

CYBER UPDATE



AWS Outage Could Be a Moderate Loss for Insurers and Reinsurers

The Oct. 20 Amazon Web Services (AWS) outage knocked out many widely used platforms for between five and 24 hours and could result in a “moderate” loss for the cyber insurance and reinsurance community, according to cyber loss modeling firms.

With household names like Venmo, Snapchat, Fortnite, Roblox, and smart home service Ring down for several hours, the service disruption highlights the systemic risk potential for digital platforms relying on a single cloud service provider, according to [commentary](#) from CyberCube.

Cyber insurance policies typically have waiting periods for business interruption coverage of eight to 12 hours. With disruptions from this event lasting on average 15 to 16 hours, insurers could see claims for contingent business interruption (CBI) come in.

“While not all losses will be insured, the event could drive CBI claims, particularly among large enterprises with high sensitivity to service continuity,” said CyberCube.

The outage was determined to be caused by a domain name service (DNS) error for AWS’ US-East-1 region, located in Virginia. DNS servers translate website domain names into IP addresses, allowing internet users to type in a web address rather than a string of numbers.

“US-East-1 is crucial because it is AWS’s largest and oldest region, hosting core services, management infrastructure, and global control planes that other AWS regions and customers depend on for authentication, routing, and service coordination,” explained CyberCube.

According to a LinkedIn post from Parametrix, a firm that specializes in cloud outage monitoring and insurance coverage, the “critical phase” for the event lasted just over 2.5 hours during the night in the U.S. This limited much of the local impact. The next phase lasted about 7.5 hours, but was

AWS restored many of its services within hours. An analysis from Moody’s of more than 570 service providers found a range of recovery times for AWS clients, with 38% back up and running in five

hours, 59% operational within eight hours, and 79% within 12 hours. For a few firms, the disruption lasted more than 24 hours. However, the firm noted that the downtime does not necessarily translate into lost revenue time.

Moody's added that the AWS event illustrates a "range of complexities" in cyber coverage, including a "misalignment" on waiting periods and the impact of downtime.

Derek Blum, senior director at Moody's, commented in the analysis that cyber policies may distinguish between malicious and non-malicious events, and waiting periods could potentially be measured by the downtime experienced by the cloud provider rather than by the client.

"The AWS event triggered cascading failures across industries and geographies, impacting financial institutions, insurers, retailers, airlines, government services, and media platforms," said Derek Blum. "This highlights the importance of robust cloud resilience strategies and the need for clarity in cyber insurance policies – especially regarding coverage triggers and waiting periods."