UII KEYNOTE REPORT 127 • MARCH 2024
DATA CENTER TYPES AND VENUES, RESILIENCY, RISK AND SECURITY, OPERATIONS, MANAGEMENT, AUTOMATION, FINANCE AND STRATEGY

uptime INTELLIGENCE

Cloud outage insurance: assessing policy option

Companies delivering mission-critical services are increasingly vulnerable to outages from third-party IT services — including public cloud platforms — over which they have little control. As data center operators use more external partners, such as the public cloud and software as a service, they are exposed to new threats relating to compute, network availability and cybersecurity.

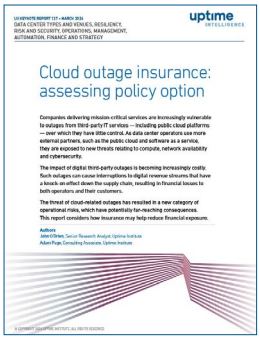
The impact of digital third-party outages is becoming increasingly costly. Such outages can cause interruptions to digital revenue streams that have a knock-on effect down the supply chain, resulting in financial losses to both operators and their customers.

The threat of cloud-related outages has resulted in a new category of operational risks, which have potentially far-reaching consequences. This report considers how insurance may help reduce financial exposure.

Authors
John O'Brien, Senior Research Analyst, Uptime Institute
Adam Page, Consulting Associate, Uptime Institute

Key points

- The frequency and cost of third-party digital outages continue to rise, highlighting the growing risks to operational resiliency and the shortcomings in current risk-management practices.
- In the event of a third-party-related cloud outage, partner service level agreements (SLAs) may fail to cover the full cost of business interruption. This can leave operators shouldering much of the rising cost of outages.
- Policies, such as contingent business interruption (CBI), technology errors and omissions (tech E&O), and cyber and parametric insurance, can help reduce the exposure to rising outage costs.
- Insurance will only ever be a partial solution and operators will need to examine the details of every policy. Care is needed to avoid expensive duplication of cover as well as to avoid underinsurance for specific risks.



Contents

Figures

Uptime Institute Intelligence is an independent unit of Uptime Institute dedicated to identifying, analyzing and explaining the trends, technologies, operational practices and changing business models of the mission-critical infrastructure industry. For more about Uptime Institute Intelligence, visit uptimeinstitute.com/ui-intelligence or contact research@uptimeinstitute.com.

Introduction

The cost of outages is rising for data center operators every year. Around two-thirds of outages now cost more than $100,000 and one in four cost over $1 million, with the number affected rising every year, according to the Uptime Institute's *Annual Outage Analysis 2023* report. The growing cost associated with outages can be traced to an increasing dependency of corporate economic activity on digital services and the data center.

With just 10% of data center outages related to third parties, operators can be led into a false sense of security about the risks. It is likely, for instance, that managers will focus mostly on first-party risks because power and cooling account for more than half of all data center outages. A failure of a critical cloud service, however, can be just as devastating as an on-site data center outage.

Operators may also believe that, in the event of a cloud or other third-party outage, compensation from provider service level agreements (SLAs) will help soften the financial blow. However, Uptime Intelligence research shows this is not necessarily the case (see *Cloud SLAs punish, not compensate*).

While the insurance industry has a role to play in resolving some of these issues, insurers struggle to offer policies in cases where the risks are not well defined. Third-party digital supply chains perfectly fit this description; they consist of complex, often opaque interdependencies where it can be difficult to determine fault or accountability. The result, from an insurance perspective, is a constantly changing mix of products, where inconsistencies in pricing, exclusions, insurance triggers, value and time limits can lead to underinsured vulnerabilities.

This report focuses on outage insurance that covers third-party digital services, including cover for potentially catastrophic consequences that result from a cyberattack, system failure or simply human error. It is part of an ongoing series of Uptime Intelligence reports that analyze IT service resiliency.

Insurance terminology

One of the first challenges for insurers and data center operators is aligning the terminology.

Cloud-related outages can be the result of failures anywhere in the network, compute processing, systems and applications that reside in connected cloud provider and data center IT systems. Cloud-related outages can include availability failures from the following: cloud providers' infrastructure as a service (IaaS), platform as a service (PaaS) or software as a service (SaaS), and data center IT systems, such as networking, servers, storage and workloads.

There are two main categories of cloud-outage risk for operators and insurers.

