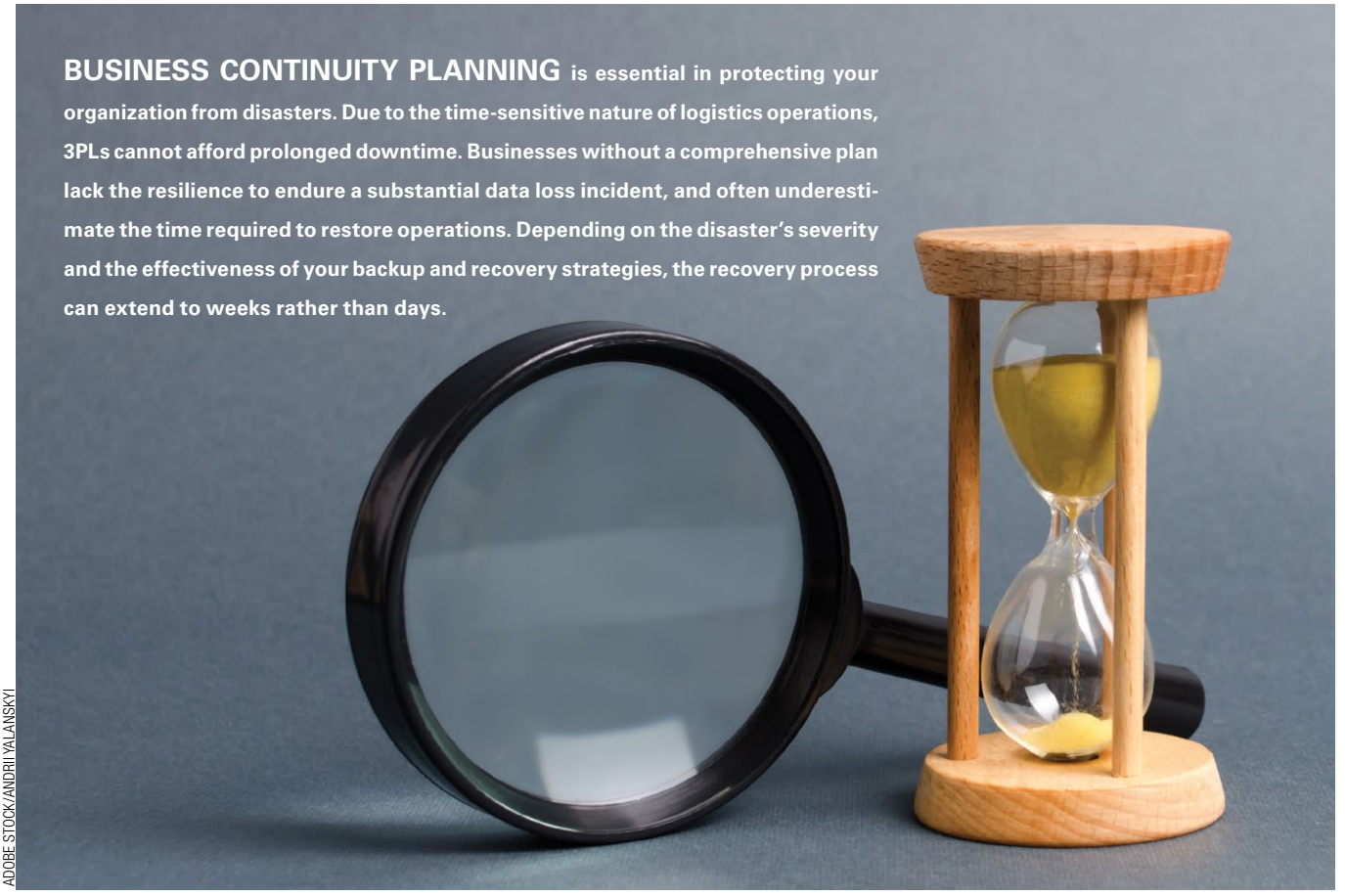
3PL PERSPECTIVES
THE THIRD-PARTY LOGISTICS MAGAZINE A TIA PUBLICATION
JULY 2023

Charting a Course for Success: Leaders in Logisitcs

TIA TRANSPORTATION INTERMEDIARIES ASSOCIATION
CENTER OF THE SUPPLY CHAIN

The Race to Reduce Downtime

Chuck Cook | RENOVODATA



BUSINESS CONTINUITY PLANNING is essential in protecting your organization from disasters. Due to the time-sensitive nature of logistics operations, 3PLs cannot afford prolonged downtime. Businesses without a comprehensive plan lack the resilience to endure a substantial data loss incident, and often underestimate the time required to restore operations. Depending on the disaster's severity and the effectiveness of your backup and recovery strategies, the recovery process can extend to weeks rather than days.

