Recovery Strategies vs. Recovery Solutions: Are Yours Aligned?

Chuck Cook | RENOVODATA

CARLOS AMARILLO/SHUTTERSTOCK.COM

TECHNOLOGY DISASTERS COME in many forms, from malware attacks to weather events, some due to human error and some from natural disasters. Some might argue that these disasters are unique, but all are highly time-sensitive because financial losses continue until operations are substantially restored.

Because of their dependence on accurate and high-speed workflows, 3PL and trucking companies incur significant losses when a disaster shuts down their operations. They simply cannot afford the interruption of current business or the lost opportunities from IT outages or data loss. Unfortunately, many of these same companies have either inadequate recovery strategies or none at all. Let's break it down from the basics to what should be included in every 3PLs recovery goals.

The Difference Between Solutions & Strategies

- In simple terms, a Disaster Recovery Strategy or Disaster Recovery Plan is a business plan that describes the objectives and outlines the procedures required for business operations to be resumed quickly after a disaster. An effective response to IT disasters begins with a strong recovery strategy. The disaster recovery plan also influences the recovery solution(s) implemented with the goal of minimizing the impact of a disaster and the time required to recover.

Importance of Having a Recovery Strategy

- Depending on your location and other factors, some disasters are more likely to impact your organization than others. Therefore, you should conduct a Risk Assessment to better understand which risks are most likely for your organization, so you can apply your valuable time and resources effectively.
- Readiness can only be accomplished with a sound recovery strategy. Quick and productive responses to disasters can make the difference between a company's success and its collapse.
- Even seemingly minor shutdowns can cause severe damage. Sometimes it is your reputation that is damaged, which impacts you long after the event occurred.
- Customers and prospects are requiring their vendors to be ready for fast recovery. Increased sophistication on the part of customers means that a well-developed recovery strategy is a significant benefit to winning the confidence of new customers.
- In many industries, a demonstrable recovery capability is becoming a regulatory requirement. The ability to respond quickly to crises and events is a sign of professionalism and stability.
- Without a well-designed recovery strategy, relationships with customers, vendors, and other allied organizations can take a beating. No company can afford to alienate those they do business with. It's not merely the potential damage caused by an IT shutdown. Organizations are judged by how they respond to all disasters.

A THOROUGH **DISASTER RECOVERY PLAN** IDENTIFIES THE STEPS **NECESSARY** TO **ACHIEVE OPTIMUM RESILIENCY,** YET THE VAST MAJORITY OF SMALL TO MID-SIZED 3PLs HAVE EITHER **INADEQUATE PLANS** OR **NONE AT ALL.**

FIREOFHEART/SHUTTERSTOCK.COM

A Strong Recovery Solution Is Based on In-Depth Planning

- A thorough disaster recovery plan identifies the steps necessary to achieve optimum resiliency, yet the vast majority of small to mid-sized 3PLs have either inadequate plans or none at all.
- The best plans are useless if they gather dust on a shelf. Revisit your plans regularly, keep improving them, and be sure to use them.
- With so many factors in the mix, disaster recovery plans are different for every company. Be sure your recovery solution is focused on the most critical aspects of your operations.
- Ensure that you have backup technology in place that lives up to your recovery goals. If data is permanently lost or corrupted, recovery will be incomplete.
- While systems are out of service, work is stopped, and the devastation piles up. The better your plan, the faster your recovery. Damages include:
  - Continuing expenses – Your company's expenses continue, often at an increased speed, while income-producing activities are stalled.
  - Contamination and loss of data – Downtime corrupts and destroys files, impacting present and future operations. Worse yet, a disaster can harm your customers' data.
  - Injury to reputation – If operations stay down for long, your customers will lose confidence in you.

An Effective Recovery Strategy Contains Key Elements

- Establish your recovery team. Determine who does what and when they need to do it.
- Estimate downtime costs. Understanding your cost of downtime helps determine your recovery objectives and budget.

