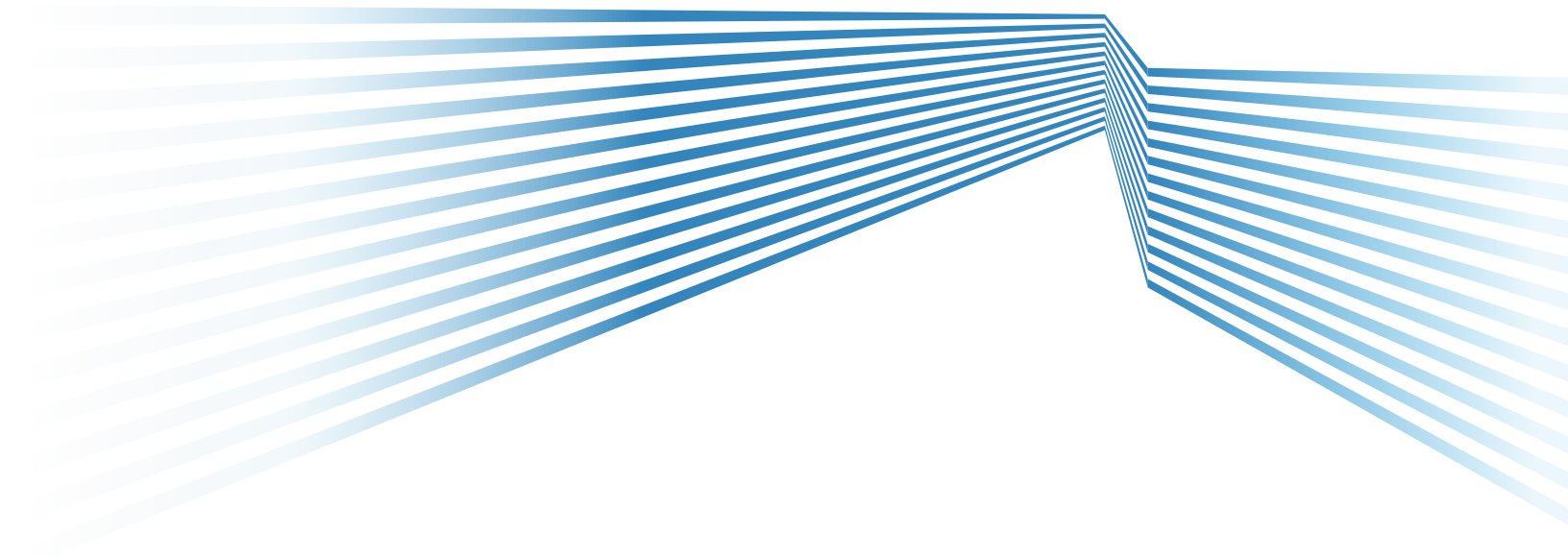
uptime INTELLIGENCE

# Annual outage analysis 2025

**The causes and impacts of IT and data center outages**

Preventing outages continues to be a strategic priority for data center owners and operators. While infrastructure equipment — as well as the design and resiliency of data centers — has improved, the complexity of modern architectures and evolving external threats present new risks that operators must actively manage. 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

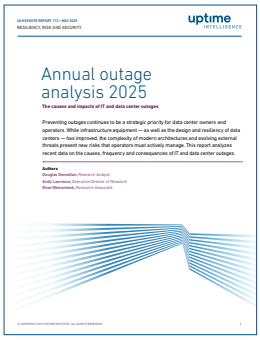


© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

# Key findings

- For the fourth consecutive year, Uptime Intelligence research suggests that overall outage frequency and the general level of reported severity continue to decline. However, cyber incidents are rising and often have severe, lasting impacts.
- In 2024, a higher proportion of publicly reported outages — via news, social media and self-reported — tracked by Uptime Intelligence had severe impacts compared with previous years.
- More than half (54%) of the respondents to Uptime's 2024 annual survey say their most recent significant, serious or severe outage cost more than $100,000, with one in five saying that their most recent outage cost more than $1 million.
- Power issues remain the most common cause of serious and severe data center outages. However, outages caused by IT and network-related issues are increasing.
- The failure of staff to follow procedures has become an even greater cause of outages than in the previous year, suggesting a major opportunity to reduce incidents through training and process review.
- Data relating to outages should be treated skeptically. All methodologies used to track the frequency, severity and costs of outages are subject to uncertainty, partly because of a lack of transparency and reliable reporting mechanisms.

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED




# Contents

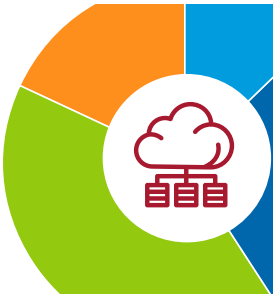
Introduction 5
Outage frequency and severity 7
Outage causes 9
- Cloud and third-party provider reliability 13
- Power outages 15
- Networking outages 16
- System and software outages 17
- The human factor 18

Cost of outages 22
Summary 23
Appendix: Sources and methodology 24

**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.

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

# Contents (continued)



## Figures and tables

**Table 1** 5
How Uptime Institute tracks outages

**Table 2** 6
Outage severity rating

**Figure 1** 7
Most operators had no or negligible outages in the past three years

**Table 3** 8
Publicly reported outages tracked by Uptime, 2016 to 2024

**Figure 2** 9
Proportion of publicly reported outages that were serious or severe, 2020 to 2024

**Figure 3** 10
Power is still the leading cause of impactful outages

**Figure 4** 10
Most common causes of IT service-related outages

**Figure 5** 11
Causes of publicly reported outages, 2024

**Figure 6** 12
Publicly reported outages by sector, 2020 to 2024

**Figure 7** 13
Most say cloud only resilient enough for some workloads

**Figure 8** 14
Most common causes of major third-party outages

**Figure 9** 15
Most common causes of major power-related outages

**Figure 10** 16
Most common causes of major network-related outages

**Figure 11** 17
Most common causes of major IT system-/software-related outages

**Figure 12** 19
Most common causes of major human error-related outages

**Figure 13** 19
Most say outages preventable with better management

**Figure 14** 20
Durations of publicly reported outages, 2020 to 2024

**Table 4** 21
Ten major outages in 2024 and 2025

**Figure 15** 22
Half of impactful outages cost more than $100,000

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

# Introduction

This report on digital infrastructure outage trends is the seventh edition in an ongoing series from Uptime Institute 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 Annual Global Data Center Survey 2024 and the Uptime Institute Data Center Resiliency Survey 2025) 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 2025

In this report we use three primary sources:

- The Uptime Institute Annual Global Data Center Survey 2024. This was conducted in March and April of 2024, with more than 850 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.
- The Uptime Institute Data Center Resiliency Survey 2025, conducted in February and March 2025, 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.
- Publicly reported/tracked outages tracked by Uptime in 2024 and the first quarter of 2025. 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.

