

Preparing for Resilience: Disaster Recovery Plans

Chuck Cook | RENOVODATA



ISTOCK.COM/AJUST_SUPER4

THE UPWARD TREND of organizational data dependency grows in tandem with the breadth, severity, and complexity of cyber threats. The potential for a data disaster from a site outage, hardware failure, or simple employee error remains ever present. Between these internal and external factors, the threat of losing valuable data—or being without it—is overwhelming. Additionally, studies show that the cost associated with the risk of data loss is significantly higher for 3PL and trucking companies, especially those with 24-hour uptime, compared to other industries. Company leadership may hope for the best, but they can prepare for the worst by investing resources into creating a Disaster Recovery Plan (DR Plan). DR Plans serve as a fail-safe guide to recovering data, systems, and networks in emergencies. If constructed well and tested periodically, DR Plans can serve as the first major step in many things your organization can do to become resilient.

Fortunately, more and more organizations are adopting DR Plans each year. But as the data landscape rapidly evolves, an organization's IT resilience must grow in parallel. The need to drive a better customer experience has driven investments into other ways to deliver applications and data, including multi-cloud or hybrid cloud environments. The increased demand for disparate cloud services can create a complex IT landscape, and a Disaster Recovery/Business Continuity (DR/BC) Plan can help minimize business interruptions to normal operations. In addition, your plans should take into consideration the following:

- Limit the extent of disruption and damage
- Establish various alternative means of operations (work-around procedures) in case of fallout
- Accompanying training materials for personnel with emergency procedures (run books, vendors, cyber insurance resources, etc.)

A recent Unitrends study showed that only 44% of surveyed organizations had a documented DR plan—and only 31% of those organizations test their plans annually or less frequently. DR Plans demand continuous process improvement that coincides with the growth, upgrades, and other adjustments that your IT environment experiences. Failure to plan is planning for failure. Can your company afford that outcome?

A DR Plan is created to protect your company's infrastructure and data during an event that could cause disruption to operations by providing procedures that minimizes downtime. Breaking down DR Plans into the required resources, the plan's components, and best practices can make the company-wide planning process much more digestible for first-time and experienced planners.


Required Resources:

Unfortunately, DR Planning is not solved simply with a monetary investment. Significant internal resources will need to be devoted to the creation of the plan. However, the fruits of the investment will bear in case of emergency and can ultimately save the organization time and money in the long run. Here are some key elements for the effective development of a well-supported plan:

- **Leadership Approval** – Efficient planning starts at the top. An organization's leadership will need to be made aware of the development of the plan and the resources needed over the planning period.
- **Budget Considerations** – IT department funds are often tight. However, having a professional third-party perspective to evaluate your plan is invaluable. Funds may need to be allocated and siloed into different budgets. Additional solutions such as employee cybersecurity training, cybersecurity software, and consulting time may need their own budget.
- **Structured Flow** – Documentation, and planning needs to be a coordinated, structured effort. Building the framework will take internal and external research, which includes conducting interviews with employees at all levels of the company to gather the information you need. The process of creating the framework ideally also includes a third-party professional, like a Certified Business Continuity Professional, to guide you through the process. Make sure all of those involved follow the same framework,
- **Organizational Access** – This applies to both the systems and the personnel. Those leading the planning need access to the critical data, systems, network, and employees that apply to the recovery flow.
- **Routine Testing & Documentation** – As mentioned, DR Planning is a long-term commitment that requires periodic if not continual attention. Plans need to be exercised periodically to ensure a smooth execution in the event of an emergency. As time elapses and your environment changes, documentation needs to be updated and IT recovery solutions need to be reevaluated to ensure they meet the evolving needs.

Plan Components:

Once the resources are provisioned, use the plans components to begin discovery and development of your plan. There are several widely accepted names for the components of a DR Plan, but they ultimately boil down to Define, Identify, Determine, and Test. Following this framework through the creation of your plan helps serve as a catch-all for the most



THERE ARE **SEVERAL WIDELY ACCEPTED** NAMES FOR THE **COMPONENTS OF A DR PLAN**, BUT THEY ULTIMATELY BOIL DOWN TO **DEFINE, IDENTIFY, DETERMINE, AND TEST**.

critical data, systems, networks, and people that are needed in emergency situations.

