
- **Tested, audited and measured DR results**
- **Tiered service delivery model**
- **Mature health care system security**
- **Integrated DR service delivery practices**

Our business model focuses on health care customer solution sets that incorporate appropriate technology with high-quality and responsive disaster recovery services. We carefully review DR industry practices and technical innovations with an eye towards extensible, flexible and cost effective DR use cases, while integrating with customers at the technical and process levels. Our solutions provide technical expertise and management teams with demonstrated relevant experience in DR integration services. With CDS, customers know that a complete disaster recovery posture is possible and executable in a measured and manageable way.

About CDS

CDS and our parent company support DR integrations for customers such as Medicare, Medicaid, TRICARE, Federal Employee Health Benefits Programs and Medicare Advantage health plans as well as commercial health plan business and infrastructure systems. More than 6 percent of all health care expenditures in the United States are processed through health care systems for which CDS maintains comprehensive, measured and effective disaster recovery services. In the ever-changing health care landscape, ensuring an economical, dependable and secure disaster recovery posture for our customers is our top priority.

Companion Data Services, LLC and its respective marks are trademarks of Companion Data Services, LLC. Because we are continuously improving our solution offerings, Companion Data Services reserves the right to change specifications without prior notice and disclaims all liability for any inaccuracies in this document including, without limitation, those arising from changes in solution offerings or from changes in technology. This material is a confidential, proprietary or trade secret product of Companion Data Services. Any unauthorized use, reproduction or transfer of these materials is strictly prohibited. For more information visit: companiondataservices.com.