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

Throughout 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 2025

IT service reliability continues to improve in 2025. However, as businesses and individuals increasingly depend on digital services, outages can have immediate and far-reaching consequences. Failures now affect end users more quickly than in previous years, sometimes due to interdependencies between separately operated services. The impact is often amplified by media coverage and social platforms, compounding both reputational and operational damage.

This growing reliance on digital infrastructure also makes it a high-value target for malicious actors and a factor in geopolitical conflict. Cyberattacks are becoming more sophisticated, and as operators adopt smart, connected devices to manage physical infrastructure, the attack surface widens — raising both the likelihood and potential severity of disruptions.

At the same time, maintaining availability is becoming more challenging and costly. Emerging technologies, particularly those driven by AI, offer promising opportunities to enhance efficiency and resiliency. However, most AI deployments are still nascent, and their risks, limitations and operational demands are not yet fully understood across the industry.

The high power demands of AI have also raised questions about the affordability of end-to-end concurrent maintainability, while liquid cooling technologies have forced a rethink over resilient designs (see *AI embraces liquid cooling, but enterprise IT is slow to follow*).

Data center operators also face intensifying external pressures. Regulators are tightening mandates around cybersecurity, sustainability and energy use, while geopolitical instability and trade tensions add uncertainty to global expansion and investment decisions.

Despite these evolving risks, most IT service outages remain brief and have limited impact. On both the IT and facilities sides, operators frequently experience contained and rapidly resolved outages. This report focuses on the significant, serious and severe outages (categories 3, 4 and 5) that can have serious consequences for businesses and governments. As digital infrastructure grows in complexity, avoiding such events continues to require careful management, resilient design and sustained investment in operations.

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

# Outage frequency and severity

Uptime Intelligence conducted analysis using the latest data from reports and surveys in both 2024 and 2025. For the fourth consecutive year, the data indicates that the frequency of outages, relative to the overall workload, is decreasing.

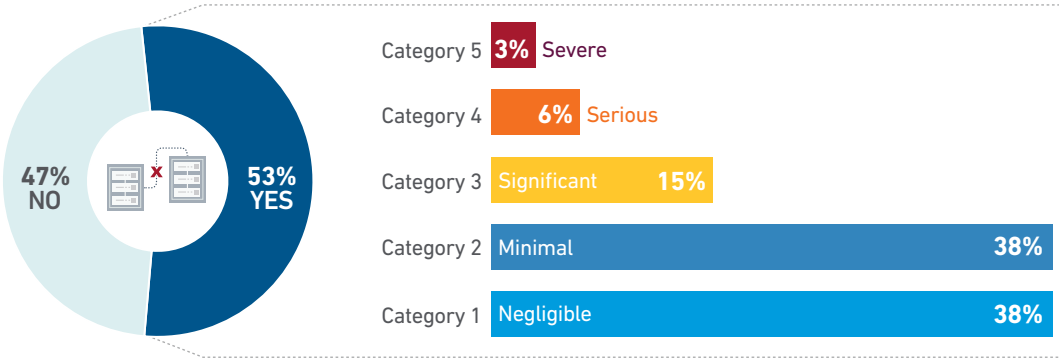
In the Uptime Institute Global Data Center Survey 2024, more than half (53%) of operators reported an outage in the past three years (see **Figure 1**). This rate continues a trend — with notable drops from 60% in 2022, 69% in 2021, and 78% in 2020. However, year-over-year improvement has slowed — the 2024 figure was down just two percentage points (55%) from 2023.

There are also signs that outage severity is decreasing. Only 9% of reported incidents in 2024 were classified as serious or severe — the lowest level recorded by Uptime to date.

**Figure 1**

## Most operators had no or negligible outages in the past three years

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=768)




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

UPTIME INSTITUTE GLOBAL DATA CENTER SURVEY 2024

These findings suggest that the industry's ongoing investments in availability — through redundancy, process improvements and operational discipline — are having a measurable effect. Some observations on these trends include:

- **Outages are becoming less frequent and less severe relative to the rapid growth of digital infrastructure.** This trend has held for several years, underscoring industry progress in risk management and reliability. However, workloads cannot be accurately measured across this (or any) sample. As a result, a rate-per-megawatt figure is not available.
- **The slowdown in improvement does not imply complacency.** Operators face mounting external risks that are largely beyond their control — including power grid constraints, extreme weather, network provider failures and third-party software issues. Improvements are occurring despite a more volatile risk landscape.

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

- **Software-based and distributed resiliency tools are expanding.** These systems improve uptime but can also introduce new risks and complexities. The use of software-based resiliency strategies alongside physical failover/redundancy is undoubtedly contributing to overall improvements in availability. However, the added complexity brings its own challenges and can blur lines of responsibility for failures, complicating root cause analysis and outage classification.
- **The pace of industry transformation is accelerating.** Soaring demand for AI is straining existing infrastructure designs — especially around power and cooling — while electricity grid limitations and global trade tensions introduce new uncertainty in supply chains and expansion plans. Together, these pressures could eventually affect the stability of current reliability trends.

Uptime anticipates continued growth in both distributed, software-based resiliency models and traditional site-level redundancy. Recent Uptime research supports this, with increased resiliency and support for hybrid cloud cited among the top drivers of data center demand (see *AI adds to rising demand for capacity*). However, the need to support AI workloads may complicate how and where these models are applied.

Hybrid cloud platforms such as AWS Outposts and Azure Arc, along with management frameworks such as VMware Cloud Foundation, have matured significantly, improving integration with on-premises infrastructure. These trends confirm that on-premises resiliency remains critical, with third-party infrastructure used strategically based on cost, risk tolerance and specific workload requirements.

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 nine 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 2024, we collected details of 119 outages.

