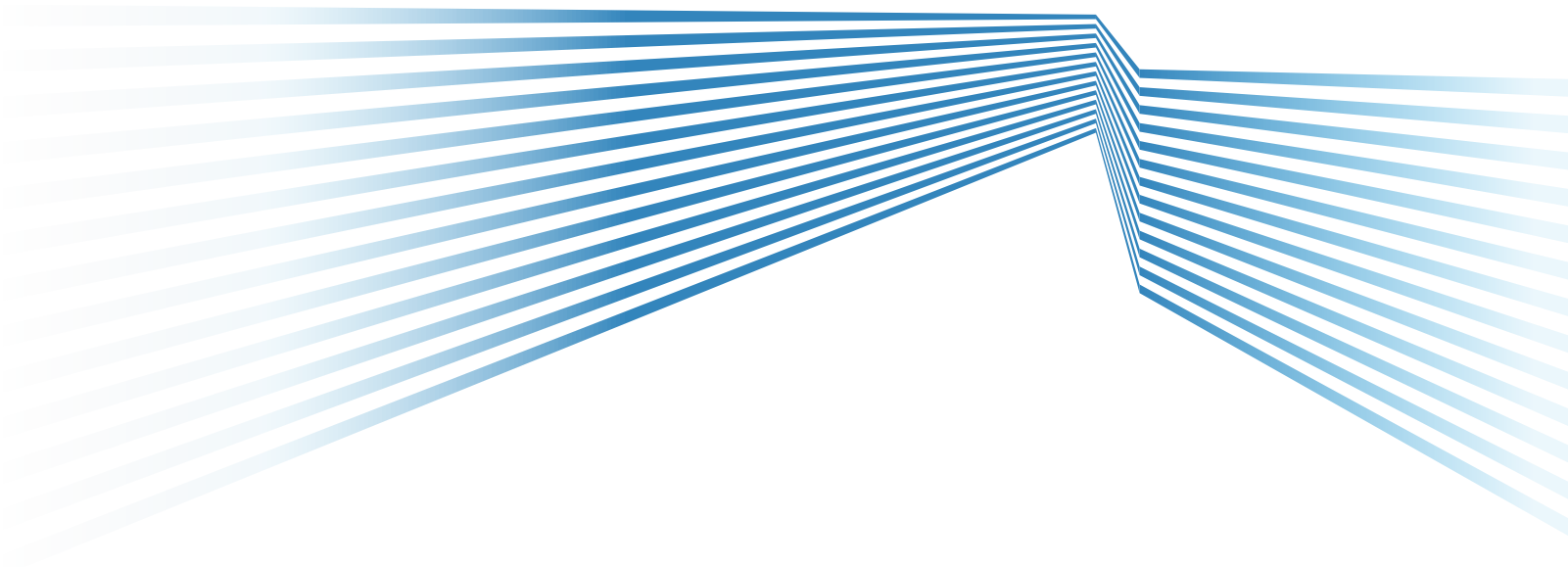
uptime INTELLIGENCE

Annual outage analysis 2026

The causes and impacts of IT and data center outages

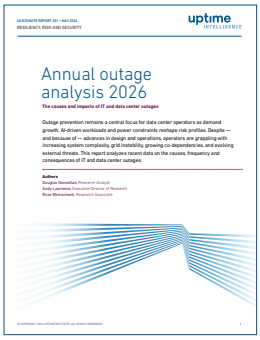
Outage prevention remains a central focus for data center operators as demand growth, AI-driven workloads and power constraints reshape risk profiles. Despite — and because of — advances in design and operations, operators are grappling with increasing system complexity, grid instability, growing co-dependencies and evolving external threats. This report analyzes recent data on the causes, frequency and consequences of IT and data center outages.

Authors
Douglas Donnellan, Research Analyst
Andy Lawrence, Executive Director of Research
Rose Weinschenk, Research Associate



Key findings

- For the fifth consecutive year, Uptime Intelligence research suggests outage frequency (on a per-site basis) is declining. However, the pace of improvement has slowed compared with previous years, and around one in 10 still say their last outage had serious or severe impacts.
- External infrastructure failures are becoming more prominent in publicly reported outages. Outages linked to fiber and connectivity issues are rising and are more likely to result in extended disruptions.
- Outage costs continue to rise slowly. More than half (57%) of the respondents to Uptime's 2025 annual survey say their most recent major outage cost more than $100,000. For the second year in a row, one in five say their most recent impactful outage cost more than $1 million.
- Power remains the leading cause of impactful outages, but risks are evolving. Failures involving UPS systems, transfer switches and generators are dominant; however, worsening grid constraints and high-density workloads are introducing new pressure points.
- Operators are adapting investment strategies toward automation and control systems to manage complexity, while resiliency assessments remain more focused on internal systems than on external and systemic risks.
- The frequency of major fires at data centers have increased gradually in recent years, with lithium-ion batteries in UPS systems a clear contributing factor. However, this rise in incidents may be partly explained by the rapid build-out of new facilities, rather than the inherent risk of deploying these batteries.



Contents

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.

Contents (continued)

Figures and tables

Introduction

This report on digital infrastructure outage trends is the eighth edition in an ongoing series from Uptime Intelligence that analyzes IT service resiliency. The analysis is based on data from a variety of sources, including publicly available reports (e.g., information reported in news and social media), Uptime surveys (e.g., the Uptime Institute Global Data Center Survey 2025 and the Uptime Institute Data Center Resiliency Survey 2026) and other data aggregated and anonymized from Uptime members and partners. Each of these data sources has limitations (see **Table 1**).

Table 1

How Uptime Institute tracks outages

Tracking outages is neither simple nor consistent. Some outages are visible and well publicized, others remain confidential. Some managers, staff and customers may be aware of outages, while others in different roles may not. In addition, some major slowdowns or disruptions may not be classified as outages. Uptime Institute uses multiple means to track the overall trends and incidents, but none provide a clear picture on their own.

This table shows the methods used by Uptime (see the **Appendix** for further information).

	Accuracy	Methodology	Limitations
Public reports	Poor	News/social media	Mainly big outages and interruptions to consumer-facing services
		Outage trackers	May lack details
		Company statements	Sources may be untrusted or poorly informed
Uptime Institute surveys	Fair/good	Industry surveys by Uptime Institute	Answers may vary according to role and sample
			All responses anonymous
Uptime Abnormal Incident Report (AIRs) database	Good/ very good	Detailed, accurate site/ facility-level data shared under a non-disclosure agreement	Information primarily facility/site-based
			All data anonymous

UPTIME INSTITUTE 2026

In this report we use three primary sources:

- The Uptime Institute Data Center Resiliency Survey 2026, conducted in February and March 2026, with responses from more than 450 operators and 500 vendor respondents. This survey is conducted annually. The outages discussed from this survey in most cases refer to all IT service outages, including those caused by data center issues, and are termed "IT services outages" unless otherwise stated.
- The Uptime Institute Global Data Center Survey 2025. This was conducted in the second quarter of 2025, with more than 800 operator respondents. This may be referred to as Uptime's annual survey. In most cases, the outages discussed from this survey refer to data center-specific issues and are termed "data center outages" unless otherwise stated.
- Publicly reported/tracked outages tracked by Uptime in 2025 and the first quarter of 2026. Because this data is less reliable and based on third-party sources, it is separated and discussed in the blue-tinted boxes throughout this report.

In this report, we discuss and categorize outages according to their obvious or perceived severity, using terms such as "serious" or "severe". The way we categorize outages according to severity is shown in **Table 2**.

Table 2

Outage severity rating

Category	Service outage	Impact of outage
1	Negligible	Recordable outage but little or no obvious impact on services.
2	Minimal	Services disrupted. Minimal effect on users/customers/reputation.
3	Significant	Customer/user service disruptions, mostly of limited scope, duration or effect. Minimal or no financial effect. Some reputational or compliance impact(s).
4	Serious	Disruption of service and/or operation. Ramifications include some financial losses, compliance breaches, reputational damage and possibly safety concerns. Customer losses possible.
5	Severe	Major and damaging disruption of services and/or operations with ramifications including large financial losses and possibly safety issues, compliance breaches, customer losses and reputational damage.

UPTIME INSTITUTE 2026

Outage risks evolve

High availability and resiliency remain essential priorities for data center operators as digital infrastructure supports an expanding range of critical services. As reliance on these systems grows, so does the importance of preventing outages and minimizing their impact when they occur.

Uptime Intelligence research shows the industry is continuing to make progress in 2026. Outage frequency (relative to the overall growth in IT) has declined further — continuing a longstanding trend of year-over-year improvements that reflects sustained investment in infrastructure, monitoring and operational practices.

However, resiliency gains are also becoming harder to achieve. Improvements in outage frequency have slowed, and the proportion of the most severe incidents has stabilized at around one in 10.