ADOBE STOCK/ANDRII YALANSKYI

Once a data disaster takes place, every minute of downtime is a threat to your organization. The confidence of customers, employees, and investors is shaken, and your reputation is in question. To safeguard your business from irreversible damage, it is crucial to respond swiftly and thoughtfully. Without adequate preparation, you run the risk of enduring irreparable harm.

A recent statistic showed that 40-60% of small and medium-sized businesses that suffer a malware attack without a comprehensive disaster recovery plan shutdown as a result. Strategizing and planning for rapid recovery of data is a key responsibility of IT managers and the organization's executive suite.

Potential downtime suffered and disaster recovery capability are influenced by several factors. The initial – and instrumental – measure is to implement secure offsite backups for your most critical files and systems. Beyond this, dedicated recovery servers and onsite data protection can significantly bolster your business continuity strength and recoverability. Molding these tools and services into a dynamic recovery strategy provides a blueprint for operations to consult and lean on to proceed through a disaster with minimal fallout.

Emergency response planning saves IT leaders the undue stress of responding

to disasters on the fly and saves businesses the risk of lost revenue. By anticipating and preparing for worst-case scenarios, essential operations are protected, and leadership is equipped with actionable steps to maintain composure and make informed decisions.

Can your business afford the fallout of downtime? Take all the internal and external factors into account and evaluate the disruption a disaster would have on operations. Without encompassing recovery and continuity blueprints in place, your business is exposed to the potential for substantial revenue loss and irreparable harm. Be proactive. Create plans that can effectively mitigate risks and enhance the resilience of your business.

Ensuring that your recovery solutions are aligned and well-prepared prior to a disaster is crucial for minimizing risk. By proactively aligning these solutions, you can effectively reduce the potential impact of a disaster and expedite the recovery process.

Balancing Act: Managing Time and Expense

In the result of a disaster, 3PL's don't have the luxury of being able to wait for replacement infrastructure to be purchased, shipped, and installed due to multiple clients being dependent on the company's operational uptime. Preparing for a breadth of disaster scenarios can minimize the delay in operability.

Vendors and partners in the continuity space can provide emergency hosting of your machines if your data center, headquarters, or network has suffered an attack or is otherwise unavailable. Partners who have been replicating your data are able to boot up a server clone and minimize the downtime while you look to replace your server.

Data disasters can be caused by several threat vectors, but the potential consequences are unchanging. Regardless of the cause of data loss or systems failure, the recovery process is inherently filled with uncertainty. Manage your user's response and reduce fallout by preparing and building response processes. Considering the high stakes involved, it is unwise to postpone preparations until such an event occurs.

Here are some of the business components threatened by disaster:

- Facilities
- People
- Communications
- Equipment
- Operating Systems
- Data

A comprehensive business continuity plan will address each of these components and will involve training that aids staff in becoming familiar with how to proceed. This plan details how to prevent or rapidly recover from a significant disruption and to resume business operations. Educated staff will then have a better understanding of what key employees do, when, and how.

One Component of Disaster Recovery are Data Backups

A recent statistic shows that 96% of companies with a trusted backup and disaster recovery plan were able to survive ransomware attacks. While 93% of companies without any Disaster Recovery strategy in place who suffered a major data disaster were out of business within one year. In today's business landscape, data serves as the foundation for nearly every organization. Protecting data and preventing business downtime will remain an ongoing challenge, particularly with the increasing number and sophistication of ransomware attacks. Looking ahead, it is crucial for businesses to adapt and find effective strategies to counter these evolving threats. It's estimated that downtime costs average $1,467.00 per minute or $88,000 per hour, according to Veeam's 2022 Data Protection Trends Report.

Strategic Planning: Key to Business Continuity and Mitigating Costly Disruptions.

It's not a question of if your business will be affected by data loss – but when. Given the multitude of potential threats to data security and the increasing reliance on multiple servers and applications, it is crucial to commence preparations for recovery long before a disaster occurs. Waiting until a disaster strikes leaves businesses vulnerable and ill-prepared to respond effectively. By proactively preparing for recovery, organizations can enhance their resilience and minimize the impact of potential disasters on their operations.

A crucial aspect of effective preplanning is the identification of vital systems, servers, and applications for business operations – and distinguishing them from less critical ones. It is essential for your organization to conduct an accurate inventory of critical applications and data, and subsequently establish your recovery priority. This ensures a coordinated and efficient response in the event of a disaster.

