Protecting Your Data in a Changing Data Landscape

Fundamentals of Data Protection, Recovery Planning & Business Continuity for 3PLs

Chuck Cook | RENOVODATA

BLUE ANDY/SHUTTERSTOCK.COM

Every Organization Is Vulnerable

For most organizations, 2020 was filled with uncertainty, unease and turmoil brought upon by the COVID-19 pandemic. Unfortunately, cybercriminals were still able to identify vulnerabilities and attack businesses relentlessly throughout the year. The following statistics reflect data about 2020 cyberattacks and disaster recovery planning:

- 400% increase in U.S. cyberattacks per day since the pandemic began.
- 84% of companies in the U.S. have been impacted by a cyberattack.
- More than 90% have been damaged by technical disruptions, with more than half experiencing four or more such events.
- 93% of companies that suffer a major data loss without a Recovery Plan (RP) in place are out of business within a year.
- 40-60% of small businesses that lose access to operational systems and data without a RP close their doors forever.
- 98% of companies with a Disaster Recovery (DR) Plan are able to survive a ransomware attack.

Owners & Management Must Lead the Way

Due to the higher frequency, impact, and media coverage, organizational awareness of cyberattacks is at an all-time high. Transportation companies and 3PLs should be particularly concerned due to operational dependence on speed, accuracy and 24-hour uptime. These factors rank the transportation industry among those most susceptible to costly server downtime, with 2020 research figures estimating an average of $7 million lost per hour. While 3PLs are being more careful, there is still a wealth of education that employees and management require to best defend themselves.

This begins with comprehensive Business Continuity Planning (BCP), which allows organizations to identify their business functions core to operations and plan how to continue in the event of a crisis. Once an organization has outlined the basics of their BCP, a DR plan is essential for accessing the required technology and infrastructure established to quickly resume business after a disaster. DR/BCP is not a "checkbox" that can be completed without updating these living documents as a company's IT environment and infrastructure evolve. The IT department will update and maintain these documents when relevant IT systems change and DR tests are completed, but both the DR/BC plan will serve as tools to be used by management. The integration of these plans calls for a culture change from management and ownership, ensuring that each employee has the tools and knowledge they need to react appropriately in times of disaster.

Where Is the Cloud?

Simply, the cloud is just a phrase used to describe offsite data storage that is accessible via an internet connection. There is no fluffy, white hard drive in the sky; it is just someone else's data storage facility. This means that data in the cloud can be just as vulnerable as data stored onsite, as it can also be subject to disaster. Signing a cloud storage agreement does not absolve your organization of responsibility, but instead, you incur the responsibility of understanding who owns the hardware, where it is located, and creating a DR/BC plan and strategy for what could go wrong. Jointly, for each change in your IT environment, it's imperative that alterations in people, software, and hardware are documented and accounted for in your recovery plan and shared with your cloud provider. Failure to plan is a plan to fail.

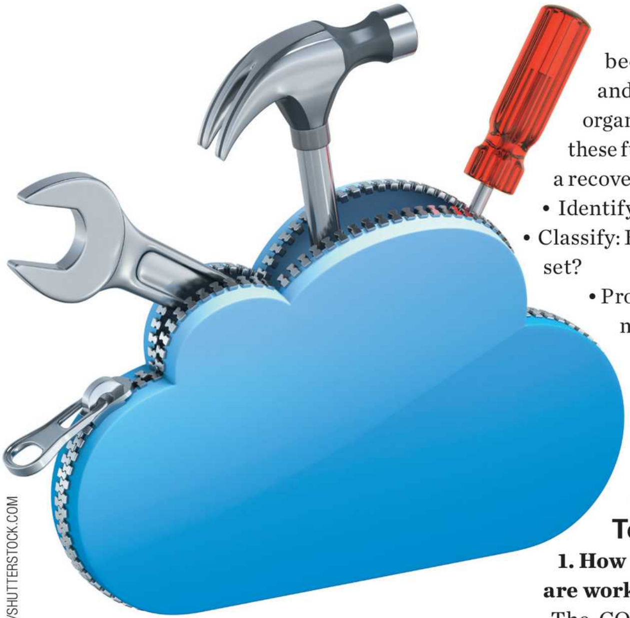
BACKUPS ARE **ONLY AS VALUABLE AS THE DATA** THAT RESIDE ON THEM. UNFORTUNATELY, YOUR BACKUPS ARE ONLY AS **USEFUL** AS WHERE **THEY ARE STORED.**