Many preventable outages still occur. For example, a growing majority of operators that have experienced an impactful outage in the past three years say it could have been prevented with better management/processes or configuration. Uptime does not count "human error" as a primary cause of outages, but identities it as a contributing factor in nine out of 10 outages.

The nature of outage risk is also changing. Failures are less often the result of a single point of failure and are increasingly linked to complex interactions between systems, including software, networks and external dependencies. As digital infrastructure becomes more distributed, outages originating outside the data center — such as those tied to power availability, network connectivity or the reliance on an external cloud service — are playing a larger role.

These shifts make it more challenging to determine the root cause of outages and increase the likelihood of recurring incidents with broader impacts. While Uptime does not expect grid power failure to be a primary cause of outages — on the assumption that resilient data centers have their own on-site primary power — grid failures can still affect the availability of on-site power. This may occur due to a failed power switchover or disruptions to diesel supply triggered by a grid failure.

Operators are adapting to these challenges through continued investment and routinely assessing operational risks. This report examines the latest trends in outage frequency, severity, causes, costs and duration, while considering how these changes influence the way operators manage risk and maintain reliability.

AI DATA CENTERS AND RESILIENCY

The recent build-out of very large AI training and hyperscale data centers, as well as smaller specialist AI labs, raises a number of resiliency-related questions. These new types of facilities are not yet a focus of this report, as most have only recently come into operation and their design and operation vary significantly. There is considerable uncertainty over future directions and levels of resiliency for dedicated AI data centers. Uptime Intelligence is currently researching:

- **How resilient will large operators choose to make their training sites, given the high cost of infrastructure at scale?**
  While inferencing workloads clearly require high levels of resiliency, there is a wider debate around training. Some large sites have been built at speed using crypto mining-style designs with relatively low resiliency. More recent evidence, however, suggests a trend toward higher levels of facility resiliency (e.g., Tier III). The incidence and causes of failures at these sites are not yet well understood. It is possible that AI sites may experience a higher number of outages due to the scale and energy intensity of their IT workloads. In addition, AI training facilities repeatedly stop and start their model runs to address IT component failures. As scale increases, these interruptions — and any related facility failures — are becoming more problematic. Major power or cooling failures, for example, could prove expensive due to lost work, even if end-user customers are unaffected.
- **What systemic risks do very large — or very numerous — data centers pose to regional power grids, and how are operators mitigating those risks?**
  There have already been some near-miss incidents that could have resulted in major grid outages. Although mitigation measures are being introduced, the likelihood of systemic failure appears to have increased in recent years and may continue to do so.
- **How resilient will large on-site continuous power facilities prove to be, especially when deployed and operated by data center owners rather than power companies or utilities?**
  These sites are still in their early stages, so the risks are not clear. The growing use of demand response and power trading during periods of stress or peak demand may add to any risks.

Outage frequency and severity

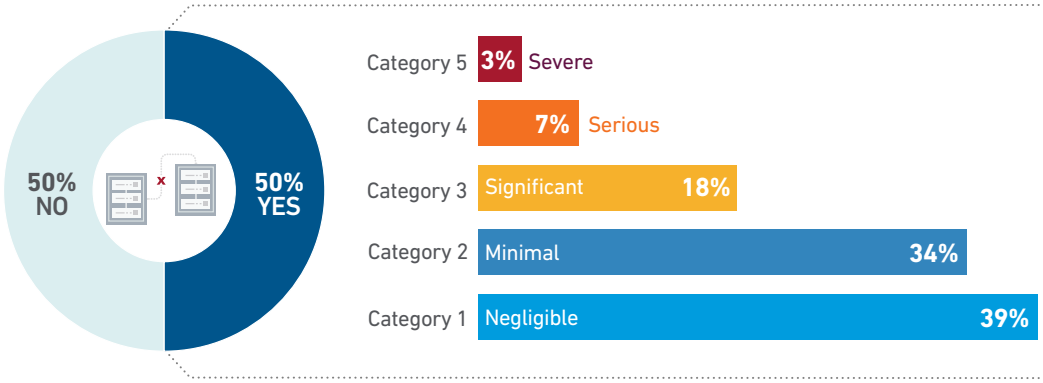
Uptime Intelligence conducted analysis using the latest data from reports and surveys in both 2025 and 2026. While the overall likelihood of experiencing an outage has declined over the past five years, recent results point to a gradual stabilization rather than continued steady improvement.

In the Uptime Institute Global Data Center Survey 2025, half (50%) of operators reported an impactful or serious outage in the past three years (see **Figure 1**). This is the lowest level recorded since 2020 and continues a multi-year trend of improving reliability (see **Figure 2**). However, recent gains have been marginal, suggesting that progress may be slowing. The proportion of incidents classified as serious or severe remains broadly unchanged, at 10% in 2025 compared with 9% in 2024.

Figure 1

One in 20 had a severe or serious outage

Has your organization had an impactful outage in the past three years? If so, how would you classify the most impactful outage on a scale of 1 (negligible) to 5 (severe)? (n=754)



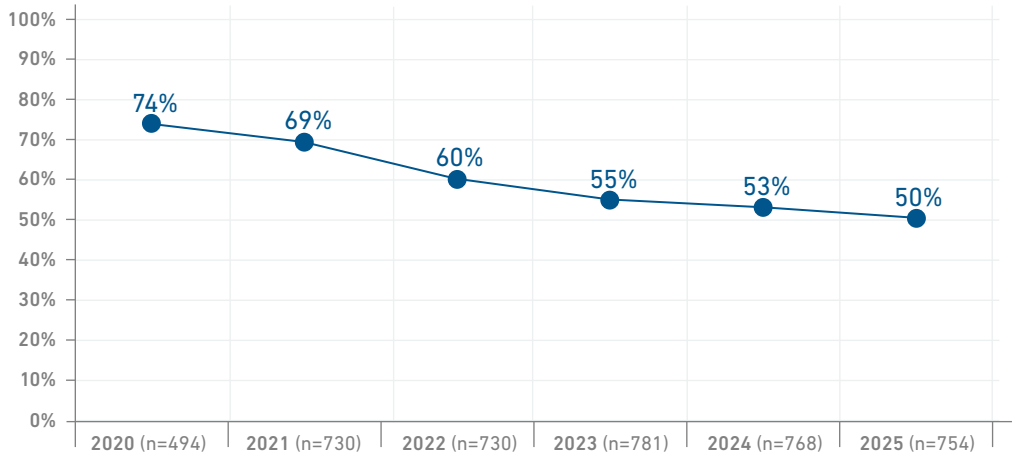
(Responses for "Don't know" are not included.)

UPTIME INSTITUTE GLOBAL DATA CENTER SURVEY 2025

Figure 2

Gradual improvements in outage frequency continue

Has your organization had an impactful outage in the past three years ("Yes" respondents)



UPTIME INSTITUTE GLOBAL DATA CENTER SURVEY 2025

As businesses and critical services rely on digital infrastructure, even brief outages now affect more users and disrupt more operations, leading to greater financial consequences. Some observations on these trends include:

1. **Reliability gains are continuing but diminishing.**
   Outages are becoming less frequent relative to the overall IT growth, but recent improvements in the outage rate are incremental. This suggests diminishing returns from current resiliency approaches, and that further gains may require changes in design, operations or risk management.
   It may also be that improvements in data center practices and design are being offset by countertrends (see below).
2. **Stable performance does not indicate lower risk.**
   The plateau in outage frequency and severity does not suggest operator complacency; instead, resiliency improvements are likely offset by an increasingly complex and demanding operating environment. As data centers support more critical workloads, even isolated incidents can carry broader consequences.
3. **System complexity is increasing as resiliency improves.**
   Software-based resiliency has improved availability for many operators. For example, approaches such as distributed resiliency and availability — which spreads active workloads across several locations — can reduce the impact of a single-site failure. But while these can reduce outage risks caused by single points of failure, they also increase the cost and complexity of synchronizing workloads and may introduce IT-level vulnerabilities that go unnoticed or unforeseen within complex architectures.
4. **Power and infrastructure constraints are emerging as systemic risks.**
   Power availability, interconnection delays and grid reliance are becoming key factors in reliability. With both the grid and the data center operator running much closer to capacity, the likelihood and cost of failures may be greater. While grid failures should not result in a data center outage, transfers to generators sometimes fail.
5. **AI workloads are reshaping risk profiles.**
   AI and high-density compute are placing new stress on power and cooling systems, especially in legacy facilities. Higher rack densities, load variability and operating closer to available power limits may increase the likelihood of cascading failures (see AI data centers and resiliency).
6. **Use of substitute components.**
   Extremely high demand has created a global shortage of critical data center equipment. Developers and operators may face significant delays in securing generators, transformers, switchgear, UPS systems and other subsystems. To work around this, some owners are buying second-user equipment or sourcing substitute components from suppliers without a proven data center track record. This is believed to have contributed to several failures and incidents at some data centers.

Maintaining current levels of reliability may itself become more challenging as demand, density and external dependencies continue to grow. Future improvements will likely depend less on incremental gains in redundancy and more on how effectively operators manage power availability, coordinate across interconnected systems and adapt to more dynamic workloads.