Intentional malicious outages

Intentional outages, mainly caused by cyberattacks, are the result of sophisticated, often novel threats, such as denial-of-service attacks, ransomware, hacks, phishing, among others. Insurers would typically refer to these as cyber risks.

Cyberattacks become more likely if the organization has inadequate cybersecurity systems and controls in place to mitigate potential risks. Cyberattacks are by their nature unpredictable, which makes them particularly difficult to assess from an insurance actuarial standpoint.

Unintentional, non-malicious outages

Unintentional outages are mainly caused by human error and failure to follow correct procedures. Some insurers might refer to these as non-cyber risks. However, it is a grey area, since human error can lead to vulnerabilities that enable cyberattacks to occur more easily. For this reason, human error is beginning to be included in some cyber policies.

Examples of risk could include errors in software coding, configuration, integration and management, as well as missed firmware updates and poor maintenance of networked systems.

Insurers will likely consider such outage events to be inevitable because the digital infrastructure and systems are still subject to equipment failure and human error.

Networked power and cooling

Outages affecting facility cooling and power systems are another grey area, with regards to cloud-related outages. This is due to the widespread use of networking and software automation to monitor and control cooling and power systems, some of which may have cloud-related dependencies. As data centers become more automated, these complexities are likely to increase.

Insurance steps in

Insurance policies seek to cover customers for a wide range of losses that can result from cloud-related outages. This typically includes business losses that have been left unaddressed by cloud provider SLA credits for availability and uptime.

Insurance in this area is commonly referred to as business interruption or contingent (or dependent) business interruption (CBI or DBI).

Business interruption insurance covers losses arising when the insured business experiences a systems problem that brings normal business to a halt.

CBI insurance covers the loss of income that follows when something goes wrong at a third-party service provider.

Typically, these insurances cover the insured's pre-tax profit it would have generated in the period of cover, had there been no outage (subject to minimum and maximum downtime periods). Cover typically includes the costs associated with running the business, including payroll costs, and the costs of managing the impact of the loss of income. A claim will require evidence-based proof of loss for the insurer to quantify the loss claimed, and this frequently involves forensic accountancy services.

However, insurers face several challenges when considering offering business interruption cover in the IT / data center sector. The following factors can result in reluctance to offer cover:

- **Policy optimization.** Traditional methodologies are unable to account for unpredictable malicious actors, their motives and their evolving methods, as well as the complexities of the supply chain. This means that policies inadequately account for the risks and their consequences, both of which can potentially be unlimited.
- **Pricing risk.** Compared with life assurance or vehicle insurance, for example, there is limited historical data, an absence of unified data types and often poor quality data. As a result, policy premiums often fail to reflect reliable measures of risk.
- **Insurer aggregation.** Opaque and highly interconnected supply chains mean insurers struggle to understand their aggregate exposure. For example, how many of their insurance customers might be exposed to an outage at a single digital facility.
- **Capacity.** Insurers need to maintain enough capital to carry the risks that they write. Demand and capacity have been volatile and uncorrelated across digital insurances, which has at times constrained the availability of cover. It also means that premiums, as well as claims' limits and exclusions, vary greatly.

The options for enterprise IT, however, may be opening up as the insurance industry responds. Specialist insurance companies have emerged in recent years that seek to plug holes in data aggregation and have more expertise in scenario modeling, pricing and policy design. Such companies build their insurance products based on models and data relating to cloud-service reliability and other relevant risks.

Reinsurance only offers a part-solution

In traditional insurance policies, reinsurance would step in to cover the portions of risk where the insurer feels overexposed — reinsurers provide insurance to insurance companies. They tend to reinsure against more extreme and unusual risks, with cyber and other digital risks falling under that category.

However, the complexity and limited visibility of the risks across digital supply chains mean that reinsurers are also at risk of being overexposed. Reinsurers are unwittingly taking on disproportionate exposure to claims, for example, those that arise from a major outage at a single cloud site. This is because of the difficulty in assessing the potential costs, which can be huge, and because a single incident may involve several affected parties, resulting in multiple claims.

Cloud providers may offer to provide a detailed fault analysis following an outage. However, in cases where there are several causes, spanning multiple organizations, it may not be clear where the fault in the supply chain lies. This creates an "aggregation" of risk for reinsurers, who respond by limiting how much risk they will take off insurance companies. That, in turn, places capacity and coverage limits on the first-line insurers.