Table 3

### Publicly reported outages tracked by Uptime, 2016 to 2024

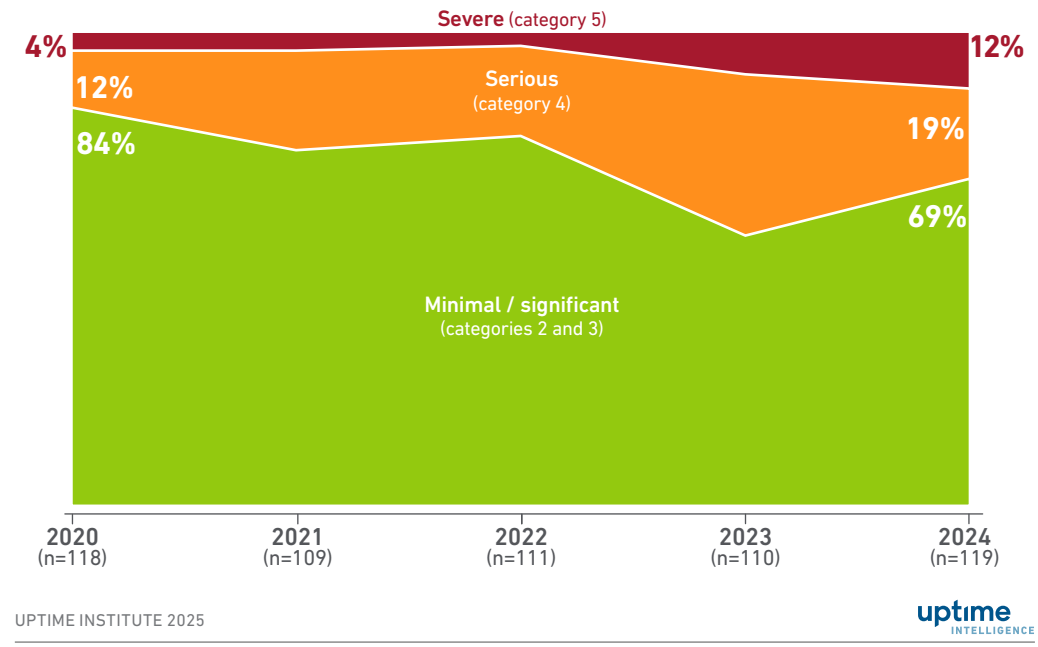
| 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | Total |
|---|---|---|---|---|---|---|---|---|---|
| 27 | 57 | 71 | 165 | 118 | 109 | 111 | 110 | 119 | 893 |

UPTIME INSTITUTE 2025

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

The proportion of publicly reported outages that were severe increased in 2024. While **Figure 2** shows that category 4 outages decreased by 10 percentage points from 2023, category 5 outages increased by seven percentage points in the same period. This is because major outages are now more disruptive and expensive as other industries become more dependent on digital services. As a result, these outages are more likely to be reported in public media outlets than those with less impact.

**Figure 2** **Proportion of publicly reported outages that were serious or severe, 2020 to 2024**




This data also suggests that each year there will probably be 10 to 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

Identifying the causes of outages is critical for reducing recurrence and guiding future investments in resiliency. However, root cause analysis remains difficult, as most outages involve interdependent failures across infrastructure, software and operations.

Uptime's annual survey finds that on-site power distribution failures remain the most common cause of serious outages (see **Figure 3**). This is consistent with previous years and underscores the vulnerability of IT equipment to even brief power disruptions — including voltage sags, switching events and total power loss.

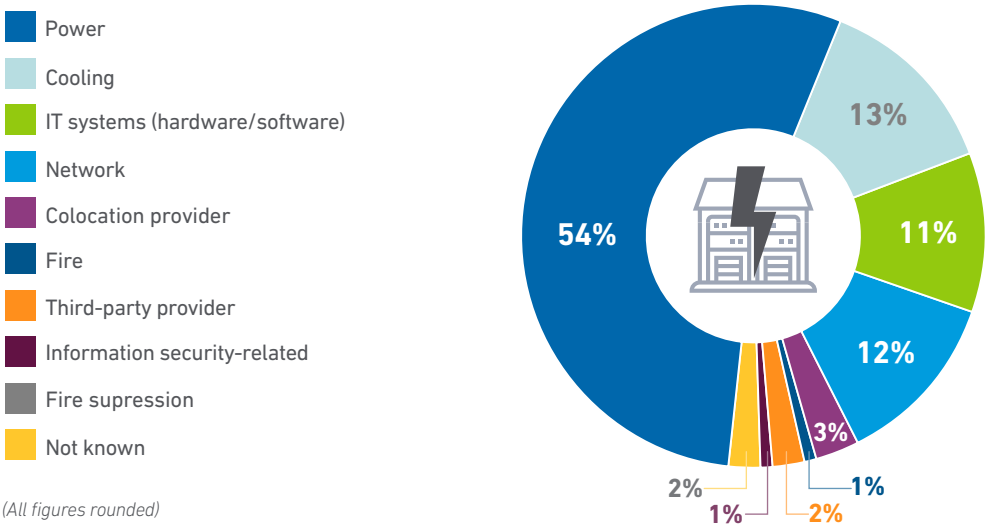
Cooling-related failures are less frequent than those caused by power issues, but they consistently account for roughly one in eight impactful outages annually. This may shift in the coming years. Expected increases in rack power density may lead to higher failure rates, although operators may respond with added redundancy or deploy UPS support for cooling systems.

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

**Figure 3**

## 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=97)




*(All figures rounded)*

UPTIME INSTITUTE GLOBAL DATA CENTER SURVEY 2024

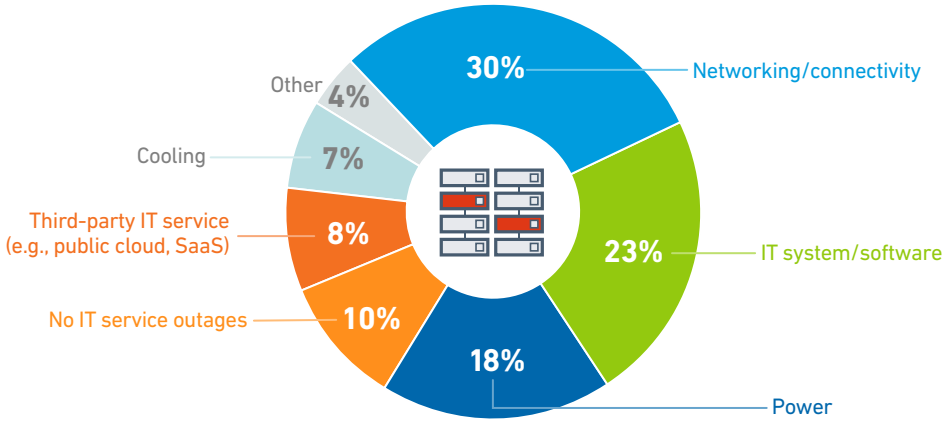
Outages from IT and networking issues increased in 2024, totaling 23% of impactful outages. This rise is likely caused by increased IT and network complexity, leading to issues with change management and misconfigurations.

