The Cloud Can't Eliminate Your Responsibility for Data Protection

Michele Vayle | RENOVODATA

IN RECENT YEARS, the cloud has become a major part of the IT landscape, bringing many advantages. Besides virtually unlimited data storage, the cloud improves speed, availability and user mobility. In some cases, it carries significant financial savings as well, including cost cuts, on-demand capacity, and reduction of resources previously allocated to infrastructure and operations. For 3PL and trucking companies, where quickness and flexibility are always critical, the options cloud services offer are especially beneficial.

©ISTOCK.COM/RZELICH

Misconceptions

For all its improvements, the cloud comes with potential challenges, and the picture is further clouded by an array of erroneous beliefs. No surprise, since every major breakthrough comes with unexpected obstacles as well as gaps in public understanding.

One prevalent misconception is that the protections the cloud provides give license to relax established safety practices. One reason for this false sense of security is that in the past, companies' critical data and services were, to a great extent, safely contained within their own servers. Now, with the rise of cloud storage and increasing reliance on internet services, organizations present more-inviting targets and more points at which breaches can occur.

Human Error

Companies often blame the technology itself for difficulties with the cloud. More commonly, problems are the result of avoidable mistakes and failures to impose fundamental security procedures. Even with cloud implementation, protective measures are as essential as ever. Preventing basic blunders is as important as safeguarding the technical complexities.

Leaving the Door Open

Masses of private and commercial data can be made vulnerable merely because web addresses or an account has been left unguarded, enabling hackers to access critical systems or capture passwords and encryption keys. This is all they need to pillage an organization's data. Attacks of this kind can severely cripple companies, all because an essential bulwark has been ignored.

The solution is simple enough: every aspect of credential protection, every user ID and password must be made secure, with emphasis on every. Most companies using cloud systems may have, at one time or another, allowed potentially lethal exposure of their cloud-stored data due to careless credentialing.

Encryption

Experts believe that better than 50% of companies fail to encrypt sensitive data properly, if at all, even though the practice is considered a security imperative. Not surprisingly, the rapid pace of activity in 3PL and trucking companies can present challenges when it comes to implementing overall data encryption.

Conclusions

These are some of the vulnerabilities that the cloud cannot guard against completely. They may be hard to detect, and one crack in your defenses can spell disaster.

Clearly, the cloud has changed the IT universe for the better, but with new benefits come new challenges. It is important to understand that although the cloud adds technological layers, the principles of solid data protection are fundamentally unchanged.

MOST **COMPANIES** USING CLOUD SYSTEMS MAY HAVE, AT ONE TIME OR ANOTHER, **ALLOWED POTENTIALLY LETHAL EXPOSURE** OF THEIR CLOUD-STORED DATA DUE TO **CARELESS CREDENTIALING.**

What You Can Do

If your security procedures have not been upgraded to accommodate the complexities of the cloud, it is time for a data protection audit. Not only will this highlight any vulnerabilities introduced by the cloud, it also identifies weaknesses caused by the addition of other IT elements over time.

The audit should be the first step in developing an airtight, system-wide business protection plan. To ensure the thoroughness, strength, and integrity of that plan, we recommend high-level guidance backed by deep experience in working with cloud-based systems.

Michele Vayle is Marketing Director for RenovoData. For more information call toll-free at 877-834-3684. RenovoData is a leading, remote cloud backup and disaster recovery service provider, helping companies protect critical data worldwide.

TRANSCREDIT

Freight Payment Index

2019 *CS-DTP

	**TIA	Non-TIA	Shippers
Jan.	95-41	93-38	78-42
Feb.	94-33	93-47	78-44
Mar.	94-32	94-45	79-32
Apr.	94-33	94-43	78-39
May	94-37	93-47	76-41
Jun.	94-34	93-45	76-42
Jul.	94-34	93-46	76-42
Aug.	93-33	92-42	75-38

2018 *CS-DTP

	**TIA	Non-TIA	Shippers
Aug.	95-35	94-38	76-42
Sept.	95-35	94-39	76-42
Oct.	95-37	94-36	77-37
Nov.	95-36	95-36	77-39
Dec.	95-37	94-41	77-48

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.

*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