VITALII VODOLAZSKYI/SHUTTERSTOCK.COM

- Establish the essential goals of your recovery strategy, specifically:
  - The Recovery Point Objective (RPO), which is the point in time (in the past) which a system or application can recover including how much data must be recreated due to an outage or disaster, and
  - The Recovery Time Objective (RTO), which is the length of time an organization can tolerate a system or application being down without causing major damage.
- Inventory your systems and applications. Include every hardware and software item, and don't forget your cloud apps because any of them could spark a disaster. Put the inventory into a regularly updated spreadsheet or table and make it available to key team members.
- Identify and safeguard critical product information (specifications, manuals, contracts, etc.). Maintain relationships with vendors, so that they will know you and your system and you will know them. Archive articles, commentaries, and reviews regarding your hardware and software products.
- Categorize your data and supporting IT systems and infrastructure. Factors include:
  - Importance of the data to business operations,
  - Difficulty of replacing specific data,
  - Sensitivity and confidentiality of the data, and
  - Regulatory requirements of the data.
- Make internal communications a priority. Employees need to be informed as soon as a disaster is detected, and a formal communications system should be prepared in advance. Alternate communications should be available, and everyone needs to know when and how to switch to alternate platforms.
- Crisis Communications. If a disaster occurs, consider if you need to issue an official corporate statement on company websites and social media. Much of the information required for a statement can be prepared in advance, ready for specifics to be filled in. Resist the impulse to cover up or minimize the event, and do not promise a better outcome than you are likely to deliver. Release updates of your progress, and if events undermine an announced recovery response, get the news out ahead of the grapevine.
- Be prepared to evacuate. Have a safe alternate site ready. If your site is impacted, consider who can work from home or if you need a workspace for specific people, systems, and equipment.
- Cross-training multiple people minimizes the risk of your recovery success contingent upon a single person.
- Schedule regular recovery drills. Even the best disaster recovery plans can have unexpected problems, such as an absent employee, an internet problem, or an unfamiliar new app. Test recovery functions at least quarterly. Remember that failing a test is not bad, since it uncovers problems and prompts

improvement. However, failure to test is a dangerous mistake.

Recovery Solutions Are the Engines That Do the Work

After a recovery strategy is established and detailed planning is nailed down, current solutions can be measured against the recovery objectives. If required, new solutions can be put in place to help you achieve your recovery goals as outlined in the strategy.

Evaluate Your First Lines of Defense

Firewalls, passwords, and antivirus are the system's gatekeepers. Competent passwords cost no more than a few minutes to create, and any number of websites offer tried-and-true formulas for stirring creativity. There is no shortage of firewall and antivirus packages, but they are not created equal. Expert online advice and publication reviews are helpful as well.

Backup Methods Should Fit the Company's Needs

The speed with which your data and systems can be restored is crucial in limiting the degree of harm your business incurs. Therefore, the specifics of your disaster recovery implementation should be chosen according to your plan, with special emphasis on your recovery objectives. Without fast, reliable, and efficient data protection, loss of data and damage to systems can blow a hole in a company's IT operations. Powerful backup solutions that match the company's requirements are the key, and there is a wide range of available tools which offer specific strengths.

Consider These Features When Evaluating a Recovery Solution:

- OS recovery tools are the ultimate guardians of your onsite or hosted data and systems. Many backup products defend against data loss but often do not protect their operating systems. Rebuilding an OS from scratch can be a time-consuming process, delaying your company's ability to get back to work.
- Offsite backup with local storage options enables companies to have rapid recovery from the local repository and offsite backup for protection against site loss or data corruption issues.
- Dedicated recovery servers provide strong protection for your onsite servers. Pristine local copies of backup files, databases and server images are safely stored, and provides the ability to "boot up" server clones until your primary hardware is restored or replaced. The result is rapid recovery from hardware failure with dramatically reduced downtime.
- Disaster Recovery as a Service (DRaaS) solutions, whether implemented to your secondary site or via a cloud provider, offer data replication tools and Wide Area Network (WAN) optimization to provide resiliency whether the problem comes from a hardware failure, network outage, or disaster affecting your site. Having a pre-built recovery environment with the ability to initiate a failover in minutes delivers constant system availability and is the best solution.
- Cloud-to-cloud backup tools house data and important software transferred from one cloud vendor to another for an added layer of safety. This eliminates the risk of a cloud vendor becoming a single point of failure.
- Email message continuity capabilities ensure that communications never disappear, even when servers go down, or during a power or cloud vendor outage. This helps prevent employee downtime, lost revenue due to customer frustration, and potential regulatory and legal problems.

SCHEDULE REGULAR **RECOVERY DRILLS.** EVEN THE BEST DISASTER RECOVERY PLANS CAN HAVE **UNEXPECTED PROBLEMS,** SUCH AS AN **ABSENT EMPLOYEE,** AN **INTERNET PROBLEM,** OR AN **UNFAMILIAR NEW APP.**

A central concern is how well the particular components of your disaster recovery solution work with your existing systems, each selected for maximum productivity and interactivity. Every component should be regularly monitored and tested to ensure proper performance.

With COVID-19 still affecting many of us, disaster recovery must be revisited to ensure it is aligned in the new normal environment. Companies that manage the turbulence well can emerge from this crisis stronger and more dynamic than ever. And that can only be done with outstanding disaster recovery programs in place that align with your strategy.

Don't Hesitate to Seek Expert Help

Many organizations, 3PL and trucking companies among them, react to the threats of malware, weather events, human error, and other causes by installing backup and recovery tools without careful planning. This can result in disappointing disaster recovery results which impact your bottom line. The better path combines outstanding disaster recovery strategy with superior recovery tools, all aligned with your recovery goals.

Chuck Cook, CBCP, is President of RenovoData. For more information and guidance regarding disaster recovery, call toll-free at 877-834-3684, reference our website at www.renovodata.com, or email us at info@renovodata.com.