For a more general view of outage causes that extend beyond (but include) the data center, the Uptime Institute Data Center Resiliency Survey 2025 also asks about the most common causes of any end-to-end IT service outages, regardless of whether they were the most recent or the most impactful. The responses have consistently shown that network-related outages are more common, and significantly ahead of power (see **Figure 4**).

**Figure 4**

## 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=412)




UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2025

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

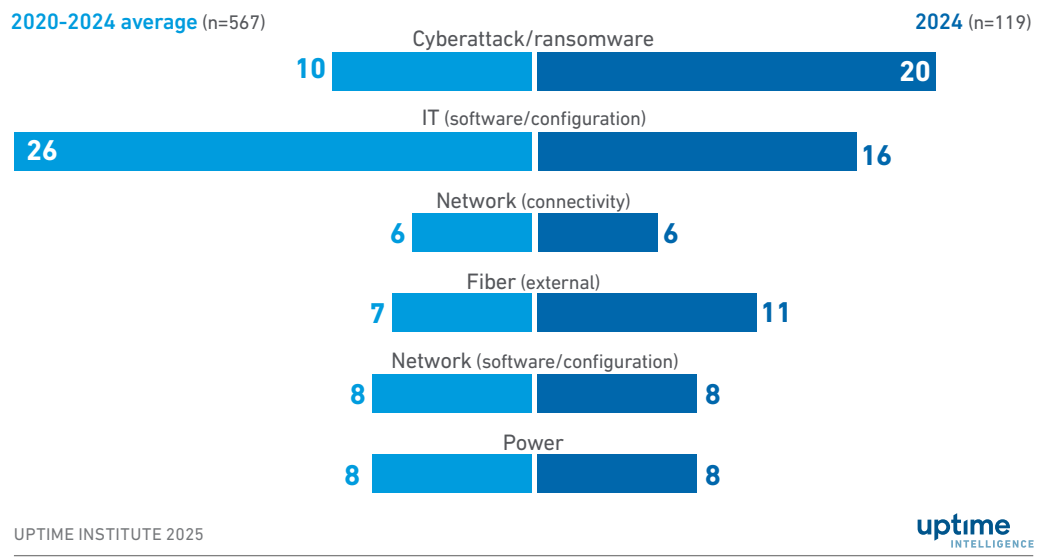
PUBLICLY REPORTED OUTAGES

## Cyberattacks lead causes of major public outages

Cyberattacks — particularly ransomware — were the leading publicly reported cause of IT service outages in 2024, showing the greatest increase compared with the 2020–2024 average (see **Figure 5**). Public outage data compiled by Uptime Intelligence includes all causes seen by the public — not just data center-specific issues. The rise in cyberattacks reflects multiple factors: increased reliance on digital infrastructure across industries, expanding attack surfaces due to complex hybrid IT environments and remote management tools, and escalating risks from third-party software and supply chains.

Attackers can infiltrate networks long before deploying ransomware, often exfiltrating or encrypting sensitive data. The true impact may be even greater than reported because some incidents may not be fully or accurately reported, or may be misattributed by operators.

Figure 5 Causes of publicly reported outages, 2024




© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

PUBLICLY REPORTED OUTAGES

## Commercial operators in the limelight

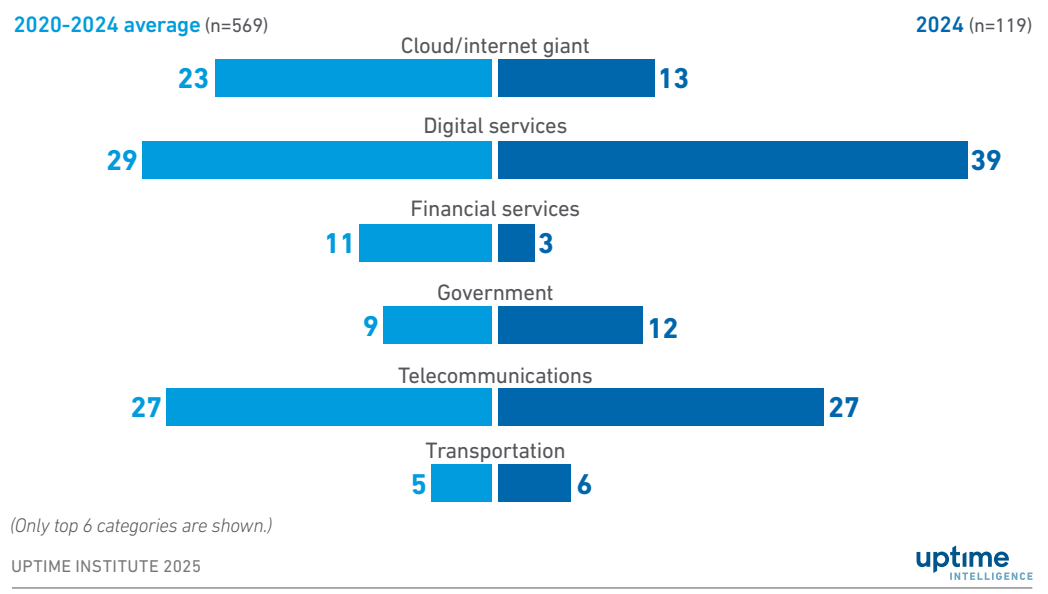
Over the nine years that Uptime has been tracking publicly reported outages, third-party IT and data center service providers — including cloud and internet giants, telecommunications and colocation companies — have accounted for about two-thirds of those reported (see **Figure 6**). This trend reflects the long-term move toward colocation providers, cloud and other third-party services. While outsourcing may reduce the risk for some enterprises, major failures still occur, sometimes with serious consequences.