PUBLICLY REPORTED OUTAGES

Major public outages — the headline makers

In addition to regular resiliency and other surveys, Uptime Intelligence also tracks major (sometimes high-profile) outages that are reported by the media or other public sources, such as social media and government. These collected and aggregated reports provide further insights into the nature and impact of outages.

Table 3 shows the number of outage reports Uptime Intelligence collected from public sources over the past 10 years. The numbers do not necessarily represent the underlying number of outages. In recent years, news and social media have reported an increasing number of outages, even though many are trivial and some are inaccurate. Therefore, we no longer collect reports of small, Category 1 outages where it is difficult to verify details and where no great financial loss, disruption or reputational damage occurred. In 2025, we collected details of 122 outages.

Table 3

Publicly reported outages tracked by Uptime, 2016 to 2025

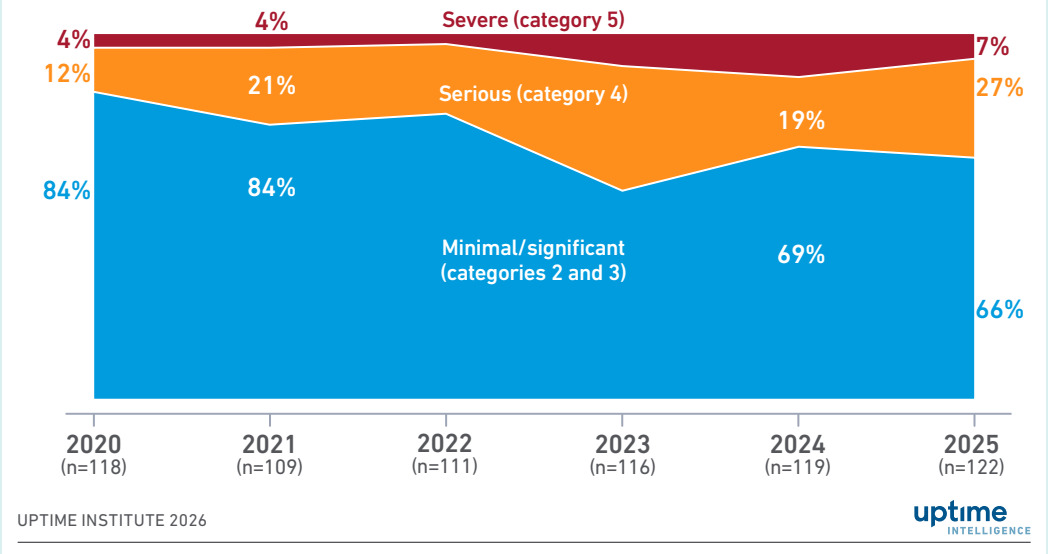
2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	Total
27	57	71	165	118	109	111	110	119	122	1009

UPTIME INSTITUTE 2026

The proportion of publicly reported outages that were severe decreased to 7% in 2025 (see **Figure 3**), down five percentage points from 2024. At the same time, the proportion of Category 4 outages climbed eight percentage points from 2024. The decline in Category 5 outages, alongside the increase in Category 4 incidents, suggests a degree of redistribution within the highest severity tiers, rather than a clear shift toward more extreme outcomes. More broadly, even where severity levels appear stable, the potential consequences may be increasing as digital infrastructure supports a wider range of critical services. As a result, severity metrics alone may not fully capture the evolving risk profile of outages.

Figure 3

Publicly reported outages by severity, 2020 to 2025



UPTIME INSTITUTE 2026

This data also suggests that each year there will probably be 10-20 high-profile IT outages or data center events across the world that cause serious or severe financial loss, business and customer disruption, reputational loss and, in extreme cases, loss of life. Some examples of these are shown in **Table 4** at the end of this report.

Outage causes

Data center outages rarely have a single cause; instead, they often arise from multiple, interrelated factors. As systems become more complex, identifying root causes becomes more challenging — but also more important for preventing recurrence and guiding investment decisions.

Results from Uptime's annual surveys consistently show that on-site power generation or distribution failures remain the most common cause of serious outages (see **Figure 4**). While power issues accounted for 45% of respondents' most recent impactful outages in 2025, this is down from 54% in 2024 — marking a reversal of an upward trend observed since 2020.

This shift may partly result from recent investments in electrical infrastructure upgrades and monitoring/analytics software (see **Figure 18**). However, growing dependence on constrained and increasingly complex power infrastructure, both on-site and on the grid, may create additional challenges that limit further improvement.

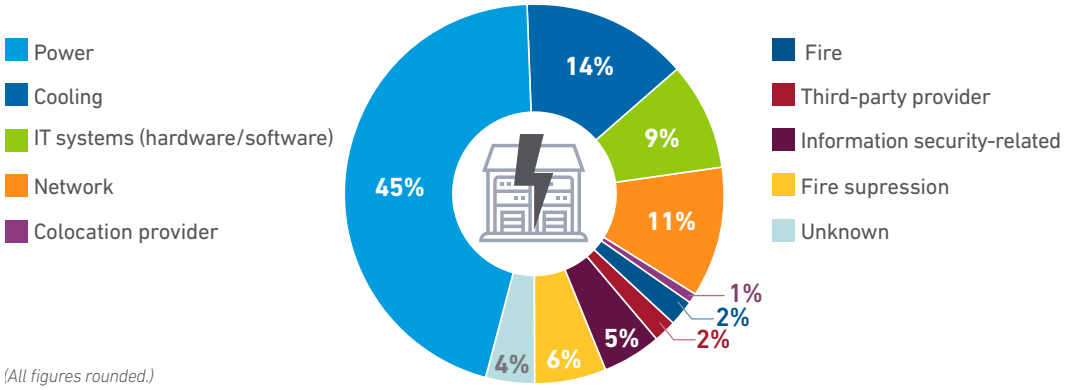
It is also possible that this apparent reduction in the share of impactful power-related outages is due to a rise in other causes. For example, the share of outages attributed to fire suppression systems rose by six percentage points year-over-year. This increase may reflect both the wider deployment of these systems and instances of accidental activation, particularly as facilities adopt more complex safety and monitoring technologies. The use of very early smoke detection apparatus (VESDA), coupled with water sprinkler systems, is now widely recognized as the most effective way to prevent and manage battery fires — but they may cause more preventive outages than some other systems.

Outages linked to information security have also increased. As IT and OT systems become more integrated, security-related risks and incidents are expanding beyond cyberattacks to include misconfigurations, access control failures and disruptions introduced during incident response or patching.

Figure 4

Power is still the leading cause of impactful outages

What was the primary cause of your data center's most recent impactful incident or outage? (n=96)



(All figures rounded.)

UPTIME INSTITUTE GLOBAL DATA CENTER SURVEY 2025

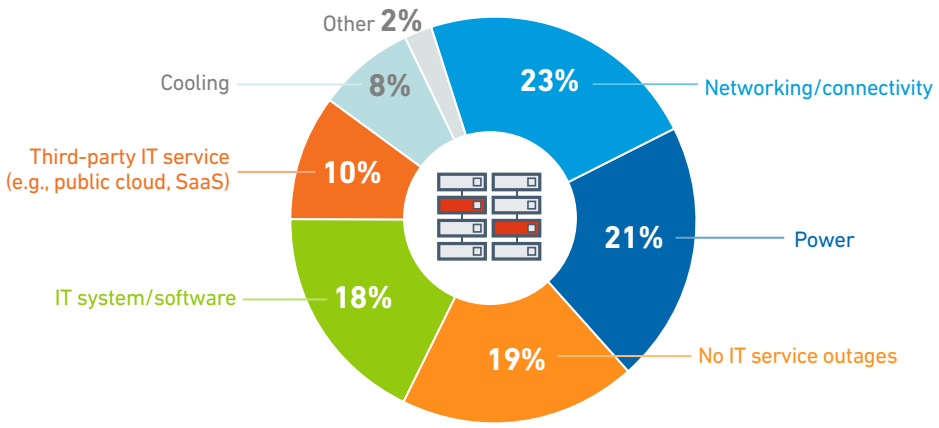
For a broader view of outage causes that extend beyond (but include) the data center, the Uptime Institute Data Center Resiliency Survey 2026 also tracks the most common causes of end-to-end IT service outages, regardless of whether they were the most recent or the most impactful.

Network-related outages continue to be the most frequently reported cause of IT service disruptions (see **Figure 5**), although by a lower margin than in previous years. Notably, nearly one in five respondents report having no IT service outages in the past three years — an improvement of nine percentage points over 2024. This may be partly due to the wider use of software-based strategies, such as automated failover and traffic rerouting, alongside better monitoring and detection tools that help contain issues before they escalate. This is a difficult category of causes to track: some disruptions may also be absorbed within distributed systems, making them less visible as discrete outages.