1. **Define:** In the definition stage, the team involved in developing the plan utilizes the company's goals and the DR Planning framework to delineate what the plan needs to provide for the organization to be considered effective.

- **Scope:** The ideal DR Plan provides resilience for the entire organization—or more specifically—for all business processes that would impact operations if they were unavailable for minutes, hours or days. Due to the digital transformation of most industries, IT resilience is at the core of business resilience. Considering this, organizations should start with defining their business processes and dependencies, and allow the recovery of business functions to align with IT recovery.

- **Recovery:** This aspect of the definition component could be the most demanding and time-consuming. What is your organizations' step-by-step procedure for the recovery of each physical, virtual, and mechanical item that is critical to operations? For example, what solutions are in place to recover our servers, phones, internet, and power if there are various types of disruptions? What needs to be done to execute the solution? What buttons need to be pressed, and who needs to be involved? This step can serve as the basis for creating, updating, and analyzing organizational runbooks—a continuity tool that organizes written procedures for completing repetitive IT processes essential to operations.

- **Alerting:** Organizations will also define the step-by-step procedure for alerting the key personnel when a disaster strikes. Are your solutions managed by a vendor? Do only a few team members know how to recover something highly technical? These key staff members' names, numbers, and alternates need to be documented and available.

- **Policies:** Clearly defined preventative policies are valuable ancillary documents to your DR Plan. For example, password policies and acceptable use policies help guide employees across the organization on how to govern their technology usage at work. Additionally, while your organization establishes security policies, IT leaders can build and define training processes that will educate and equip employees.

- **Authorization:** Who is authorized to declare a disaster?

2. **Identify:** The definition component will consume a large portion of the documentation legwork needed in a DR Plan. Conversely, the identification and determination components will involve applications of what was defined.

- **IT Risks & Impact Analysis:** It is best to document recovery processes for each critical machine initially, but the relative criticality matters—and applications, servers, and data sets should be classified and ranked accordingly. If one machine or application has multiple critical functions depending on it—which is often the case due to the fast-paced, high-volume, and interconnected nature of 3PL operations—then that risk needs to be identified in the plan. This is an example of how DR Planning can identify shortcomings in your solutions and can help you budget toward the machines or processes that could have the largest impact on operations.

- **IT Resources:** Risk and impact analysis will identify the greatest risks to your organization's operations, but what investments have already been made to mitigate those risks? Has organizational management invested in a cyber insurance policy? If so, who are the primary contacts when a disaster strikes? Evaluate your vendors or partners' emergency resources to determine upfront their role if a disaster occurs (i.e., emergency hosting, data drive restoration, additional support, etc.).

- **Equipment:** It's unrealistic to assume an organization can afford to have duplicates of each critical piece of machinery on hand, but it's important to know how quickly you could have them if needed. Hardware failure, internet outage, and site disasters all need measurable contingencies to potentially fall back on.

- **Communications:** Managing communications both internally and externally in a disaster is not an easy task. Developing sample alerts and instructions to be distributed to your employees in the time of a disaster is wiser than scrambling to do so. Similarly, creating sample messaging for customers that are relying on your services during a disaster state can also help ease the stress during disaster. Crisis management resources are also an important service extended depending on your cyber insurance policy.

3. **Determine:** This component of the plan reflects what you've learned in Definition, and what you've decided in Identification, and provides real, measurable, valuable data pertaining to protection. Monetary and time costs are assigned to the recovery of critical business processes. If the investment of time or money is too steep to meet all recovery objectives, it is strategically sound to allocate available resources toward the most critical processes and goals first and save additional protections for the next budget cycle.

- **Recovery Time Objective (RTO) & Recovery Point Objective (RPO):** Extensive documentation of critical systems, the solutions that make them resilient, and the resources that manage the solutions provides your organization the information required to define the actual time it takes to recover. RTO can be assigned for each application, or each supporting



machine based on how quickly you can recover it. Likewise, RPO (how recent the data we are recovering is) can be determined based on the capabilities of the solution and your business processes. These values serve as benchmarks and tests should be measured against them.