In 2024, outages attributed to digital service providers increased, while those from cloud/internet giants declined — possibly due to hyperscalers' investments in distributed resiliency and regional failover.

For the third consecutive year, the financial sector saw a decline in outage frequency compared with the long-term average since 2020. This improvement may reflect the impact of stricter regulations and heightened oversight following several major, high-profile outages prior to 2021.

Figure 6

### Publicly reported outages by sector, 2020 to 2024




© COPYRIGHT 2024 UPTIME INSTITUTE. ALL RIGHTS RESERVED

## Cloud and third-party provider reliability

Cloud and internet-based services are built for high availability, leveraging distributed infrastructure (availability zones and regions), layered software architectures and dynamic traffic rerouting. These design strategies allow major cloud and IT providers to minimize outages at scale. However, as these systems grow more complex and interdependent, failures remain inevitable. Some failures, although rare, can cascade and become systemic — affecting multiple services, zones or regions.

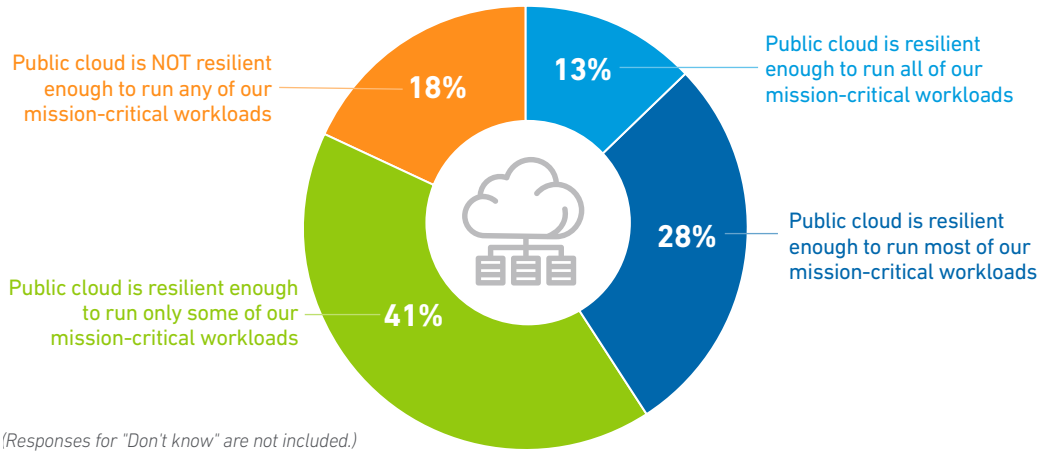
As more enterprises shift core operations to the cloud, the impact of even brief outages is magnified — often disrupting thousands of users and drawing significant public scrutiny. This partly explains why many organizations remain cautious about entrusting their critical workloads to third-party platforms. Another commonly cited reason is the lack of transparency and oversight (discussed below).

Only 13% of respondents to the Uptime Institute Data Center Resiliency Survey 2025 believe public cloud services are resilient enough for all their mission-critical workloads — down three percentage points from 2024. Nearly one in five (18%) say they are not comfortable placing any mission-critical workloads in the public cloud — a figure consistent with previous years. Most organizations fall somewhere in between, carefully weighing the trade-offs between agility, cost and operational control (see **Figure 7**).

Figure 7

### 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 2025

Despite these concerns, Uptime Intelligence data shows the average application availability annually is 99.97%, which is equivalent to around three hours downtime per year (see *Outage data shows cloud apps must be designed for failure*). When applications are deployed across cloud regions, availability improves further. Organizations should not automatically rule out public cloud for their workloads. The suitability of public cloud should be assessed in terms of specific application requirements relating to cost, security and performance.

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

For the second consecutive year, data security was the most frequently cited obstacle to placing mission-critical workloads in the cloud (60%, n=248). While cloud providers continue to invest heavily in security and emphasize their strong performance in this area, enterprises are often deterred by limited visibility and a perceived lack of control.

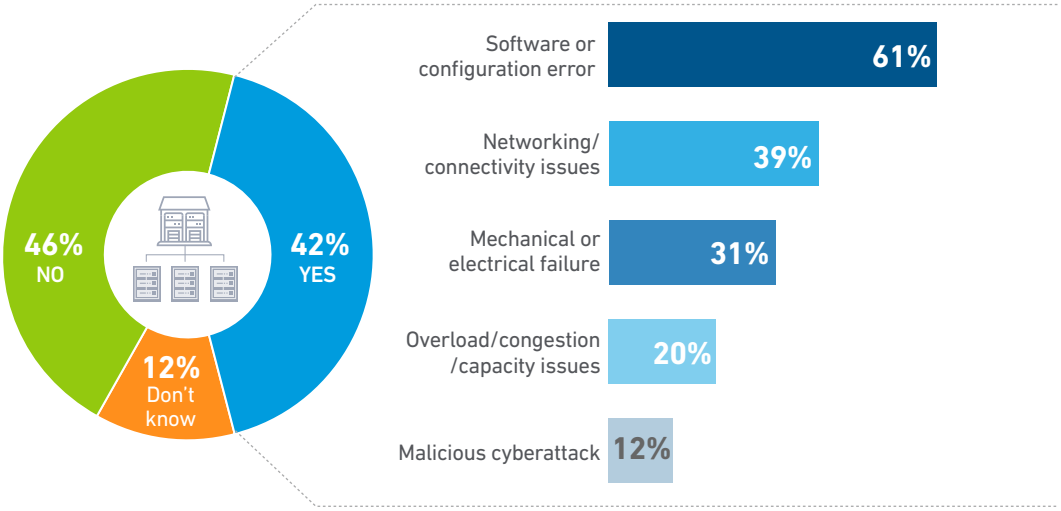
Among the respondents who do not use the public cloud for critical workloads (n=407), 36% say they would reconsider if providers offered greater transparency into service resiliency. In financial services, some of this transparency and control is now being mandated through the Digital Operational Resilience Act (DORA) — an EU regulation that may become a blueprint for legislation across more countries and sectors (see *DORA update: what the EU act means for data centers*).