All of which leads to volatility in the demand and supply of CBI, so that the price of cover, as well as the limits and exclusions imposed on policies, tends to vary widely compared with the cover offered in more mature sectors.

Non-insurance mitigations

In order to model, price and offer cover many insurers (and reinsurers) are increasingly assessing multiple factors and strategies that would serve to minimise both outage risks and their consequences, including:

- Adoption of multi-cloud strategies.
- Security and compliance protocols.
- Physical security.
- Server and network maintenance protocols.
- Application updates and maintenance.
- Natural disaster risk and protection.
- Failure scenario testing protocols.
- Staff training regimes.
- Automation of failover, backup, replication and restoration mechanisms.
- Service provider site track record.
- Site location.
- Outage communication plans.
- Response and recovery protocols.

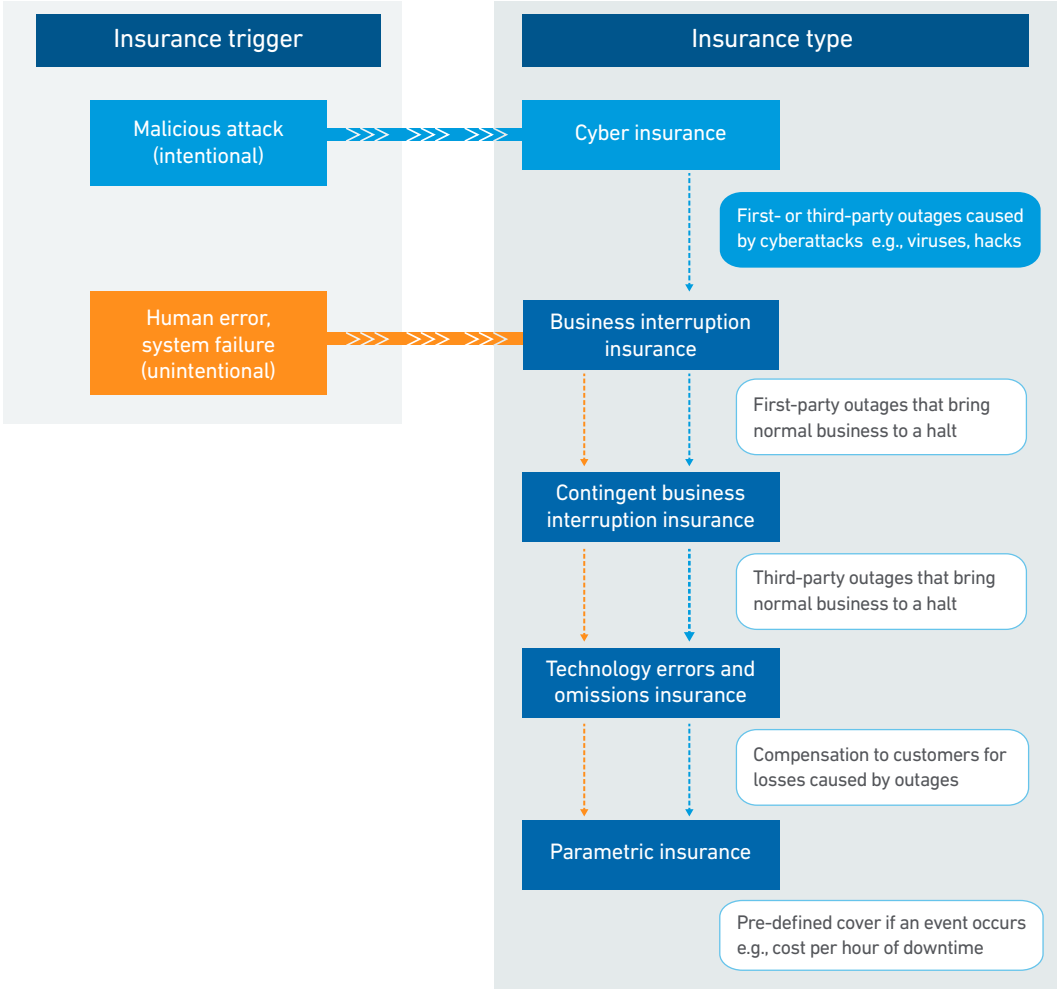
Assessing the options

This section examines the various types of cloud outage insurance options that are available, including cyber, business interruption, CBI, technology errors and omissions (tech E&O) and parametric. Some of the policy types overlap, particularly cyber insurance, where providers now typically offer elements of business interruption and CBI policies.

