Brown & Brown

PROPERTY & CASUALTY

Cloud Outages

Insurance Considerations

By, Susan Leung

Recent outages involving major cloud service providers have drawn significant attention across industries, with preliminary estimates suggesting that tens of thousands of organizations may have been affected. Despite the scale of disruption, there are currently no reliable assessments of the proportion of insured losses, as claim notifications and evaluations remain in the early stages.

Cloud outages can trigger widespread system failures, particularly for organizations that rely heavily on cloud infrastructure for core operations, data storage and customer-facing services. These disruptions can cascade across supply chains, interrupt business continuity and expose vulnerabilities in redundancy planning. The impact is often magnified when multiple services, such as authentication, data access and communications, are hosted on the same cloud platform.

At present, market sentiment suggests that the insurance impact from recent outages is expected to be minimal. However, cyber underwriting executives have noted that events of this nature are consistent with modeled scenarios and have been considered in the design of coverage solutions. These incidents reinforce the importance of evaluating cloud dependency and resilience strategies as part of cyber risk management.

Below, we explore key policy complexities that may influence potential recoveries.

Systems Failure

Multiple types of events can cause cloud outages: a recent cloud outage in the news impacted the Domain Name System (DNS), a foundational component of internet infrastructure responsible for translating human-readable domain names into numerical Internet Protocol (IP) addresses. This failure disrupted the ability of cloud services to route traffic properly, resulting in widespread interruptions across web-based applications, websites and internet-connected devices.

DNS functions like a real-time phonebook for the internet, converting domain names (e.g., www.sample.com) into IP addresses (e.g., 123.1.2.3) to locate and connect users to the correct online resources. When DNS fails, even well-functioning systems can become inaccessible.

If the network interruption occurred within the infrastructure of an insured organization using cloud services, it could potentially be classified as a first-party “Systems Failure” or Business Interruption resulting from such a failure. System failure is separate from security failure, which requires a malicious action.

Whether coverage applies will depend on the specific terms of the insurance contract. Coverage may hinge on whether the definition of your computer system or network includes third-party IT infrastructure, such as hosting services, cybersecurity platforms or threat detection systems. This interpretation can vary significantly across carriers and policy language.

Business Interruption and Contingent Business Interruption

The recent cloud service outage may also trigger Contingent Business Interruption (CBI) coverage under cyber insurance policies, depending on the nature of the disruption and the role the cloud provider played in the insured's operations. Key considerations include whether the insured's systems were hosted by the affected provider and directly impacted, whether the insured experienced direct operational effects without being hosted or whether the outage disrupted the operations of the insured's vendors or clients. Cyber insurance coverage can differ depending on the type of third-party company that is impacted.

Time Element Deductible / Waiting Period

Another critical factor is the time element deductible or waiting period, along with the period of restoration. Most Business Interruption clauses require a minimum downtime, typically eight to 12 hours for small to mid-sized enterprises, and up to 24 hours for large accounts—before coverage begins.

Carriers will require documentation proving that network operations were suspended for the required duration. Restoration may occur in phases, with some business components recovering earlier than others. Quantifying Business Interruption involves assessing which systems were impacted, associated revenue losses, whether the waiting period was met and how the Period of Restoration is defined. Determining how Contingent Business Interruption is worded in a policy in terms of dependency and whether cloud services are included as a covered vendor should be evaluated.

Customer Attrition

Customer attrition is another potential area of loss. For example, cloud outages have recently impacted retail financial institutions, media and communications platforms. If customers choose alternative providers due to these disruptions, the resulting costs of switching providers may be considered.

Some cyber policies limit coverage to income lost during the outage, while others extend coverage to include post-restoration customer attrition. Determining the full financial impact may require forensic accounting and negotiation with carriers, especially when evaluating historical revenue trends and direct links to cloud outages.

Supply Chain Coverage

Contingent Business Interruption may also apply to supply chain dependencies. For instance, disruptions to banks or credit card processors could delay product or service delivery. Coverage for non-malicious acts affecting third-party dependencies outside the insured's IT network is another area to review in the cyber insurance contract.

Extra Expense

Extra Expense coverage may address costs associated with downtime, including incident response, customer remediation, compliance exposure and catch-up work. These costs are critical in assessing the financial impact of a cloud outage.

Financial Deductible

In addition to the time-based deductible, insureds may face a financial deductible. For example, if a policy includes a 12-hour waiting period and a $500,000 financial deductible, and the insured's recovery took 15 hours but resulted in only $250,000 in lost income, coverage will not apply. Some policies require only the waiting period to be met, while others require both thresholds.

Conclusion

Cloud outages present a unique set of circumstances. Early reporting offers insight into its potential scope and cost, but carriers must evaluate numerous factors before determining coverage. These include the number of insureds using cloud services, the nature of their claims and the specific language of their policies.

New cyber insurance solutions are developed to cover outages from cloud providers that allow prompt recovery without the need to retain forensic accountants to evaluate the loss. These policies provide indemnity on a pre agreed hourly dollar amount depending upon the time the cloud provider was interrupted.

How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

Find Your Solution at BBrown.com