Software and configuration errors linked to third-party IT service outages likely reinforce the security concerns that trouble enterprise IT managers. These errors are the most common cause of outages stemming from third-party issues (see **Figure 8**) and can also lead to data breaches. For example, incorrect access settings or misconfigured encryption can disrupt services and expose vulnerabilities in security systems. While just 12% of these third party-related outages are caused by cyberattacks, this number is expected to grow. Cyberattacks often create a need for system resets and reconfigurations, which introduces a window for further problems to occur.

Figure 8

## Most common causes of major third-party outages

Has your organization experienced a significant, serious, or severe IT service outage(s) that was caused by a problem with a third-party IT service provider over the past three years? If so, what are their most common causes? Choose no more than three. (n=207)




*(Only top 5 outage categories are shown.)*

JPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2025

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

## Power outages

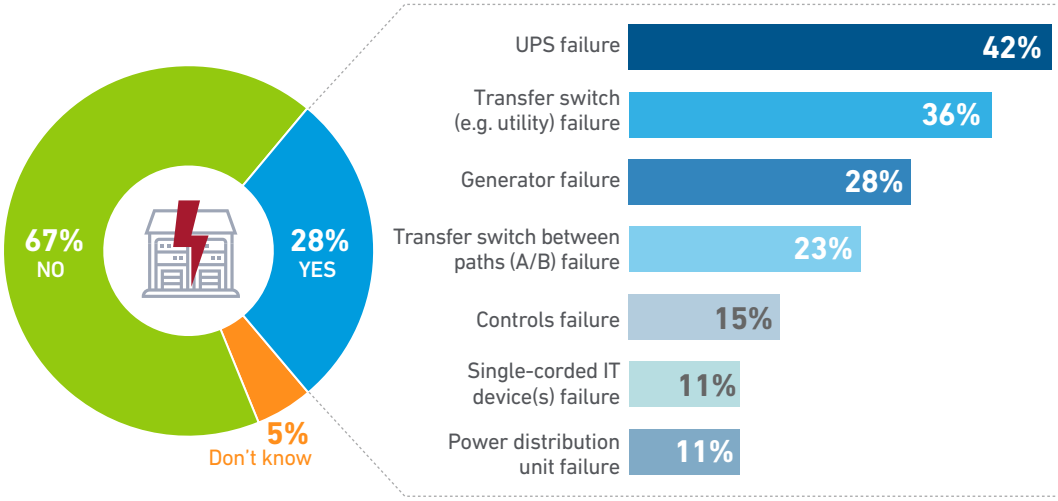
Year after year, Uptime's annual survey data shows that power-related incidents remain the leading cause of major outages, accounting for more than half of all cases (see **Figure 3**). Power failures at a rack, data hall or site level can all be highly disruptive, partly because the impact is usually immediate and total — all systems in the affected domain are lost, and many connected systems may experience data loss or service interruptions. In addition, rebooting systems, resynchronizing data and addressing damaged equipment can further extend outage durations by several hours — even if electrical service is restored quickly.

More than one in four respondents to the 2025 Uptime resiliency survey report a serious or severe IT outage at their site due to a power issue within the past three years (see **Figure 9**). Given the centrality of power to data center operations, many of these likely involved full site outages.

Figure 9

### Most common causes of major power-related outages

Has your organization experienced a significant, serious, or severe IT service outage(s) that was caused by a problem with a power system over the past three years? If so, what are their most common causes? Choose no more than three. (n=409)




*(All figures rounded. Only top 7 categories are shown.)*

UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2025

The most frequently cited cause is UPS failure — a trend that has persisted since Uptime began tracking these responses. As in previous years, Uptime engineers working across many data centers report the following as the most common problems with static UPS systems:

- Fans fail frequently because they are usually inexpensive and constantly in operation. A single fan failure does not take down a unit, but the failure of multiple fans may.
- Snubber capacitors can fail from wear and tear. Regular preventative maintenance will reduce the number of failures.
- Batteries fail because of age. They require good management, close monitoring and adherence to replacement schedules. Many batteries fail because they are not monitored closely enough by experienced technicians.
- Inverter stack failures are least common. These are more likely to occur when the unit is overloaded, although wear and tear can also cause failures.

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

Other elements in the power chain, such as generators and automatic transfer switches (ATS), are generally reliable but still vulnerable. Generators must be regularly tested, serviced and fueled to remain effective, while ATS units can fail due to control system malfunctions or mechanical issues such as jammed switches or worn-out bearings. In recent years, outages have been caused by intermittent faults in the power supply and by mismanaged or misconfigured failover to generators.

Beyond the facility, grid instability is a growing concern. Rising demand, aging infrastructure, extreme weather and the variability of renewable energy sources may increase the frequency of external power disruptions — making robust on-site systems even more essential. Even in countries with a long history of grid stability, there is some evidence that failures are becoming more likely.

## Networking outages

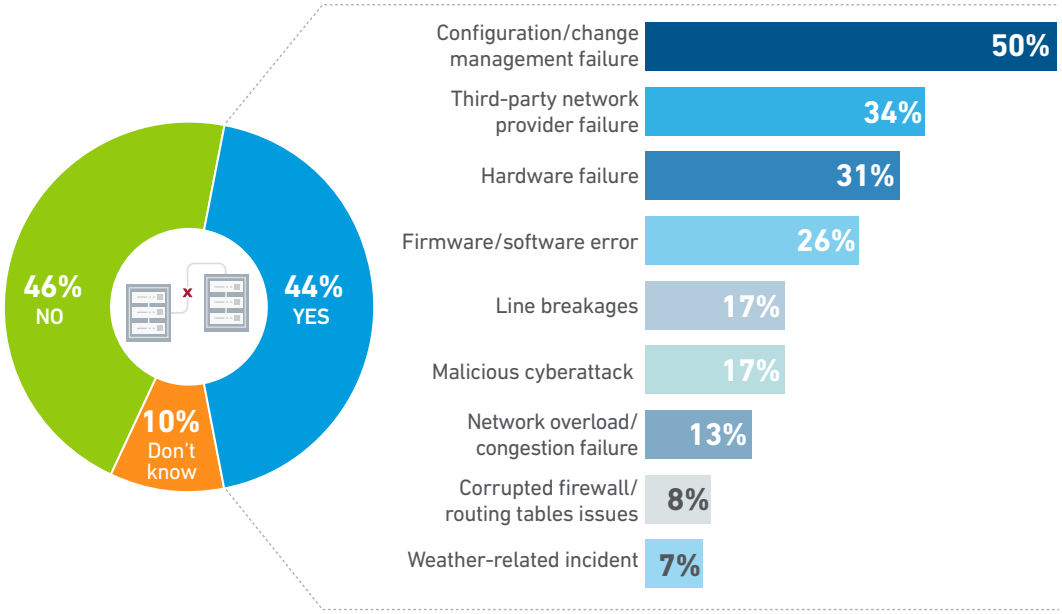
Network-related issues continue to play a growing role in IT service outages. The 2025 Uptime resiliency survey again identifies configuration and change management errors as the top cause of these incidents (see **Figure 10**).