Figure 1 below outlines the different cloud outage insurance options and policies that can be added, depending on the level of protection required. The dotted lines provide an example of how each subsequent insurance type might fill a potential gap in coverage from the preceding insurance type.

Figure 1

Different types of cloud outage insurance, triggers and coverage



UPTIME INSTITUTE 2024

Cyber insurance

Cyber insurance is primarily concerned with the unauthorized access, theft or destruction of digital assets and data — mostly caused by malicious acts. However, some providers are now starting to include employee error. A claim can be triggered by a wide range of digital events, including hacking incidents and other data breaches, phishing attacks, cyber extortion (such as ransomware attacks), malware intrusions and funds transfer fraud. The claim may include costs for notifying the affected individuals, public relations efforts, forensics and even setting up call centers for affected parties. It can also cover a business's liability if customer data is exposed.

Cyber policies do not necessarily include coverage for business interruption caused by third-party cloud outages (see **Business interruption insurance**, below) — a major limitation in many circumstances. It will typically be limited in value, unless otherwise negotiated. If included, it normally covers lost income between two fixed points in time: the "waiting period" (often 24 to 48 hours after the reported incident) and the "recovery period," which might be a matter of a few weeks later.

The most prominent cyber risks are privacy risk, security risk, operational risk and service risk, which together may give rise to one or more of the following costs:

- Payment of ransomware.
- Privacy liability.
- Data recovery and restoration.
- IT systems restoration.
- Legal expenses.
- IT forensics / cyber forensics.
- Breach notification to consumers.
- Cost of temporary location.
- Public relations and reputation management.
- Credit monitoring.
- Identity restoration.
- Business interruption.

Common exclusions from a cyber insurance policy include:

- Regulatory fines, penalties and sanctions.
- Outage costs that result from cyber warfare or terrorism.
- Losses arising from the outage or failure of critical national infrastructure, such as electricity, gas, water, satellite or telecoms.
- Claims brought by related entities.
- Failure to maintain security measures.
- Loss caused by technical or network operations.

Although business interruption appears in some cyber policies, in many cases it is either limited or excluded. Tech E&O may also be either limited or excluded.

Business interruption insurance

Business interruption insurance is concerned with the interruptions that result from first parties. There are several common exclusions that can seriously limit coverage in the event of a claim:

- Business interruption cover limits are typically low, and would likely not cover the true costs of the outage.
- The interruption may be too narrowly defined; for example, it may require an entire business to shut down for a claim to be made.
- In some policies, cover may be excluded if the source of the systems failure is the result of malicious intent.
- Losses from outages due to scheduled maintenance or upgrades are usually excluded.
- Losses from natural disasters are often excluded unless explicitly stated.
- Deductibles, also referred to as policy excess or retentions, can vary significantly.

Contingent business interruption insurance

CBI insurance is concerned with interruptions that result from third parties. It can be included in cyber policies but is frequently limited in the value of the cover. Around 60% of cyber policies exclude cover for CBI, according to the International Association of Insurance Supervisors 2023 *Global Insurance Market Report*.

Standalone CBI insurance places a value on lost income during a period of cover and is typically for any outage regardless of its cause (i.e., whether it is due to a cyber or non-cyber incident). However, as with all insurance contracts, different insurers will include their own exclusions. In general, policies will include outages that result from a range of non-malicious causes, including software failures, power failures, misconfigurations, resource exhaustion, data center cooling problems and natural disasters.

For data center operators, cloud outage insurance payouts enable them to recover:

- Revenue loss and disruption.
- Data recovery expenses.
- System recovery costs.
- Lost productivity value.
- Legal fees and liabilities.
- Brand and reputational damages.

However, CBI insurance policies can frequently include certain limits and exclusions, such as:

- Cover is only effective in relation to approved service suppliers.
- Waiting periods, which in some cases have recently fallen to as low as six hours but historically have been within 12 to 24 hours.
- Losses due to contractual disputes or the insolvency of suppliers.