- **Recovery Failover:** Failover is the ultimate solution to combat site outages, but it comes with a cost. Having the ability to failover your machines to an alternate location, whether your own or using a vendor's emergency hosting solution, can save hours to days while your organization tries to resolve the disaster. Knowing exactly how long a failover would take, and what it would cost is another opportunity to document emergency processes and can prevent you from being blindsided during a disaster.

- **Preventative Controls:** All the steps leading into the determination function help build a better picture of cybersecurity protection needs. In addition to recovery, aiming to decrease the likelihood of errors before they occur increases resilience. Determining what security practices or tools—such as scheduled patching, multi-factor authentication, layered security at each endpoint, dark-web monitoring, network access controls, file encryption, air-gapped backups etc.—helps determine if the organization need to fortify its data.

4. **Testing & Evaluation:** Ensuring that your DR Plan is comprehensive, accurate, and current is just as important as making one. Organizations make investments and changes in their IT and business processes at least every year, and their plans need to reflect that. The following are tips for having thorough and productive tests:

- **Timing:** Recovery drill testing should be administered on days when all relevant personnel are available and won't be pulled away by operations.
- **Document:** Each step of the test should have the *time to complete* logged, along with any hang-ups that were experienced.
- **Sectioning:** Depending on the size of your organization, it will likely be impossible to complete the full scope of the DR Plan testing in one day. Segment different aspects and test in pieces.

Invest in your organization by dedicating the time, money, and personnel to create a DR Plan. 3PL and trucking companies need to think of cyber resilience as a recovery effort more than ever due to growing cyberattacks and modern supply chain disruptions. A DR Plan will help fill the gaps of cyber resilience and answer questions that business leaders, IT administrators, general employees, and customers will have when your organization experiences a disaster.

RenovoData is a leading cloud backup and disaster recovery planning company and DR/BC planning service provider helping companies protect critical data worldwide. For more information and guidance, please call toll-free at 877-834-3684, reference our website at renovodata.com or email us at info@renovodata.com

**Best Lawyers
LAW FIRM
OF THE YEAR
USNews
TRANSPORTATION LAW**

100+ FREIGHT INTERMEDIARIES CAN'T BE WRONG

Over the years, Benesch has provided legal consultation and pragmatic business advice to well over 100 Transportation Brokers, Surface Freight Forwarders, Ocean Freight Forwarders, NVOCC's, Air Freight Forwarders, Warehousemen, 3PLs, 4PLs, and other Freight Intermediaries of all kinds. They know that when it comes to corporate structuring, mergers and acquisitions, transportation and logistics contracts, best practices, regulatory challenges, insurance and risk management, freight loss and damage or freight charge disputes, catastrophic personal injuries, and independent contractor relationships — **Benesch knows Intermediaries.**

Benesch Counsel for the Road Ahead®

*Benesch received the distinction of being named **Transportation Law Firm of the Year** by Best Lawyers®—Best Law Firms in 2022, 2020, 2017, 2016 and 2014. Only one law firm per practice area in the U.S. receives this recognition each year, making this award a particularly significant achievement.*

www.beneschlaw.com

Celebrating Cyber Awareness

Graham Gonzales | RELIANCE PARTNERS



SONG_ABOUT_SUMMER/SHUTTERSTOCK.COM

OCTOBER IS CYBERSECURITY Awareness Month, which has never been more applicable to the transportation industry than it is today.

The digital world hasn't been as kind to every industry. There was never an invitation for the transportation industry to join, though it was pushed in this direction as transportation technology players continued to emerge. A

historically manual industry took rapid steps towards modernization. The speed at which Transportation Management System (TMS), load board, Electronic Logging Device (ELD), visibility, and other necessary tools became common

in the hands of transportation companies only made sense. There is a clear shift from the manual systems which built the 3PL's role in the supply chain to the rise of the modern 3PL that may operate more efficiently.