Issues with third-party network providers — previously a close second as a cause of corporate outages — declined by eight percentage points compared with 2024. This continues a trend of improvements brought about by software-defined networking (SDN), such as better automated failover, route switching and anomaly detection.

Figure 10

### Most common causes of major network-related outages

Has your organization experienced a significant, serious, or severe IT service outage(s) that was caused by a problem with networking/connectivity over the past three years? If so, what are their most common causes? Choose no more than three. (n=414)




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

UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2025

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

While centrally managed networks and architectural approaches, such as SDN, can simplify network management, they can also introduce risks. Configuration changes can be deployed instantly across entire data center networks — but errors in those changes can also propagate quickly, potentially causing widespread outages. Careless or unchecked keystroke errors have caused some major, system-wide failures in recent years.

Similar to configuration errors in third-party and IT systems, network misconfigurations can also create vulnerabilities in security systems. Attackers may exploit these weaknesses through distributed denial-of-service (DDoS) attacks or Domain Name System (DNS) hijacking to disrupt traffic and bring down services. This may help explain the slight (five percentage point) increase in network-related outages attributed to cyberattacks compared with 2024.

## System and software outages

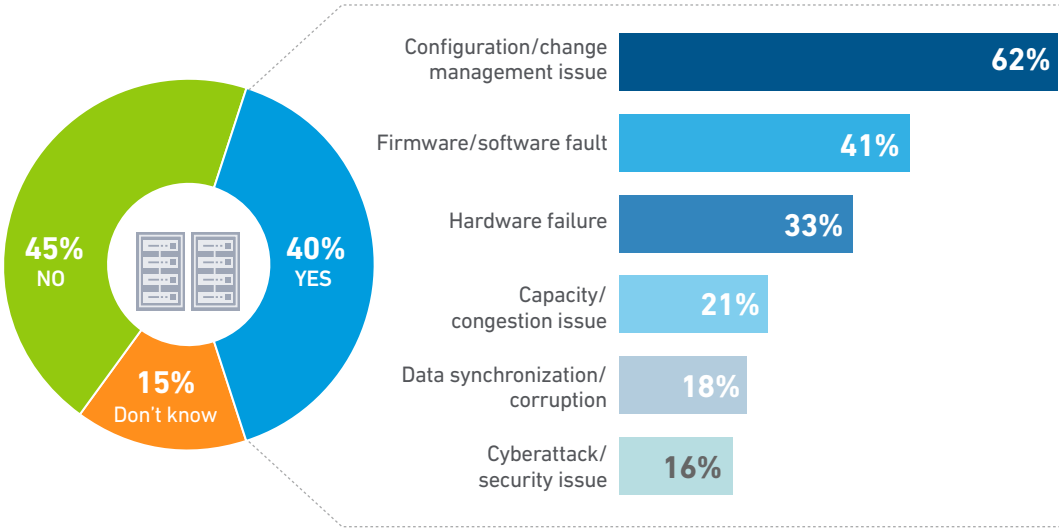
IT systems and software continue to be a major source of outages in 2025 — and the problem appears to be growing. While small, contained system errors and short outages occur regularly with almost all IT systems, for the fourth consecutive year a rising share of operators report experiencing a significant, serious or severe outage caused by IT system or software failures within the past three years (see **Figure 11**). Since 2022, this figure has climbed from 31% to 40%, a nine-percentage-point increase.

This trend reflects the growing complexity of digital infrastructure environments. As infrastructure becomes more automated, distributed and integrated with third-party platforms, errors can be harder to isolate and contain. While technical advances support scalability and improve availability in many cases, they can also introduce new points of failure and expand outage impacts.

Figure 11

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

Has your organization experienced a significant, serious, or severe IT service outage(s) that was caused by a problem with IT systems/software over the past three years? If so, what are their most common causes? Choose no more than three. (n=404)




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

UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2025

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

Notably, the distribution of root causes for IT software-related outages has remained stable for three years. Configuration and change management issues have consistently been responsible for around 60% of software-related outages since 2022. However, this apparent stability masks emerging risks tied to growing software supply chain complexity, shrinking maintenance windows and increasing dependency on interconnected platforms. Managing these risks is more challenging because change-related disruptions — especially those involving third-party systems — can be difficult to predict and test for.

Enterprises have made substantial progress in reducing the impact of these incidents through better processes and improved tools for anomaly detection, change simulation and sandboxing, and automated validation. Still, data center operators continue to struggle to keep pace with evolving security threats, capacity growth and performance requirements — suggesting that software-related outages may remain a persistent challenge.

Hardware and software bugs, while less common than change-related issues, still account for a meaningful share of outages. This underscores the importance of pairing resilient infrastructure design with up-to-date operational safeguards that reflect the speed and complexity of modern deployments.

## The human factor

Preventing human error remains one of the most persistent challenges in data center operations. Mistakes can arise from a range of issues — such as inadequate training, unclear procedures, operational complexity, staff fatigue or limited resources. Ambiguity around how incidents are defined can also complicate analysis. For example, it is often unclear whether a hardware failure caused by a software issue at the manufacturing stage qualifies as human error.

Uptime typically treats human error as a contributing factor rather than a root cause, but it is involved — directly or indirectly — in most outages. Historical data shows that between two-thirds and four-fifths of major IT and data center outages involve some element of human error.

