Disaster Recovery: Time Is of the Essence

Chuck Cook, CBCP | RENOVODATA

YOUR DATA IS both your most valuable asset and the one most likely to be damaged or lost. While this is true for any enterprise, the fast pace and volume of 3PL and trucking companies' data generation make them even more vulnerable than most operations.

In the event of a disaster, the speed with which your data and services can be restored significantly limits the harm to your company. As long as your system is down, the cost meter keeps running, so recovery time must always be a central concern.

How long you can afford for each component to be down? This includes databases, software and hardware, email, ancillary devices and operating systems.

A potential outage might be measured in hours, days, or even weeks, so your plan should cover everything that could influence or be affected by a shutdown. The plan should encompass areas in addition to data backup and disaster recovery. The goal is to ensure business continuity.

Misconceptions about disaster recovery time abound, and this can have dire consequences for 3PL and trucking companies of any size. Here are the most pervasive myths.

- **A certain amount of downtime is OK.** Even small outages cost money, so the time that operations are suspended is a top issue. Aim for zero outages.
- **With disaster recovery tools in place, speed isn't all that important.** Any event, however minor, that shuts down a system can become a major problem if it is not corrected promptly. Having tools is one thing, but being able to use them quickly and effectively is another. Minutes count.
- **Rapid-recovery tools are too expensive.** The cost of fast and thorough recovery could be dwarfed by that of a single disaster. What's more, wise choices that fit your operation can lower expenses substantially.
- **Our company rarely suffers long-lasting outages.** Disaster can strike any 3PL or trucking company at any time. Today's cyber threats can take down an entire network with one wrong click of a user's mouse. It only takes one such accident to severely cripple your organization.
- **The length of downtime we might experience would not harm our customers.** Even if a company's outages are brief, customers can often detect them with relative ease. Moreover, more companies now demand swift and

flawless service. Again, having tools is one thing but being able to use them quickly and effectively is another.

- **We do not need disaster recovery capabilities because we have solid data backup.** Data backup is an important part of disaster recovery, but the two are not the same. Restoring data from backup is just one phase in the disaster recovery process. No backup method is perfect because problems such as software glitches, unexpected interruptions, and human error can always occur.

10 Key Time-Sensitive Tasks for Optimizing Your Disaster Recovery Plan

- **Create a Business Impact Analysis (BIA).** The BIA will identify your company's most vital systems and processes as well as the effect an outage would have on business. The greater the potential impact, the more money your company should consider spending to restore that aspect (whether a system or process) quickly. In short, a BIA helps companies set a restoration sequence to determine the order in which critical systems and processes should be restored.
- **Develop and practice a contingency plan that includes a succession plan for your executives.** These are your most basic questions:
  - How much will your downtime cost you?
  - What do you want to protect your business against?
  - What do you want to protect?
  - What do you do once a disaster or issue arises?
  - Test the plan, then manage.
- **Keep it real.** While you do not want to traumatize your staff, making business continuity exercises realistic gives you essential insight into how an individual may potentially react in a stressful situation.
- **Get to know your local first responders.** They will do a better job if they know your people and your business.

IN SHORT, A BIA **HELPS** COMPANIES **SET A RESTORATION SEQUENCE** TO DETERMINE THE ORDER IN WHICH **CRITICAL SYSTEMS** AND **PROCESSES** SHOULD BE **RESTORED.**

- **Train employees at every level to perform emergency tasks.**
- **Develop crisis communication plans for top executives and senior staff.**
- **In case telephone networks go down, invest in alternate means of communication, with emphasis on external and internal email and chat.**
- **Perform regular data recovery drills.**
- **Test your business plan regularly.**
- **Evaluate your company's performance truthfully and re-evaluate it from time to time.**

Elements of Recovery

The disaster recovery process touches many areas of your organization. Here are the main components.

Facilities

No location is immune to disaster, whether the threat is fire, earthquake, weather, or other natural or manmade devastation. The same is true for major hardware failures and network outages.

Cloud solutions or Disaster Recovery as a Service (DRaaS) capabilities virtually eliminate such risks. Total offsite duplication enables companies to keep going whatever disaster may befall the primary location.

This requirement can be a stretch for 3PL and trucking companies, so it pays to examine available solutions and their costs. This is an area that is especially likely to require expert assistance.

People

You can have the best possible disaster recovery technology, but if your employees are not active participants your security suffers. Everyone in the company should know what to do and how to do it.

Your staff should be well-versed in disaster-related duties as well as the policies behind them. Regularly scheduled training and drills ensure that everyone is always up to speed.

Restrictions may need to be placed on an individuals' access to critical data, and everyone should understand the reasons for those restrictions.

Communications

Procedures should be in place to immediately notify the entire organization when a disaster has struck and that they must switch to safe platforms and take well-rehearsed actions to combat and mitigate the damage.

Also, it is imperative to have text prepared in both electronic and paper form, so that you can quickly inform your customers, allied businesses, and other concerned entities that you have a problem and are dealing with it. And by all means, be honest.

Disasters can hurt mainstream communications, especially when malicious insiders attack telephones and other internal media. Alternatives such as cloud-based telephone systems ensure that critical information keeps flowing.

When disasters occur, email must be preserved. Without it, lost revenue, employee downtime, customer dissatisfaction, and potential legal or regulatory problems are likely. Protecting cloud email means backups out of that cloud to another location.

The best defenses against insider sabotage and human error are solid communications, employee education, and thorough training.