Technology errors and omissions insurance

Tech E&O insurance offers liability cover that protects a business if it fails to deliver a contracted technology product or service to its customer. In the context of a cloud outage, this cover goes beyond the compensatory payments for loss of revenue that business interruption and CBI cover may provide. Instead, tech E&O offers further cover in the event that the outage prevents the insured from delivering services to its own customers (who might make a claim against the business for failure to deliver the service).

Parametric insurance

Parametric insurance represents a major departure from traditional models of insurance because it uses real-time data and system monitoring to make both the policy and claim process more transparent and streamlined:

- First, it automates the claims process, principally by eliminating the requirement for proof of cause and proof of loss.
- Second, it automates the valuation of losses. For the insured, this means they will receive compensation to a known value within a short period of time and without the disruption caused by convoluted claims processes.

Parametric insurance works by computing and triggering payouts based on independent indices or thresholds. This type of insurance has been used in the agriculture industry for many years where, for example, rainfall exceeding a certain amount or hours of sunshine falling below a threshold will automatically trigger compensatory payments to a farmer whose crop has suffered as a result.

This type of insurance is now finding its way into the cloud service ecosystem. It is reliant on independent and reliable (i.e., verified) real-time monitoring of data on the uptime of data centers and other measurable supply chain elements.

The common variables within policies — quantum of compensation per hour of downtime, the length of the waiting period and the restoration period — are all negotiable up front to suit a client's needs. However, parametric insurers will also take into consideration other external factors when pricing the cover, including the identity of the cloud provider and even the specific location, the type of services being provided and redundancy between regions.

Parametric policies offer a particular advantage in the insurance mix, so it can be seen as a complementary insurance to cyber, tech E&O and business interruption insurances. This type of insurance is likely to account for a growing proportion of cloud outage cover in the future. However, this will depend on several factors, including the sector's claims payment track record becoming more visible and transparent, the volume and quality of data improving and wider insurance programs becoming better understood.

Summary

Data center operators should give serious consideration to assessing insurance in the face of rising cloud outage costs. Business interruption, for example, will inevitably become a growing consequence of cloud outages, due to economic dependency on digital services. With cyber risks on the rise, operators need to ensure that they are adequately covered for all eventualities — both malicious and non-malicious.

The insurance industry still faces uncertainties in how it can design and price cloud outage policies, due to:

- Limited historical data.
- The complex nature of both malicious and non-malicious causes of cloud outages.
- The opaque interdependencies that lie within the structure of the digital services sector.
- The potentially unlimited scale of losses in more extreme scenarios, such as catastrophes.

Insurers will need to work closely with the data center industry to overcome these challenges. It will mean cloud outage insurance policies evolving to become more tailored to specific customer cloud-outage risks.

Other related content published by Uptime Institute includes:
Cloud SLAs punish, not compensate
Digital resiliency: global trends in regulation

About the authors

John O'Brien

John O'Brien is Uptime Intelligence's Senior Research Analyst for Cloud and Software Automation. As a technology industry analyst for over two decades, John has been analyzing the impact of cloud migration, modernization and optimization for the past decade. John covers hybrid and multi-cloud infrastructure, automation, and emerging AIOps, DataOps and FinOps practices.

jobrien@uptimeinstitute.com

Adam Page

Adam Page spent three decades in regulated financial environments, from investment banking (equities research and corporate finance) to private equity and venture capital. He has an MSc in Finance from the London Business School and an MA in Philosophy and AI.

apage@uptimeinstitute.com

All general queries

Uptime Institute
405 Lexington Avenue
9th Floor
New York, NY 10174, USA
+1 212 505 3030

info@uptimeinstitute.com

About Uptime Institute

Uptime Institute is the Global Digital Infrastructure Authority. Its Tier Standard is the IT industry's most trusted and adopted global standard for the proper design, construction, and operation of data centers — the backbone of the digital economy. For over 25 years, the company has served as the standard for data center reliability, sustainability, and efficiency, providing customers assurance that their digital infrastructure can perform at a level that is consistent with their business needs across a wide array of operating conditions. With its data center Tier Standard & Certifications, Management & Operations reviews, broad range of related risk and performance assessments, and accredited educational curriculum completed by over 10,000 data center professionals, Uptime Institute has helped thousands of companies, in over 100 countries to optimize critical IT assets while managing costs, resources, and efficiency.

Uptime Institute is headquartered in New York, NY, with offices in London, Sao Paulo, Dubai, Riyadh, Singapore, and Taipei.

For more information, please visit **www.uptimeinstitute.com**