Figure 5

Most common causes of IT service-related outages

Which of the following issues has been the most common cause of any IT service outages that may have affected your organization over the past three years? (n=403)



UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2026

PUBLICLY REPORTED OUTAGES

Fiber/cable issues lead causes of major public outages

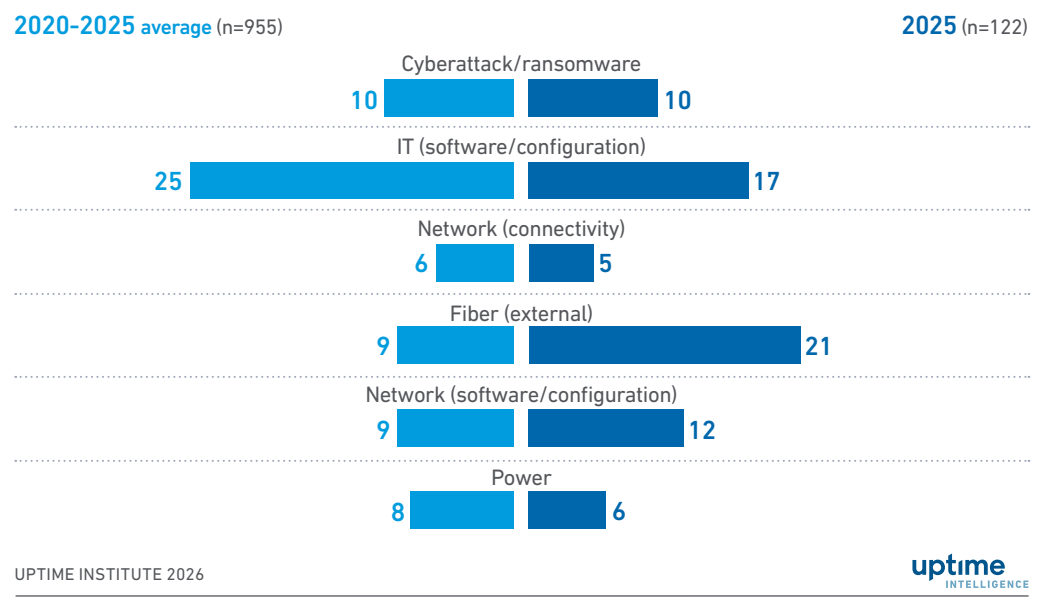
Fiber/cable-related incidents were the leading cause of publicly reported IT service outages collected by Uptime Intelligence in 2025 and showed the largest increase compared with the 2020-2025 average (see **Figure 6**). This compiled data includes all causes visible to end users, rather than just data center-specific issues.

The rise in external fiber incidents reflects a growing reliance on network infrastructure that extends beyond the data center. These assets, including subsea cables and terrestrial fiber routes, are vulnerable to deliberate sabotage, accidental damage, theft and environmental factors.

As digital services become more distributed, outages caused by failures in external connectivity infrastructure may become more prominent. These incidents are commonly beyond an operator's direct control and can affect large geographic areas or multiple services simultaneously. In recent years, governments have become increasingly concerned at the vulnerability of subsea cables to foreign attack. As with other publicly reported outages, the full impact may be underrepresented due to inconsistent reporting and challenges in attributing root cause across complex, multi-provider networks.

Figure 6

Publicly reported outages by cause, 2020 to 2025



PUBLICLY REPORTED OUTAGES

Commercial operators in the limelight

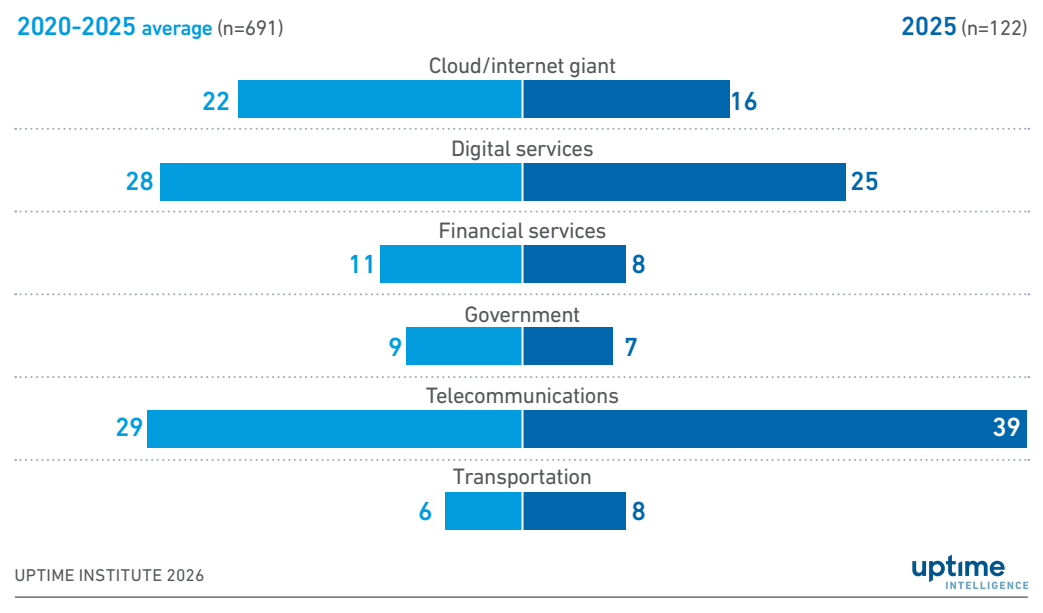
Over 10 years of tracking publicly reported outages, third-party IT and data center providers — including cloud, telecommunications and colocation companies — have consistently accounted for a majority of incidents. This reflects the continued shift toward outsourced services (i.e., the cloud) and distributed digital infrastructure, where large-scale failures can have a widespread impact.

Building on this trend, outages involving telecommunications providers in 2025 rose significantly above the 2020-2025 average (see **Figure 7**). This likely reflects the exposure of external connectivity infrastructure to a broader range of risks, including accidental damage, extreme weather, and, in some regions, geopolitical instability. Telecommunications networks are particularly exposed because they span large geographic areas and depend on infrastructure outside controlled data center environments.

By contrast, outages involving cloud and internet providers fell below average. This likely results from ongoing investments in distributed resiliency, which have strengthened their ability to prevent or recover from disruptions.

Figure 7

Publicly reported outages by sector, 2020 to 2025



Cloud and third-party provider reliability

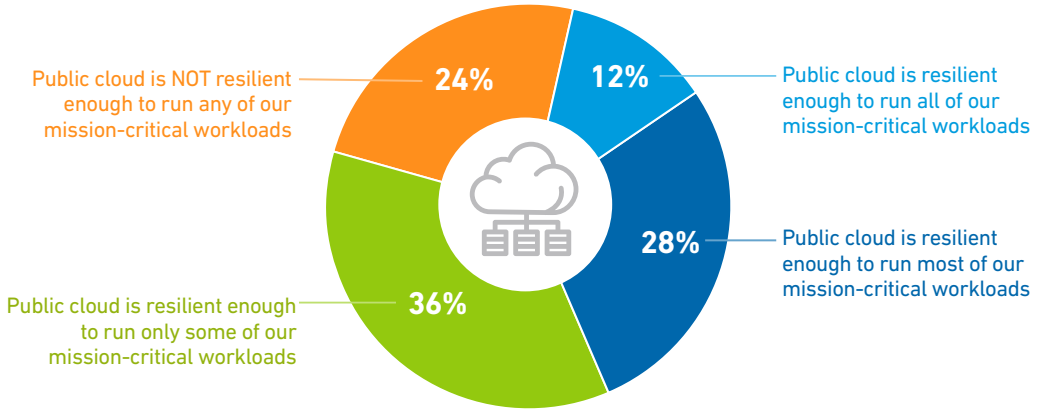
Cloud and internet-based services are designed for high availability, using distributed infrastructure, layered architectures and dynamic traffic and load management to limit disruption. However, as these environments grow more complex and interdependent, failures can cascade across multiple services, regions or providers. As reliance on third-party platforms grows, even brief outages can have widespread operational and financial consequences.

Recent Uptime survey results suggest that the rate (i.e., outages relative to the overall sample) of both data center outages and IT service disruptions caused by third-party provider issues — including those from public cloud providers — have improved slightly compared with 2024. Despite this, enterprise confidence in public cloud resiliency appears to be weakening. In the Uptime Institute Data Center Resiliency Survey 2026, the share of respondents who say public cloud is not resilient enough for any mission-critical workloads increased by six percentage points from the previous year (see **Figure 8**). This continues a gradual shift observed since 2021, showing that concerns about cloud resiliency remain persistent.

Figure 8

Most say cloud only resilient enough for some workloads

Regarding public cloud services, do you think public cloud is resilient enough to run all of your organization's mission-critical IT Workloads, most of them, only some of them or is public cloud not resilient enough to run any of your organization's mission-critical IT workloads? (n=372)



(Responses for "Don't know" are not included.)

UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2026

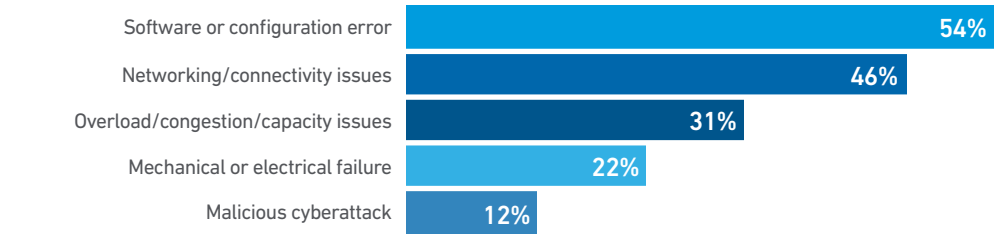
Why are operators hesitant to use the cloud for mission-critical workloads? For the third consecutive year, results from the Uptime Institute Global Data Center Survey 2025 showed that data security remains the top barrier.

These concerns are reinforced by the nature of third-party outages, which are most often linked to software and configuration errors (see **Figure 9**), and can often be unpredictable in their duration and impact. Although these remain the dominant cause, other factors — such as mechanical, electrical and capacity-related failures — are becoming more prominent. This shows that software techniques and load sharing cannot fully sidestep the fact that workloads still rely on physical facilities, and the larger these workloads are, the greater the "blast zone" of a failure.

Figure 9

Most common causes of major third-party outages

Which are the most common root causes for third-party IT service provider-related outages experienced by your organization's data centers over the past three years? Choose no more than three. (n=59)



*(*Only respondents who indicated their organization experienced a significant, serious or severe outage caused by an issue related to a third-party IT service provider are included. Only the top 5 response categories are shown.)*

UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2026

This growing reliance on third-party services is also reflected in risk management strategies. For example, the Uptime Institute Data Center Resiliency Survey 2026 finds that nearly one in five organizations (18%, n=348) now insure against outages involving cloud providers — a figure that has been rising gradually year-over-year. Overall, while cloud adoption continues to rise, many enterprises remain cautious, balancing the benefits of scalability and flexibility against concerns about control, transparency and systemic risk. High-profile failures of some cloud providers in 2025 undoubtedly added to concerns about an overreliance on single cloud providers.

Power outages

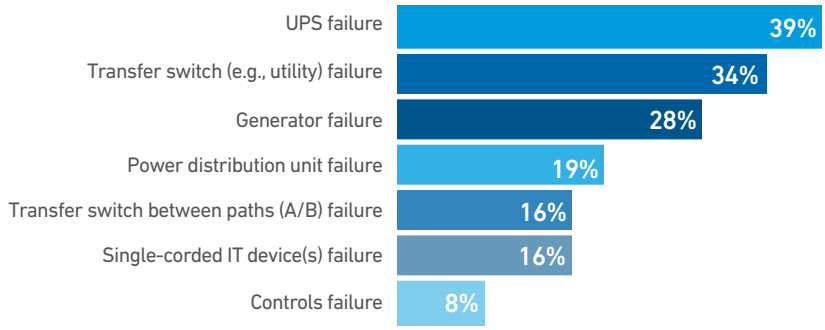
Uptime survey results continue to show that power-related incidents are the leading cause of major outages, accounting for 45% of impactful events in 2025 (see **Figure 4**). While this represents a notable decline from 2024, power failures remain highly disruptive due to their immediate and often total impact on affected systems. Even brief interruptions can lead to extended recovery times as systems restart, data is resynchronized and damaged equipment is repaired or replaced.

Building on these findings, the Uptime Institute Data Center Resiliency Survey 2026 reveals that power-related issues also caused more than one in five IT service outages reported over the past three years (see **Figure 5**). The most frequently cited causes remain consistent: UPS failures, followed by transfer switch and generator issues (see **Figure 10**). At the same time, outages linked to power distribution units, transfer switching and single-corded IT equipment increased significantly from the previous survey conducted in early 2025.

Figure 10

Most common causes of major power-related outages

Which are the most common root causes for the power-related IT outages at your organization's data centers over the past three years? Choose no more than three. (n=129)



*(*Only respondents who indicated their organization experienced a significant, serious or severe outage caused by a power-related issue are included. Only the top 7 response categories are shown.)*

UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2026

Outside the facility, grid conditions are becoming an increasingly important factor to consider when assessing outage threats. Rising demand, aging infrastructure and exposure to extreme weather all raise the likelihood of disruptions. In some cases, limited grid capacity or delays in interconnection and upgrades can restrict redundancy options or introduce additional risk during system changes. Meanwhile, high-density workloads — particularly AI — are placing more stress on both power and cooling systems, introducing greater load variability and reducing the margin for error.

Overall, power remains a well-understood risk, but maintaining reliability is becoming more demanding. It depends not only on robust on-site infrastructure, but also on how effectively operators manage external dependencies and coordinate across increasingly interconnected systems. In the years ahead, operators will have to deal with higher rack densities, higher voltages, lower grid reliability, and increased on-site energy storage; these challenges may add to the risk of outages. Certainly, they highlight the need for robust policies, training and sufficient on-site expertise and capacity.

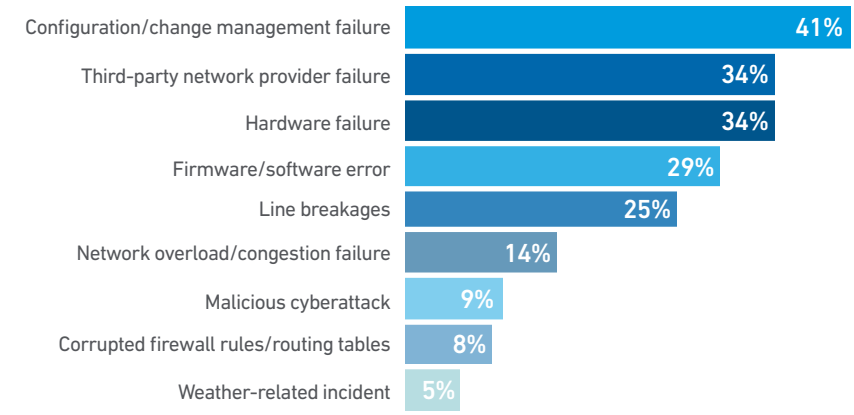
Networking outages

Network-related issues continue to account for the largest share of IT service outages in the 2026 Uptime resiliency survey (see **Figure 4**). As in previous years, these are driven primarily by configuration and change management failures (see **Figure 11**). However, the share of outages attributed to these failures declined by nine percentage points compared with 2025. This shift may reflect a relative increase in other causes, such as hardware failures and firmware/software errors.

Figure 11

Most common causes of major network-related outages

Which are the most common root causes for the networking/connectivity-related IT outages at your organization's data centers over the past three years? Choose no more than three. (n=122)



*(*Only respondents who indicated their organization experienced a significant, serious or severe outage caused by a network-related issue are included. Responses for "Other" and "Don't know" are not included.)*

UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2026

External dependencies also play a major role in network-related outages. Failures involving third-party network providers remain a leading contributor, while incidents related to line breakages have increased eight percentage points from 2025.

These dynamics are likely to intensify in the coming years as the growth of AI workloads places greater demands on network performance. At the same time, software-defined networking (SDN) and automation are improving flexibility and recovery, but also increasing the risk of configuration errors and cascading failures. As a result, maintaining reliability will depend not only on reducing individual failures, but on limiting how far and how quickly those failures can propagate across interconnected systems.

System and software outages

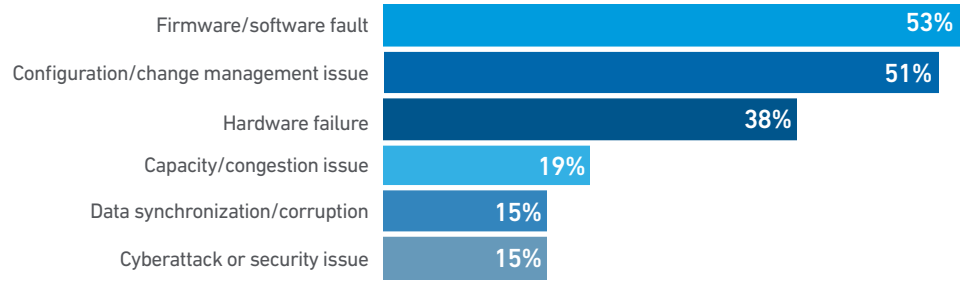
IT systems and software issues remain a major source of outages (see **Figure 12**). In previous years, these were mostly driven by configuration and change management problems. However, results from the Uptime Institute Data Center Resiliency Survey 2026 now show that firmware and software faults account for the largest share.

While related, these issues are distinct. For example, a configuration issue might involve an incorrect IT setting or change, while a software or firmware fault can stem from a bug or defect in the system itself. This shift suggests that outage risk is moving deeper into the technology stack, from operator-driven errors toward faults tied to software behavior, updates and interactions between components. In future years, the use of AI may in theory reduce these errors — but equally, AI could itself introduce errors.

