Cloud Solutions Are Not Created Equal:

DIFFERENCES INCLUDE SECURITY, PRIVACY, DATA MINING, AND MORE

Michele Vayle | RENOVODATA

IN ADDITION TO virtually limitless data storage, cloud computing can offer higher speed, simple scalability, lower administrative costs, and more-efficient IT operations. Because 3PL and trucking companies rely so heavily on fast, maximum-performance systems, these are major advantages. But while all cloud vendors offer large-scale storage, there are significant differences between them.

LIGHTSPRING/SHUTTERSTOCK.COM

Your data belongs to you, but with some cloud providers it is not fully within your control. Some vendors are not in business to protect your data. When they offer cheap or free storage, they might secretly use your files for such purposes as the selling of your personal information or the mining of your data. These activities violate established good practices and regulations, but are common among some providers.

Because 3PL and trucking company IT operations must be reliable on a day-to-day basis, their cloud providers should demonstrate proven stability and a commitment to long-term goals. It is not unusual for tech companies to be sold, to change direction, or to be eclipsed by competitors. If such shifts overcome your vendor, your data could be damaged, compromised, or could disappear entirely, so you should be confident that such crises can be avoided.

To make the best uses of your cloud resources you need to ensure that your Disaster Recovery (DR) solutions meet the Recovery Point Objectives (RPOs) outlined in your DR Plan. This encompasses the protection of your data privacy and security by all available means. To reap the full benefits of the cloud at the lowest risk, join forces with trusted experts who have deep knowledge of current technology, understanding of regulations, and the highest ethical standards.

Planning

Cloud-based activities should be backed by a thoughtful DR Plan that ensures successful operations with a minimum of glitches, the anticipation of potential hazards, and consideration of future requirements.

Recovery should be a central element of the plan. Natural disasters, power outages, hardware failures, or data corruption due to viruses or malware are always possible. Who is responsible for system outages, data corruption, or cybersecurity events? Knowing "who" is responsible for "what" is essential. A crucial, but often-overlooked element is the involvement of all employees, including management.

With solid planning and vendor feedback, powerful recovery capabilities can assure that data loss is eliminated or reduced to a manageable level.

Encryption

Even with the cloud, it is important to safeguard data with more-advanced encryption than is provided by most vendors. Too many 3PL and trucking companies neglect to do this. Layers of complexity can be added to data encryption to prevent content from being read. However, this type of security improvement can actually make the system harder to use and may even cause elements to malfunction. You are well-advised to enlist expert guidance when seeking to optimize encryption without damage to overall functionality.

Also, be aware that when systems' web addresses are poorly protected, cyber-criminals are able to capture encryption keys, which exposes a company's data to plunder. To eliminate this risk, all IDs and passwords can be secured with relative ease.

Privacy

Not all cloud providers can be counted on to keep your data private. A close look at the details of any contract you would be asked to sign may unearth some disturbing details. Here are some examples. A provider may:

- Be allowed to share your data or information about your company with third parties.
- Have access to your system information.
- Be able to hand over to third parties statistical or other non-identifiable information about your company and your data.
- Hang on to your data for some time after you have asked for it to be handed over or deleted. This is illegal, but it happens.
- Share your data if required by law. Obviously, this exception has merit, but only if you are consulted in advance.

Such legal caveats simply mean that some providers will protect your property's privacy until they decide not to do so. If they can decrypt your data, they can dip into it at will with only their ethical standards to prevent them from doing so. Although there are steps other than encryption that you can take to make your cloud-housed data harder for a provider to access, such actions on your part may interfere with cloud-storage performance and your ability to use your data.

Security

Conscientious providers put your interests above their own, but not all cloud companies are so scrupulous. Dishonest operators can use your data for financial gain, either by selling it or otherwise exploiting its contents.

Here are some of the risks:

- Ineffective protection against security breaches, malware, and man-in-the-middle attacks
- False claims of solid security
- Sharing of data with unauthorized third parties
- Poor design
- Sloppy performance
- Slipshod procedures

Data Mining

Theft of information has become commonplace, and a similar but more subtle practice is unauthorized data mining, which is not theft in the conventional sense.

Data mining is the use of highly sophisticated algorithms to analyze large bodies of data in search of patterns and trends. For decades, analysis of data-mined information has been a helpful source of business intelligence, revealing connections between such elements as demographics, industry trends, climate, marketing, and price fluctuations. When properly used, it identifies and analyzes market behavior that might otherwise be invisible.

If performed in a legal and above-board fashion, whether using a company's own data or that of a cooperating organization, data mining is a useful tool. However, unauthorized mining constitutes theft of usage. For example, if your data demonstrates that a certain industry is going through changes that affect its trucking utilization, a competitor accessing your data on the subject without authorization would be stealing your hard-earned knowledge.

Conclusion

The main objective of cloud technology is to protect your data. Good cloud providers deliver solutions that enable full and rapid recovery from crises.

For safe and complete utilization of cloud technology, it is imperative for 3PL and trucking companies to work with trusted vendors to implement data protection and data recovery capabilities, as well as business continuity and DR Plans that fit the organization's needs precisely.

Michele Vayle is Marketing Director at RenovoData, a leading remote cloud backup and disaster recovery service provider helping companies protect critical data worldwide. For more information, call 877-834-3684 or log on to www.renovodata.com