Equipment

Pay close attention to potential system and application failures.

- **Take an inventory and document all systems and applications.** You need to fully understand every element because the failure of even one could bring down the whole system. Include every hardware and software item since any of them could be involved in a disaster. Inventory your systems and applications and become familiar with product information available from your vendors. Put the inventory into a regularly updated spreadsheet or table and make it widely available at all times. Be sure to ask these questions:
  - What is the recovery priority of each item?
  - Have business needs changed since each item was installed?
  - Are all new applications properly protected?
  - How are new servers or hardware protected?
- **Include in your plan the order in which you want your systems to be restored.** Divide them into two or more levels of time sensitivity, separated in terms of importance versus urgency. Which ones do you need to be operable as rapidly as possible and which ones, though important, can remain inactive for a while without causing too much damage?
- **Keep all vendor-supplied product data (specifications, manuals, contracts, etc.) on file, and enable employees to become familiar with these documents.** Maintain relationships with vendors, so that if and when you need their help, they will know you and your system, and you will know them.
- **Familiarize yourself with your Service Level Agreements (SLAs).** Make certain that your vendors are contractually obligated to lend assistance if the need arises. SLAs should cover the full range of disaster contingencies. They should stipulate that work should commence and be completed within a certain time. If necessary, strengthen your SLAs at once.
- **Determine potential infrastructure vulnerabilities.** Your servers, routers, and switches are subject to cybersecurity attacks. Because 3PL and trucking companies can have many items connected to their systems, extra care is recommended to make sure none of them are overlooked.
- **Look for software weaknesses.** Hackers know which outdated packages and plugins have easily exploited flaws, so you should keep up with all software updates, taking care to uninstall older versions. Newer editions can be extremely helpful because of bug fixes and the addition of security features.
- **Identify single points of failure.** These are parts of a system that are without redundancy and can include hardware, software, apps, small devices, and even people that need to be duplicated. It is especially important for 3PL and trucking companies to be certain that every single system-connected gadget that company employees use are updated.
- **Internet of Things (IoT).** Do not overlook entry pathways created by endpoints such as smartphones, tablets and other small devices. These are easy for hackers to penetrate, and once in, cybercrooks can see what each device contains and use weaknesses to plant malware and steal data.

ISTOCK.COM/KOYA79

- **Operating systems.** These keystone elements of your installation have special areas of vulnerability, especially when the same operating system is used for multiple computers, as is often the case for 3PL and trucking companies. If that is the case, an attack on one could easily move to others.
- **Physical servers.** If you experience a disaster and need to perform a "bare metal recovery," which requires locating another server, loading an operating system that is an exact match with the one you have been using, installing applications, and then restoring data creates downtime which can balloon to company-killing proportions. However, with a permanently installed duplicate clone of your server and operating system, recovery can be swift and sure.
- **Affordable, effective solutions are available.** With a cloud disaster recovery capability in place, operating systems, applications, and data are fully protected, even if the physical plant is compromised. Alternatively, an in-place recovery server stores local copies of your backup files, databases and server images.
- **Evaluate each critical system and application to see how long you can keep going if it is disabled.**
- **Look for viable workarounds for when critical systems go down.**
- **Identify the systems that, while they may not be the most important, are best able to help you through a period of downtime.**

HAVING **TOOLS** IS ONE THING, BEING ABLE TO **USE THEM QUICKLY** AND **EFFECTIVELY** IS ANOTHER. **MINUTES COUNT.**

While well-planned disaster recovery protects entire systems, its core objective is to defend the company's data, ensuring that important material will not slip through the cracks.

Don't hesitate to ask for help. For 3PL and trucking companies, building a comprehensive, effective disaster recovery program that moves at high speed is a tall order. It requires expert knowledge of baseline technologies, the best and latest products and methods, the types of disasters that can take place, and the most efficient means of overcoming them. You can have high-end disaster recovery solutions at a reasonable cost, but it takes concentrated effort and thoughtfully chosen guidance.

And remember, there is no time to waste.

Published by Chuck Cook, CBCP, President, RenovoData. For more information on how to develop a thorough, fast-reacting disaster recovery capability, call toll-free at 877-834-3684, reference our website at renovodata.com, or email us at info@renovodata.com.

2021 *CS-DTP

	**TIA	Non-TIA	Shippers
Jan.	91-35	89-37	73-44
Feb.	91-36	89-37	73-41
Mar.	90-33	89-40	73-39
Apr.	90-32	89-40	74-35
May	90-32	89-40	74-35
Jun.	90-33	89-39	77-33
Jul.	90-35	89-39	74-34

2020 *CS-DTP

	**TIA	Non-TIA	Shippers
Jul.	91-34	88-45	73-43
Aug.	91-35	88-43	73-44
Sept.	91-34	88-44	73-44
Oct.	91-35	88-44	73-45
Nov.	91-37	89-43	73-45
Dec.	91-37	89-42	73-45

Freight Payment Index

Since 1987, TransCredit has produced credit reports exclusive to the trucking industry. Compiling data on how freight bills are paid, they offer a widely accepted CreditScore and Days-To-Pay™ trends that are posted on most load boards throughout the USA and Canada.

TRANSCREDIT

*CS= Credit Score, DTP = Days-To-Pay™
**TIA = Composite rating of TIA Membership
Non TIA = Rating of over 11,150 Non-Member Intermediaries
Shippers = Ratings of over 398,700 truck-load shippers