Figure 12

Most common causes of major IT system-/software-related outages

Which are the most common root causes for the IT system/software-related outages at your organization's data centers over the past three years? Choose no more than three. (n=74)



*(*Only respondents who indicated their organization experienced a significant, serious or severe outage caused by an IT system / software-related issue are included. Responses for "Other" and "Don't know" are not included.)*

UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2026

As with network-related incidents, outages caused by IT systems and software issues are likely to increase with the growing scale and complexity of modern systems. Greater reliance on software to ensure availability across multiple facilities — including those managed by third parties — also introduces additional risk. As a result, issues that would once have been contained can now propagate across systems before they are detected.

Hardware failures also remain a major contributor to IT service outages, underscoring the continued importance of managing and maintaining physical infrastructure, even in highly software-defined environments. Even as more functionality shifts into software, reliability still depends on the performance of underlying hardware components.

The human factor

Preventing human error is a persistent challenge in data center operations. Failures can arise from many sources, including gaps in training, unclear procedures, staff fatigue, operational pressure or limited resources.

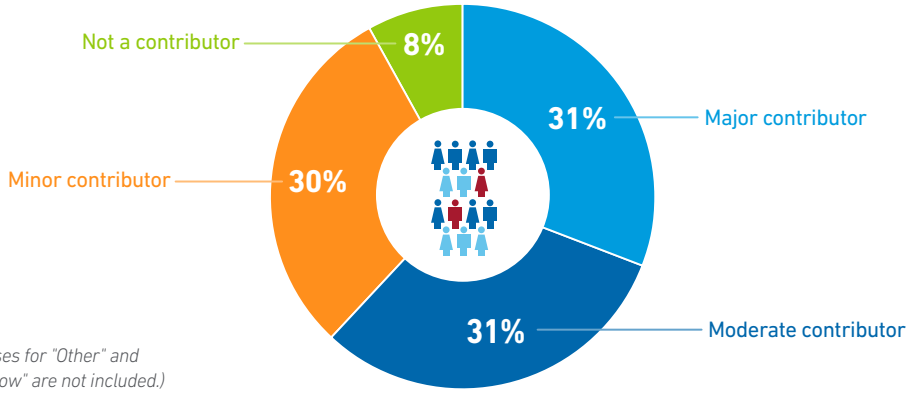
It is often difficult to determine the extent to which human error causes an outage. For example, an outage resulting from a misconfigured system update may stem from a software defect, an incorrect change, or failed testing, making attribution difficult. And if there is a defect, did it escape detection or correction due to human error? In other cases, a UPS failure or a generator failing to start may result from a testing or maintenance misstep — but these are usually attributed to power issues rather than human error.

As a result, Uptime generally treats human error as a contributing factor rather than a root cause. Historical data shows that between two-thirds and four-fifths of major IT and data center outages involve some element of human error. Results from the Uptime Institute Data Center Resiliency Survey 2026 affirm this, as 92% of respondents say that human error is at least a minor contributor to their most recent impactful outage (see **Figure 13**). This reinforces the view that even when technical failures are the immediate cause, underlying human and organizational factors are often involved.

Figure 13

Human error contributes to most outages

To what extent would you say human error has contributed to any significant, serious, or severe outage(s) that your organization has experienced over the past three years? (n=220)



(Responses for "Other" and "Don't know" are not included.)

UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2026

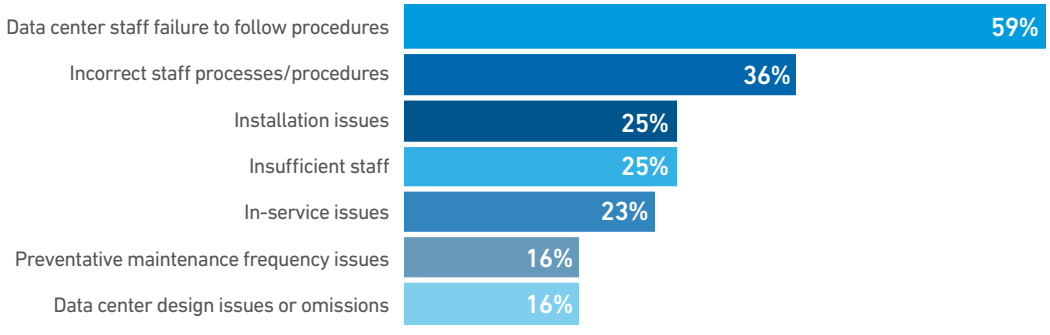
As in previous years, failures to follow established procedures remain the leading driver of human error-related outages (see **Figure 14**). Issues such as inconsistent or unclear processes are also common, alongside installation and in-service errors.

These patterns suggest that managing human error is less about eliminating mistakes and more about designing systems that anticipate and mitigate them. As data center environments become more complex and automated, human operator roles are shifting toward oversight of increasingly dynamic systems, where errors can propagate more quickly and have wider impact.

Figure 14

Most common causes of major human error-related outages

What are the most common ways human error has contributed to IT service outages at your organization's data centers over the past three years? Choose no more than three. (n=199)



UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2026

Improving reliability will depend not only on training and procedural discipline, but also on clearer processes and system designs that reduce the likelihood and impact of human error. Uptime research suggests that such improvements can significantly reduce outage risks from human error. For example, the 2025 Uptime Institute data center survey found that 87% of the respondents (n=98) who experienced an impactful outage in the past three years say it could have been avoided with better management, processes or configuration — an increase of seven percentage points from 2024.

This reinforces the need to pair infrastructure investment with ongoing operational improvements. Measures such as regular testing, staff training and more disciplined change management are likely to remain among the most effective — and cost-efficient — ways to reduce outage risk.

PUBLICLY REPORTED OUTAGES

Are big outages getting longer?

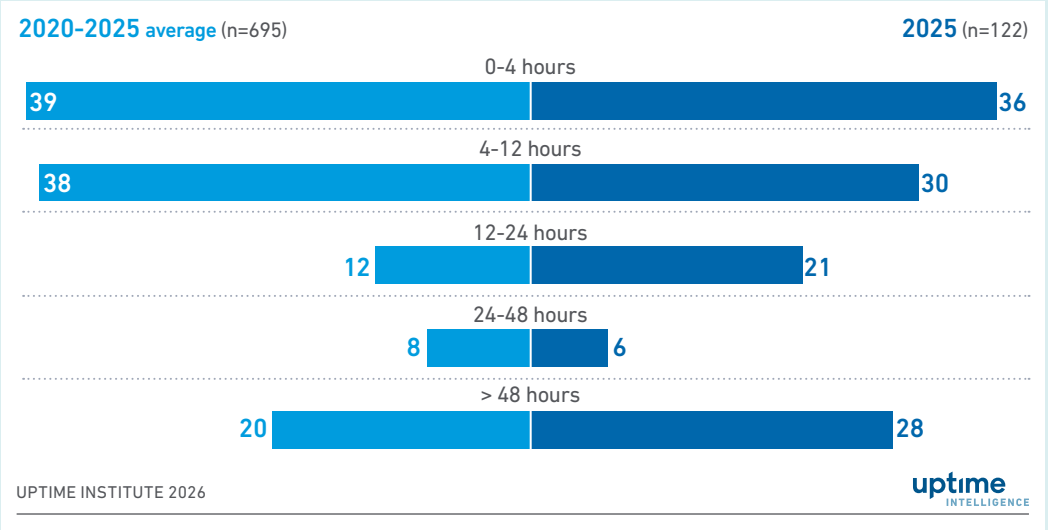
Longer outages tend to have a greater impact, including financial losses and reputational damage. While a majority of publicly reported incidents are still resolved within 12 hours (55%), the share lasting more than 48 hours has increased for the second consecutive year (see **Figure 15**).

This pattern is partly linked to a rise in outages involving external connectivity infrastructure, particularly damaged or disrupted fiber and subsea cables. In 2025, these incidents occurred at more than double their long-term average (see **Figure 6**). Because they often require physical repair and coordination across multiple stakeholders, they typically take longer to resolve than facility-level or software-related failures.

More broadly, the increase in longer-duration outages reflects a shift toward risks originating outside the data center. These incidents are harder to diagnose and resolve, often involving multiple providers and regions. Cybersecurity attacks are also a cause of longer outages. These result in a devastating loss of data or access to data, and lengthy recovery processes. As a result, even as overall outage patterns remain stable, the duration and complexity of some events are increasing.

Figure 15

Durations of publicly reported outages, 2020 to 2025



PUBLICLY REPORTED OUTAGES

Recent serious/severe outages

Most years, there are 15-20 outages publicly reported that Uptime classes as "severe" or "serious" (Category 4 or 5). This means that, depending on the services involved, the outage(s) may result in high costs, reputational damage, threats to life or safety, and serious breaches of compliance rules.