Backups STILL Matter

No matter the location of your data, multiple backups and Disaster Recovery as a Service (DRaas) are essential to your organization's recoverability. Malware and other viruses can breach your first line of defense (passwords, firewalls, and antivirus) and continue to spread across your network like wildfire. Your organization should be able to rely on offsite data backups to repopulate your servers with data that was removed from the infected network. Similarly, when investing in data backups—whether they are file backups or image backups—it is crucial to understand what the capabilities are of each solution. For example, do not expect to rebuild a computer operating system with file backups. Instead, understand a bare metal restore will need to take place which will take time and money. Here are a few examples of backup and recovery solutions and capabilities that 3PLs should consider.

- Offsite backup with local storage is an excellent first step towards data resiliency and protection. This allows organizations to recover files rapidly from the local repository, while still having offsite backups for restoration in case of onsite data corruption or entire site outage.
- Operating System (OS) recovery tools are the supreme protectors of onsite (or hosted) data and systems. Many backup products don't have this capability, but the benefit of achieving a reduced Recovery Time Objective (RTO) gained from not having to rebuild an OS from scratch could save your organization significant loss from operations.
- Dedicated recovery servers provide redundancy for your server hardware onsite. Backups are copied and safely stored on alternate hardware, providing the ability to put the clones online while primary machines are being replaced or restored. Dedicated recovery servers rapidly decrease downtime.
- 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.

Along with playing a critical role in recovering from a cyberattack, data backup and DRaaS technology can allow you to restore errors made by your most valuable asset—your employees. Social Engineering cyberattacks are more complex and frequent than ever, and accidents can happen. In the instance of accidental deletion, corruption, or even a malicious internal attack, data backups will save your organization time, money, and stress by recovering what was lost. Backups are only as valuable as the data that reside on them. Unfortunately, your backups are



MIPAN/SHUTTERSTOCK.COM

only as useful as where they are stored. For example, it would be great to have local data backups for the sake of rapid recovery, but if they are connected to the infected network, they will be useless in the time of a cyberattack. To prevent this, you will want to add an air gap between your local backup and your offsite data infrastructure, ensuring that there is a protected separate location in the cloud or otherwise to access your data.

Recovery Planning Fundamentals

A combination of best-in-class hardware and software to enhance the recoverability of your IT infrastructure is a great, albeit expensive, foundation. Conversely, recovery planning is not something you can purchase out of a box and implement. Recovery planning is a way to prioritize business-driven data requirements and help with documenting recovery strategies that meet your recovery objectives. Recovery plans can range from a simple yet precise action plan to building a secure secondary failover site if a disaster occurs. Regardless of the plan's depth, they demystify the recovery process and proceed to save time and money when disaster strikes because recovery, testing, and training documentation is organized and simplified. Follow these fundamentals when drafting a recovery plan.

- Identify: Where does my data live?
- Classify: How important is each data set?
- Protect: Apply budget where it matters most.
- Recover: Mitigate the impact of unexpected events.

Five Considerations for Today's 3PL

1. How many of your employees are working remote?

The COVID-19 pandemic forced organizations across the globe to establish a remote workforce presence. Many organizations are now considering leaning into the trend. Recently, a Gartner survey revealed that 74% of CFOs intend to shift some employees to remote work permanently. This could present a host of difficulties or new charges depending on your backup solution. It's imperative that remote users' work data is being backed up, regardless of where they are working geographically. If an employee is using a personal computer, which fails and isn't being backed up, the ripple effect caused by lost data could cripple operations, cause significant downtime and run up expenses.

Unfortunately, permitting access to company hardware, software, and data offsite presents a host of new security concerns as it pertains to the organization's data landscape. One way to help govern company data is by establishing an Acceptable Use Policy (AUP). An AUP is a set of rules established by an organizations' management and IT staff that dictates the way employees act with the company's data and network to create a more secure IT environment. For example, an AUP would include security standards for an employee's personal device that they use to access the company's data or network (i.e., a password protected screensaver automatically activated within 10 minutes).