Establish your Recovery Objectives

The heart of pre-planning is your company's Recovery Time Objective (RTO). This is the length of time you've identified that your business can endure without a critical system or data before exceptional harm takes place. The RTO will help determine how often a Recovery Point (RPO) should be scheduled – an exact frequency of time files are backed up and available for restoration by a system or application if necessary.

Depending on the organization's requirements, a daily backup schedule may suffice for some, while many 3PL's may require more frequent backups, such as hourly or continuous protection that replicates the constant influx of real-time processing, tracking, and reporting. After determining the backup frequency, it is essential to consider the impact on different aspects of your operations and anticipate the specific needs of each. These areas can be logically grouped into the following categories:

Recovery Workspace Essentials

Facilities – Consider how your business will proceed if your physical servers are damaged by a flood, fire, hurricane or tornado, or other natural disaster. Having an alternative for your physical sites will minimize downtime. What's your plan for a temporary workspace that your users will connect to? By identifying and securing appropriate space, you ensure that critical operations can continue smoothly, even in the face of a disaster or disruption.

People – To ensure smooth operations with minimal disruption, it is crucial to educate management well in advance. Department heads should be well-versed in the steps to follow and how to maintain daily operations during a crisis. Additionally, considering the added complexity of supporting a remote workforce, it becomes essential to address the unique challenges associated with remote work in the disaster recovery plan. Conducting data disaster drills is a valuable practice to consider. These exercises challenge employees to make quick decisions and reinforce appropriate choices. They serve to test the effectiveness of your disaster recovery plan and identify areas for improvement. Regular testing and evaluation allow your plan to adapt to evolving needs, ensuring its ongoing effectiveness in safeguarding your business.

Continuity for Communications

Communications – How can key employees communicate via email or server-based communications if these systems are unavailable? Identify a contingency plan that ensures key personnel have internal contact information such as telephone numbers as a backup. This sounds obvious but think about how many individuals and corporations now rely on web-based platforms for phone contact.

Protecting Operating Systems

Operating System – Safeguarding your operating systems for servers and PCs is of utmost importance to minimize downtime.

SAFEGUARDING YOUR **OPERATING SYSTEMS** FOR SERVERS AND PCS IS OF **UTMOST IMPORTANCE** TO **MINIMIZE DOWNTIME**.

Implementing solutions like Bare Metal Backup, Virtual Machine backups, and server replication can significantly reduce the time required to rebuild Operating System Environments (OSEs). It is crucial to recognize that every company has slightly different Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). Therefore, it is beneficial to mix and match snapshot and log-based replication solutions based on the level of criticality. This approach helps protect your operating systems, critical hardware, applications, and data during the recovery process, effectively mitigating your organization's risk.

The Ability to Recover with Data Backup

Maintaining frequent backups on a regular schedule is essential for your business. By establishing and consistently maintaining timely backups of data, you can significantly reduce the potential impact of data events. Treating data recovery as a critical business planning responsibility is crucial in safeguarding your operations from stressful and potentially costly data failures. Taking proactive measures to protect your data ensures business continuity and minimizes the risks associated with data loss.

While it is possible to undertake data protection and recovery planning on your own, it is advisable to seek the expertise of specialists in this field. Protecting and recovering data files requires specialized knowledge and experience.

Working with a trusted partner who specializes in data protection and recovery can provide valuable assistance and advice throughout the process. When engaging a partner, it is recommended to seek their assistance and guidance in each of the following steps to ensure the most secure and optimal outcome for your business:

- To develop an effective strategy that prioritizes quick recovery of data and protection, it is crucial to enlist the help of your team. Involve leadership, management, and team members in the process to ensure alignment and comprehensive input.
- Establish Recovery Objectives and define the success parameters of an effective recovery and make sure your planning addresses these appropriately.
- Install effective backup. Establish a timely and secure backup protocol for creating duplicates of critical files, especially those without which you would find it difficult to remain in business – such as financials, tax records, inventory, jobs currently in process, operational protocols, etc.
- Choose solutions that align with your overall strategy. You can begin with a simple plan of action that outlines the necessary recovery steps and assigns responsible individuals for each task. However, to make your plan more robust, consider assembling a task force internally.
- Seek expert help. Consider appointing an expert who can explain and work through your needs, explaining in layman's terms how your recovery plan can be most effectively executed. If the steps outlined above seem a bit daunting, please know that you're not alone. Recovery planning is an important task for every business.

Time is of the essence when it comes to restoring critical IT services after a downtime event. Investing in the evaluation of all the components that would be affected by a disaster or data loss event in advance, coupled with having the correct recovery solutions in place that meet your company's Recovery Objectives will minimize your company's downtime.