Some examples of major publicly reported outages in 2025 are shown in **Table 4**. The list is largely made up of cloud and/or digital services companies, where outages can affect a wide variety of customers.

Table 4

Ten major outages in 2025 (Category 5)

Company	Industry	Year (quarter)	Cause	Impact
Barclays	Financial services	2025 (Q1)	Configuration error/ software	A mainframe software failure disrupted online banking and payments during the UK tax filing deadline, resulting in outages lasting multiple days. More than half of transactions failed, leading to millions of pounds in compensation payouts.
Marks & Spencer	Retail	2025 (Q2)	Cyberattack/ ransomware	A ransomware attack encrypted core systems, halting online sales for 46 days and exposing customer data. The incident cost an estimated £300 million in lost sales and led to a sharp decline in market value.
Government of South Korea	Government	2025 (Q3)	Lithium-ion battery fire	A lithium-ion battery entered thermal runaway during removal from an IT facility, triggering a fire that disrupted hundreds of systems including emergency services. It resulted in permanent loss of hundreds of terabytes of government data as well as injuries to personnel.
Jaguar	Manufacturing	2025 (Q3)	Cyberattack/ ransomware	A ransomware attack using stolen employee credentials forced Jaguar to shut down manufacturing and dealership systems for five weeks. Estimated losses reached £1.9 billion, with widespread supply chain disruption. The UK government provided financial support to mitigate broader economic impact.
Ingram Micro	Digital services	2025 (Q3)	Cyberattack/ ransomware	A ransomware attack forced Ingram Micro to shut down core systems, halting order processing and logistics operations. Attackers accessed systems via compromised VPN credentials and threatened to leak 3.5TB of stolen customer data.
Telecom Egypt Company	Digital services	2025 (Q3)	Fire	A suspected electrical fault caused a fire at Cairo's Ramses exchange, disrupting national connectivity. Critical services, including emergency communications and financial systems, were affected, and the incident resulted in fatalities and injuries.
Microsoft Azure	Cloud/internet giant	2025 (Q3)	Configuration error/ software	A global Azure outage disrupted core services, including Microsoft 365, Outlook and enterprise platforms. Tens of thousands of incidents were reported within hours, with widespread business and consumer impact.
Amazon Web Services	Cloud/internet giant	2025 (Q4)	Networking system/ configuration error	A defect in DynamoDB's DNS management system propagated incorrect records, causing cascading failures across dependent services. Thousands of enterprises were affected during a prolonged recovery, with disruptions lasting several hours for many users.
Cloudflare	Digital services	2025 (Q4)	Configuration error/ software	A configuration error in Cloudflare's Bot Management system caused proxy failures and widespread service disruption. Millions of outage reports were recorded, with significant downstream incidents affecting online services and merchants.
CME/ CyrusOne	Digital services	2025 (Q4)	Cooling failure	A procedural error during cooling system maintenance caused a chiller failure, resulting in an 11-hour outage that affected global trading systems. Major financial markets were disrupted, with significant impacts on trading activity.

UPTIME INSTITUTE 2026

Cost of outages

The cost of data center outages continues to rise. The Uptime Institute Global Data Center Survey 2025 revealed that, for the second year in a row, one in five outages exceeds $1 million in total costs (see **Figure 16**). Additionally, a growing share of outages cost between $100,000 and $1 million. This is partly due to persistent challenges such as inflation, rising labor and hardware costs, service level agreement (SLA) penalties and longer recovery times persist. But primarily, it is caused by the increasing number of services and businesses that may be dependent, directly or indirectly, on a single data center or availability zone.

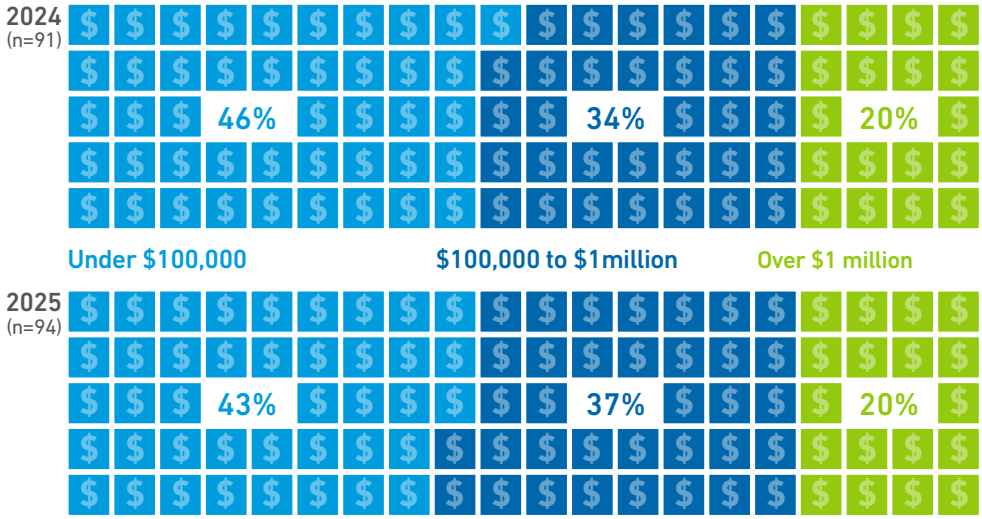
At the same time, failures increasingly affect interconnected systems spanning cloud platforms, networks and third-party providers, amplifying downstream effects. This interdependence can make incidents harder to contain and prolong recovery efforts, increasing both direct and indirect costs.

This trend is likely to intensify in the coming years. The growth of AI and high-density compute is increasing both the value of uptime and the potential cost of disruption, particularly for time-sensitive or resource-intensive workloads. As a result, outage costs are likely to remain elevated, driven less by the frequency of failures and more by the scale, complexity and criticality of the systems they affect.

Figure 16

Outage costs rise steadily

Estimate the total cost of this downtime incident (from outage to full recovery), including direct, opportunity and reputation costs.



UPTIME INSTITUTE GLOBAL DATA CENTER SURVEY 2025

Building resiliency and assessing risk

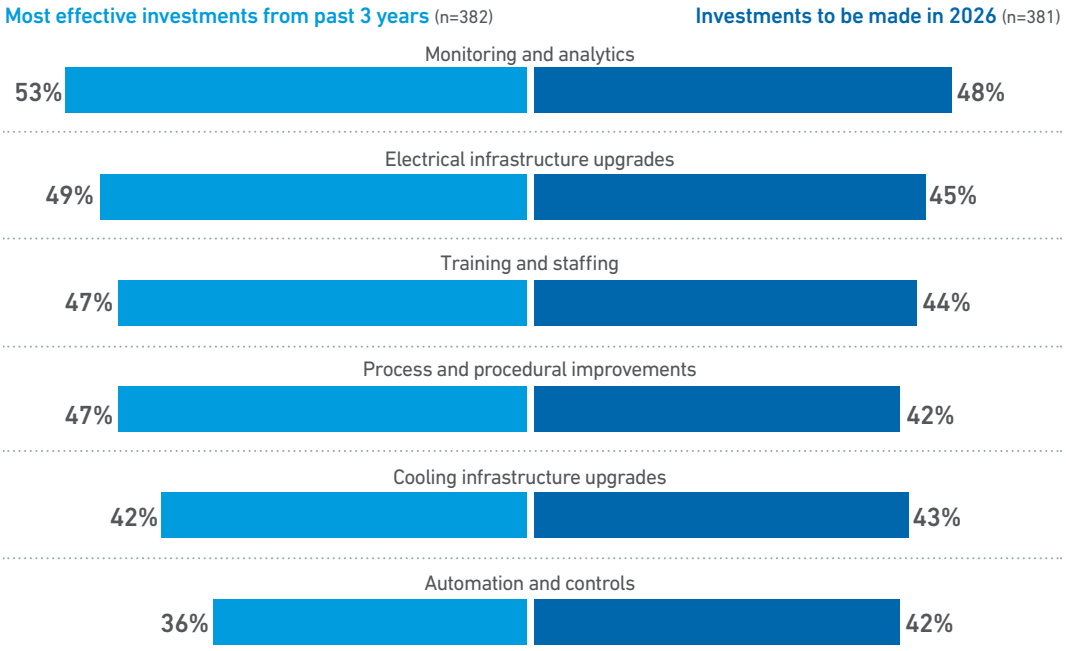
Operators continue to invest heavily in resiliency. Recent gains in availability have undoubtedly been helped by infrastructure upgrades, improved monitoring and stronger operational practices. Over the past three years, monitoring and analytics, electrical systems, and process and staffing improvements have delivered the greatest benefits (see **Figure 17**).

Looking ahead, investment is shifting toward automation and controls, alongside continued upgrades to cooling and power systems. This points to a transition from strengthening the core infrastructure to managing more dynamic, large-scale environments.