In combination with backups and use standards set for remote workers, the data itself must be recognized as the company's intellectual property. All confidential information living on remote employees' machines must be fortified from bad actors and recoverable in a data loss event. Employees personal network security has become a liability to the employer with remote work, and it needs to be addressed through training, documentation and software.

2. What happens when your cloud vendor goes down?

It is estimated that roughly 90% of organizations now use multiple cloud vendors for storage and business applications. This has led to many companies building a dependency on their cloud that they're not necessarily prepared to counter in a vendor outage scenario. It is the duty of the organization to seek out the recovery plan used by their own vendor and ask some of the following questions.

- Are there georedundant backups in place in case of an outage at the primary site (cloud)?
- What kind of onsite redundancy do you have in case of a disaster (i.e. power, internet)?
- Do you have redundant recovery servers onsite in case of hardware failure?
- What is your work-around procedure if this cloud service is down?

3. What if your office internet goes down?

Internet availability often feels like it is at the whim of your Internet Service Provider (ISP), and out of your control. Today's 3PLs are dependent on internet connectivity for load management, and therefore the risk of costly downtime calls for contingencies and recovery plans. Management can choose to invest in: software that provides an additional network line for resilience, an uninterruptable power supply, which would provide battery power for the internet in case of an outage, or simply purchase extra equipment (i.e., routers and modems) to swap in case of failure. Another viable tactic is to simply subscribe to an additional ISP, providing an alternate internet connection in case of provider failure. There are plenty of examples of strategies that management can use to mitigate the impact of internet loss, but it's most important to preempt the disaster by establishing trust and recovery plans with your ISP.

4. How many clouds is too many?

Cloud services that were created to help streamline your operations are hard to resist, especially when there is a wealth of options that can solve any number of business inconveniences. The challenge when adopting multiple clouds is to use the products to improve your security posture, not endanger it. Diversify the allocation of your data, ensuring that your organization does not get caught with all its eggs in the same basket. Not every cloud is created equal. Some clouds only provide storage, while others bundle services such as options for emergency hosting. Elite cloud providers bundle expert assistance in integrating their solutions with other clouds, but the onus is on the user to oversee the process. This includes authenticating, credentialing, device evaluation, encryption and malware detection.

5. Can I backup my data out of this cloud?

Many organizations use a primary big-box cloud provider to store or backup the company's data. This is also an example of a single point of failure. When selecting a primary cloud provider, it should be assessed as to whether the software allows backup functionality to a different site or an entirely different cloud that the company can store low-cost backups within. Once the cloud has been adopted, regularly scheduled testing is vital. Testing doesn't just identify issues in your backup processes, but it also provides the most up-to-date knowledge about your system and its changes. Some cloud vendors charge additional fees for data transfers, restores and recovery testing, so management should factor in testing costs for the frequency in which they intend to evaluate their backup ability.

ALONG WITH **PLAYING A CRITICAL ROLE** IN **RECOVERING FROM A CYBERATTACK,** DATA BACKUP AND DRAAS TECHNOLOGY CAN ALLOW YOU TO **RESTORE ERRORS** MADE BY YOUR MOST VALUABLE ASSET—YOUR EMPLOYEES.

Five Lessons Learned from COVID-19

- Evaluate your data sets. Has your data landscape shifted? More remote users make for a more dispersed threat landscape. Is your organization ready to assume the liability of an employee's home network?
- Reevaluate your recovery plans and adjust. Your organization is not the same as it was in January 2020. What new locations, systems, or personnel will impact your current recovery plan?
- Assess all your tools, techniques and procedures considering current conditions. Ransomware attacks are not a rarity anymore. What is your roll-back capability if something goes wrong?
- Verify critical data is safe and being backed up. Are you familiar with how your cloud apps, on-premises apps and remote computer apps are being backed up?
- Educate users and keep heightened awareness of cyberthreats. Are your users adept at identifying modern phishing techniques? Have you established an AUP?

Reach Out to Data & Disaster Recovery Experts

3PLs and trucking companies suffered exceptional strain from the COVID-19 pandemic. Business is beginning to expand once more, and with it, the need for a fortified IT environment. It is vital that organizations allocate resources to cloud backups and recovery tools to offset the risk of natural disaster, equipment failure, or even a ransomware attack from impacting the companies' bottom line.

RenovoData is a leading cloud backup, disaster recovery 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 or email us at info@renvodata.com.

VOYAGER624/SHUTTERSTOCK.COM