AXIS / Technology

Practical Guidance

When the Cloud Goes Dark: Lessons from the AWS Outage?

Why every cloud-reliant business needs to review its service dependencies and insurance protections.

Amazon Web Services (AWS), the world's largest cloud provider, experienced a major service disruption on October 20, 2025, leaving thousands of businesses temporarily offline. According to AWS, the outage stemmed from a network configuration error that cascaded across key systems, affecting services including EC2, S3, and Lambda in multiple regions.

While the disruption lasted only a few hours, the ripple effects were immediate: e-commerce transactions stalled, internal systems froze, and critical SaaS platforms went dark. For companies whose operations hinge on uptime, even short outages translate to lost sales, reputational damage, and contractual penalties.

As one CIO noted, "It's a reminder that our 'resilience' still depends on someone else's system."

The Hidden Exposure Behind the SLA

Many businesses assume that their Service Level Agreements (SLAs) with hyperscale providers like AWS, Azure, or Google Cloud fully compensate them for downtime. In practice, these SLAs offer limited remedies, typically in the form of service credits worth only a fraction of monthly fees. They exclude consequential losses such as business interruption, lost revenue, or reputational damage.

More importantly, these SLAs are designed to protect the cloud provider, not the user. Liability caps, exclusions, and narrow definitions of "service unavailability" mean that customers have little contractual recourse when a major outage occurs.

The result is a liability gap for cloud computing companies that depend on these platforms. Even if the root cause lies with an upstream provider like AWS, a SaaS or IaaS provider may still be contractually obligated to compensate its own customers for downtime under its own SLAs.

That disconnect between limited upstream protection and broader downstream commitments is what creates true financial and reputational exposure during an outage.

The SLA Dilemma: What You Promise vs. What You're Covered For

Cloud computing companies often back their reliability with strict SLAs, committing to 99.9% or even 99.99% uptime. These commitments are not just marketing language; they are binding performance warranties.

If an outage occurs, the provider may owe service credits or even contractual penalties to customers. While these may seem minor, they can escalate rapidly when applied across hundreds or thousands of enterprise clients.

Moreover, SLAs often include reciprocal obligations:

1. Customers expect compensation for downtime, even if the root cause lies with an upstream provider.
2. Providers may still be liable to their clients even when the failure originated beyond their control.
3. SLA exclusions often limit the provider's ability to recover those same losses from their upstream partner.

This creates a mismatch of liability whereby cloud computing companies bear contractual exposure for outages they did not cause and cannot control.

Understanding that chain of dependency from AWS to you, and from you to your customers is essential. Each link defines who bears financial responsibility when the cloud goes dark.

The Insurance Angle: Turning Downtime into Recoverable Loss

1. Parametric Coverage to Backstop SLA Warranties

Parametric insurance can be structured to trigger automatically when a cloud service outage exceeds defined thresholds (for example, two hours of downtime in a given AWS region).

For cloud providers, these policies can serve as a financial backstop to SLA warranties, providing rapid funds to offset customer credits, lost revenue, or remediation expenses. Because they pay based on a verified event rather than a lengthy claims process, they deliver liquidity exactly when reputational and contractual pressures peak.

2. Dependent System Business Interruption (BI) Coverage

Dependent system BI coverage extends traditional cyber or property business interruption protection to include losses caused by outages at third-party providers, such as AWS, Microsoft Azure, or Google Cloud.

This ensures that when an upstream provider fails, your business, and your customers, aren't left absorbing the full financial impact.

Together, these solutions form a more resilient financial framework: parametric coverage fills the gap in SLAs, while dependent system BI coverage protects against external infrastructure risk.

Beyond the Outage: Contractual Clarity and Risk Transfer

Insurance alone is not enough. Every cloud computing company should routinely review:

1. **The SLAs they offer clients:** What commitments are being made, and are they insured or indemnified?
2. **The SLAs from upstream vendors:** Do they provide reciprocal protection, or are you assuming risk without recourse?
3. **Force majeure and limitation-of-liability clauses:** Are they aligned with actual exposure, or do they create uninsured promises?

In many cases, aligning your contractual language with your insurance structure is the key to avoiding uninsured losses during an outage.

A Few Hours This Time. What About Next Time?

The October AWS outage lasted only a few hours. But if the disruption had extended for a day, or multiple days, the economic losses could have reached billions. For many SaaS and infrastructure providers, such a scenario would test not only technical resilience but also financial survivability.

Takeaway

Business continuity is not just about servers and redundancy, it's about contracts, coverage, and capital. Cloud outages are inevitable. Financial ruin from them is not. By understanding your SLA obligations, mapping dependency chains, and integrating parametric and dependent-system BI insurance into your risk transfer strategy, your organization can turn unpredictable downtime into manageable exposure.

For a detailed review of your SLA commitments, vendor dependencies, and insurance response, contact the Axis Insurance Technology Practice.

We can help assess whether your current program is positioned to respond the next time the cloud goes dark.

Contact Us

Chris Jones
Account Executive,
Mining & Technology
+1 (778) 788-2853
Chris.Jones@axisinsurance.ca

Clive Bird
Senior Vice President,
Mining & Technology
+1 (604) 817-8072
Clive.Bird@axisinsurance.ca

Stacey Copeland
Vice President,
Mining & Technology
+1 (604) 619-7775
Stacey.Copeland@axisinsurance.ca

Tristan Smith
Business Development Specialist,
Mining & Technology
+1 (416) 885-0671
Tristan.Smith@axisinurance.ca

About

Axis Insurance – Safeguarding the Exceptional. Axis Insurance is your strategic advantage; we cut through the complexity of risk management enabling you to confidently embrace the opportunities of tomorrow. Our role is to provide you with the best insurance value that combines coverage, service and price. We also provide personalized, quality service that includes professional insurance advice, ongoing policy maintenance and claims support. When any issue arises regarding your insurance coverage, we are your advocate, using our professional experience to best represent your individual interest. Follow Axis on LinkedIn, X, Facebook and Instagram. Stay up to date by signing up for our newsletter here.

axisinsurance.ca
555 Burrard St, #400, Vancouver, BC, Canada, V7X 1M8
1-800-690-7475