Figure 17

Monitoring and analytics tools lead resiliency investments

Which of the following investments have been most effective at improving resiliency in your organization's data centers over the past three years; and which of these investments will your organization be increasing in 2026 to improve resiliency?



UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2026

Taken together, these findings suggest that the industry is continuing to invest in improving resiliency, despite the new imperatives of AI and the increasing complexity of the operating environment. The role of software, and ultimately automation, is becoming ever more critical.

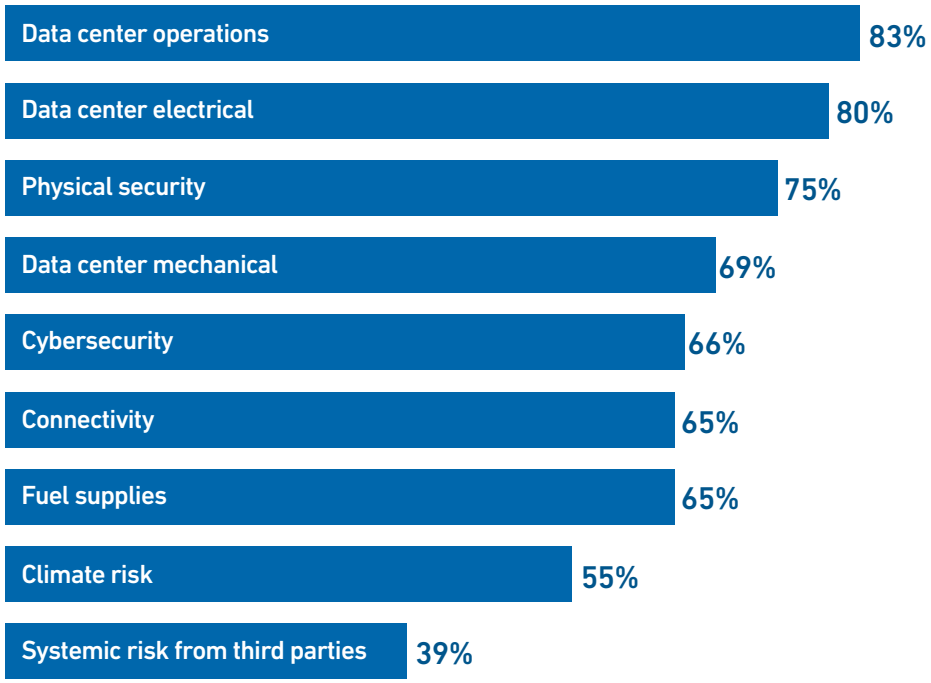
New technologies are introducing additional challenges while also enabling more advanced approaches to monitoring and control. Continued improvement, however, may depend on extending resiliency practices beyond the facility, with greater focus on external dependencies and coordination across systems. This may involve developing monitoring capabilities that extend beyond the facility to the third parties, where some of the major risks lie.

Uptime's data shows that most operators — nearly four out of five in recent years — conduct their own risk assessments. However, only about 40% assess third-party and systemic risks, a question asked for the first time in 2026 (see **Figure 18**). With so many interconnected critical services, often running at near capacity, there is a risk that a single failure can trigger cascading disruptions — sometimes affecting services operated by organizations only loosely or indirectly connected to those suffering the initial failure.

Figure 18

Fewer operators assess systemic third-party risk

Which of these areas are covered by your resiliency risk assessments? Choose all that apply. (n=310)



UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2026

Summary

As digital infrastructure continues to support an expanding range of critical services, high availability and resiliency remain central priorities for data center operators. AI makes little or no difference to this imperative.

Uptime's research indicates that the industry as a whole is making steady progress: outage frequency continues to decline, and investments in infrastructure, monitoring and operations are improving overall performance.

However, recent trends suggest that further gains are becoming harder to achieve. Improvements in outage frequency have slowed, and the proportion of the most severe incidents has largely stabilized. At the same time, a growing share of incidents are preventable, underscoring the need to strengthen processes, training and system design.

Risk is also becoming more distributed — spanning power systems, software, networks and external dependencies. As a result, outages are less often caused by isolated faults and more often by interactions between systems.

Operators are responding to these challenges. Investment priorities are shifting toward automation, monitoring and controls that enable more dynamic operations, while resiliency assessments continue to cover key areas such as operations, electrical systems, mechanical systems, cybersecurity and connectivity. Software-based resiliency, distributed architectures and improved operational discipline are helping to limit the impact of incidents, even as environments grow more complex.

Maintaining reliability in the coming years will require extending these practices beyond the facility itself. External risks — including power constraints, network dependencies and third-party services — are playing a larger role in outage events. With continued focus on coordination, visibility and process improvement, operators are well positioned to manage these evolving risks and sustain progress in resiliency.

Appendix

Sources and methodology

Uptime Institute currently has four main data sources for monitoring data center and IT outages or incidents that could lead to outages:

Uptime Institute Global Data Center Survey

This long-running series of global annual surveys asks detailed questions about outages. Some of the findings are discussed here. This represents the most statistically significant dataset relating to outages in the critical infrastructure industry.

Uptime Institute Data Center Resiliency Survey

This global survey specifically focuses on outages and resiliency-related issues. The first survey was conducted in January 2021, with 642 respondents split between data center operators and suppliers/services companies. The results are compared and contrasted with those from the Uptime Institute Global Survey of IT and Data Center Managers, which is conducted midyear.

Uptime Institute Intelligence's public outages database

Since the beginning of 2016, Uptime Institute has collected data about major IT outages from media reports and other public sources (social media, outage detection sites, etc.). This has enabled us to collect information on major outages that become visible to the public and the media, and to identify patterns over time.

Uptime Institute's Abnormal Incident Report (AIRs) database

This is a long-standing confidential system for global Uptime Institute members to share details of incidents under a nondisclosure agreement. Most incidents recorded do not actually lead to outages — many are "near misses". We do not include such incidents in the analyses described in this report.

Uptime Institute Professional Services

This is a less formalized source of information. Uptime Institute conducts Digital Resiliency Assessments and root-cause analyses of failures on behalf of clients globally. Although these assignments are confidential, the experience garnered from these incidents informs our analyses.

The public outages media database, used for some of the findings in this report, is particularly limited and the data should be understood in this way — it is primarily useful for trending. Moreover, while we believe it is directionally accurate, it is not a representative dataset for all outages. There are several limitations:

- If a failure is not reported or picked up by the media or Uptime Institute, it will not be recorded. This immediately means there is a bias toward coverage of large, public-facing IT services, and sometimes more so in geographies with a well-developed and open media.
- Uptime limits failures to those that had a noticeable impact on end users — a major fire during data center commissioning, for example, may never be registered. All Category 1 outages have been eliminated — small, short failures where the business or reputational impact is negligible.
- The amount of information available varies widely from outage to outage, and sometimes there is very little. It has regrettably been necessary, in some of the analyses, to include outages for which the cause is "not known" — which means information was never disclosed.
- Finally, while Uptime includes IT system failures, cybersecurity breaches are generally not included, except those that can lead to complete service interruptions.

Other related content published by Uptime Institute includes:
The Uptime Institute Global Data Center Survey 2025
Annual outage analysis 2025

About the authors

Douglas Donnellan

Douglas Donnellan is a Research Analyst at Uptime Intelligence covering sustainability in data centers. His background includes environmental research and communications, with a strong focus on education.

ddonnellan@uptimeinstitute.com

Andy Lawrence

Andy Lawrence is Uptime Institute's Executive Director of Research. He has spent three decades analyzing developments in IT, emerging technologies, data centers and infrastructure, and advising companies on their technical and business strategy.

alawrence@uptimeinstitute.com

Rose Weinschenk

Rose Weinschenk is a Research Associate at Uptime Institute covering staffing and education in data centers. Her background includes psychology research, with a focus on ethics.

RWeinschenk@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. With over 4,000 awards issued in over 122 countries around the globe, and over 1,100 currently active projects in 80+ countries, Uptime has helped tens of thousands of companies optimize critical IT assets while managing costs, resources, and efficiency. For over 30 years, the company has established industry-leading benchmarks for data center performance, resilience, sustainability, and efficiency, which provide customers assurance that their digital infrastructure can perform across a wide array of operating conditions at a level consistent with their individual business needs. Uptime's Tier Standard is the IT industry's most trusted and adopted global standard for the design, construction, and operation of data centers. Offerings include the organization's Tier Standard and Certifications, Management & Operations reviews and assessments including SCIRA-FSI financial sector risk assessment, the Sustainability Assessment, and a broad range of additional risk management, performance, availability, and related offerings. Uptime Education training programs have been successfully completed by over 100,000 data center professionals, such as the much-valued ATD (Accredited Tier Designer) and AOS (Accredited Operations Specialist). The Uptime Education curriculum has been expanded by the acquisition of CNet Training Ltd. In 2023.

Uptime Institute is headquartered in New York, NY, with offices in London, Sao Paulo, Dubai, Riyadh, and Singapore, and full-time Uptime professionals based in over thirty-four countries around the world.

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