Disaster Recovery in the Age of Ransomware

***Drew Schlussel,** director of product marketing at Wasabi, explains why traditional disaster recovery strategies aren't effective against ransomware and what organizations can do to make their systems less attractive to attackers.*

How have storage-related cybersecurity challenges changed since the pandemic?

Security changed relative to all IT operations, but especially around storage. With the shift to remote work, content and other data was being generated everywhere and needed to be shared and backed up. Organizations suddenly had everyone outside the firewall, so every asset was more or less exposed through all these new endpoints. Organizations had to figure out how to keep things safe and secure in this new environment.

Are organizations as prepared as they think they are to recover from ransomware attacks?

Unfortunately, they're not. There's a belief that if you have good backup practices, you can just restore your data if something goes south. However, with ransomware, the bad actors go after backups to eliminate any reason their victims might have to not pay a ransom. In terms of best practices, it's not just about having multiple copies of your data spread within the organization. You need to store backups outside your organization, so there is an "air gap" between the network and the data backup. Another issue is organizations often don't practice how to restore their data, so they have no guarantee their backups will work. Imagine reaching the end of a 48-hour restore operation on your largest databases only to discover the backups are completely useless because they're corrupt, incomplete or encrypted by the ransomware.

"Immutability" has become a buzzword in data protection and disaster recovery. What does it mean and why is there more focus on it?

Immutability means that nobody can alter or delete your data — not the IT director, the root user, anyone in charge of your network or your cloud service providers. In the event of a ransomware attack, immutability puts you in a very powerful position. It guarantees that you have full integrity of your data so you can confidently execute the restore operation and not pay the ransom — even if the hackers take over your network and steal or encrypt your data.

How can state and local governments use the cloud to achieve immutability?

They can capitalize on recent funding to enable immutability by combining better data backup solutions with an air-gapped cloud storage service. Before cloud storage services came along, the only way to air gap data was to dump it onto a tape, stick it on a truck and send it to a secure offsite vault. The problem is that it can take hours or days to retrieve that data. With the cloud, you get the same advantage of storing backups offsite. But you can also retrieve that data immediately and have a completely different set of credentials that protects access to that information and employs immutability. Air gapping and immutability go hand in hand when it comes to leveraging a cloud storage service to protect your data.

How can organizations balance the need for timely data access and rapid recovery with the need to minimize storage costs?

One reason cloud storage services are succeeding is because they provide high performance at a much lower cost than the large cloud providers. Many hyperscale cloud storage providers use service tiers where organizations can store certain data "deep and cheap" for governance or compliance reasons. However, data retrieval can take hours or days and data egress fees can be very expensive. By contrast, a high-performance storage service that doesn't use service tiers offers a better model for organizations that are fighting ransomware and need active data and a fast response time. Cloud storage services also don't charge a data egress fee — unlike many hyperscale cloud providers. This means disaster recovery teams can regularly practice restoring their data without paying a fee every time they do so.

What advice do you have for organizations as they consider storage and recovery requirements for specific data?

Planning is paramount. Have a plan before you create a single byte. Have a plan for how you're going to protect data and restore it. And make sure you actually follow your plan. Then practice, practice, practice. You need to be ready for when the real thing happens, otherwise what's the point of having a backup and a plan in the first place?

Learn more at **Carah.io/GT-Dec-Wasabi**

DISASTER RECOVERY IN THE AGE OF RANSOMWARE

- Protect data from accidental or intentional deletion or alteration
- Support for Governance and Compliance Modes Required by CJIS, FINRA, HIPPA and more
- Seamless integration with Veeam, Commvault and other backup solution providers
- Simplified management for access limits and retention periods

Wasabi is Simple, Predictable and Affordable with the P's That Just Make Sense

Price

80% less than AWS S3

No egress charges

No API request charges

Performance

Faster than the competition

Quick uploads & downloads

Private network options

Protection

11x9s data durability

Immutable storage

Regulatory Compliance

wasabi.com/ransomware

Have questions?
Carahsoft@Wasabi.com

wasabi®
hot cloud storage