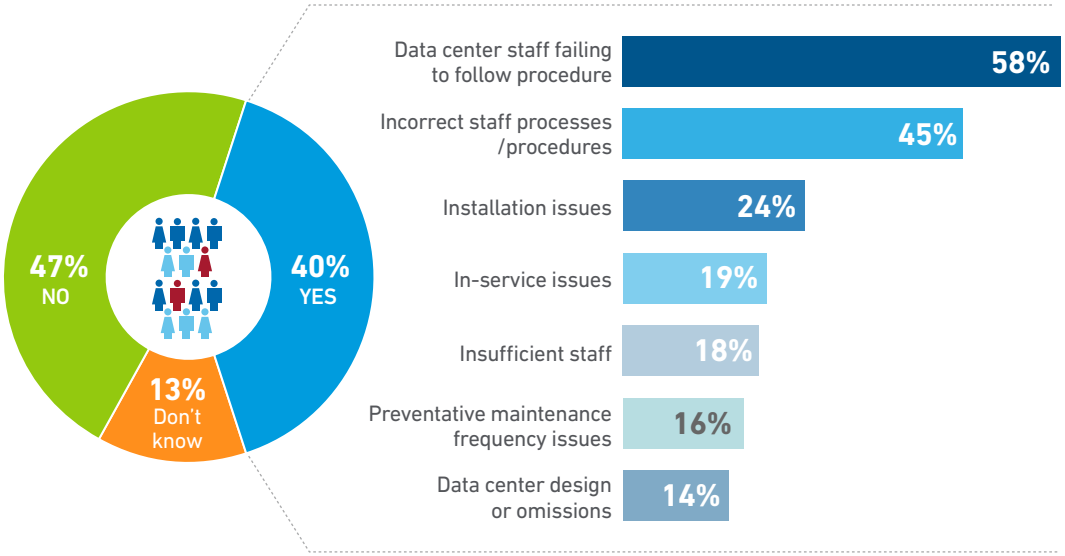
To better understand these dynamics, recent Uptime resiliency surveys have explored how human error occurs. As shown in **Figure 12**, most incidents stem either from staff not following established procedures or from flawed or insufficient processes.

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

Figure 12

## Most common causes of major human error-related outages

Has your organization experienced a significant, serious, or severe IT service outage(s) that was caused by human error over the past three years? If so, what are their most common causes? Choose no more than three. (n=397)




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

UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2025

In 2025, the proportion of human error-related outages caused by failure to follow procedures rose by 10 percentage points compared with 2024. The reason for this rise is unclear but it may be a consequence of the rapid growth of industry and the resulting staff shortages in many regions. While improving documentation and processes remains important, greater focus on staff training and real-time operational support may reduce risks more effectively.

The case for dedicating more resources to staff training and support is strengthened by results from a separate survey question, which shows that four in five (80%) operators believe that better management and processes would have prevented their organization's most recent downtime incident (see **Figure 13**). This proportion is consistent with previous years' data and suggests that further investments in this area can significantly reduce downtime incidents.

Figure 13

## Most say outages preventable with better management

Would your data center's most recent impactful downtime incident have been preventable with better management/processes or configuration? (n=97)




UPTIME INSTITUTE GLOBAL DATA CENTER SURVEY 2024

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

PUBLICLY REPORTED OUTAGES

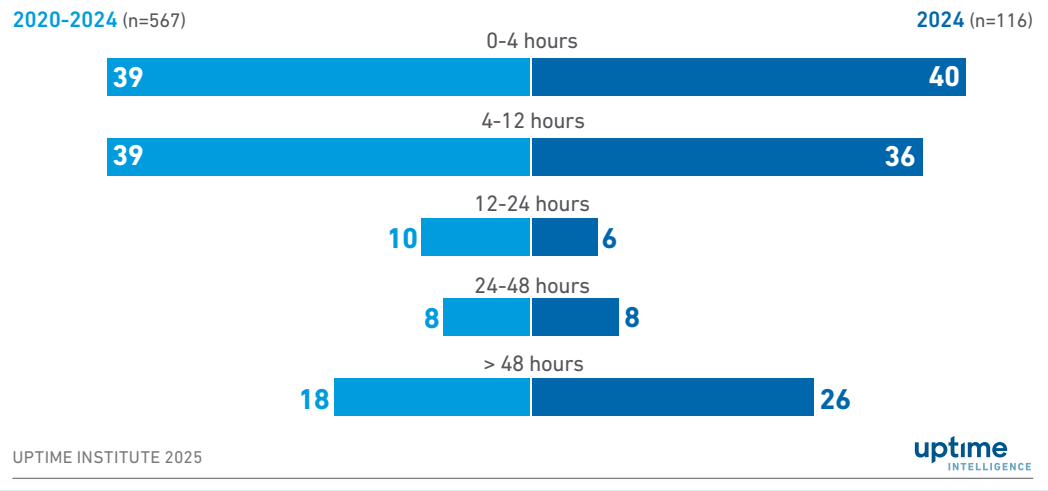
## Are big outages getting longer?

Longer outages are typically more costly and disruptive, increasing the likelihood of reputational damage and media attention. Even among publicly reported, high-profile incidents, most (66%) are resolved within 12 hours. However, one concerning trend stands out: the share of outages lasting more than 48 hours is rising (see **Figure 14**). This increase may be driven by the rise in ransomware and other deliberate attacks, such as cable cuts.

Major outages attributed to cyberattacks in 2025 have occurred at double the average rate between 2020 and 2024 (see **Figure 5**), showing a clear increase. These incidents tend to last significantly longer than other failures due to the need for careful recovery and system rebuilds using clean, uncompromised data (see *Publicly reported outages see increase in deliberate attacks*).

Figure 14

### Durations of publicly reported outages, 2020 to 2024




PUBLICLY REPORTED OUTAGES

## Recent serious/severe outages

Most years, there are 15 to 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 2024 and early 2025 are shown in **Table 4**. The list is largely made up of telecommunications, cloud and/or digital services companies, where outages can affect a wide variety of customer.

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

## Table 4

## Ten major outages in 2024 and 2025

| Company | Industry | Severity rating | Year (quarter) | Cause | Impact |
|---|---|---|---|---|---|
| **United Healthcare/ Change Healthcare** (US) | Healthcare | 5 | 2024 (Q1) | Cyberattack/ ransomware | Cybercriminals exfiltrated roughly 6 terabytes of data and deployed ransomware after nine days of undetected access to networks. Considered the largest healthcare data breach in US history, the attack disrupted hospitals, physicians and pharmacies for nearly two months and cost the company over $1.5 billion, including a $22 million ransom paid in bitcoin. |
| **AT&T** (US) | Telecommunications | 5 | 2024 (Q1) | Network configuration error | A configuration error and failure to follow standard procedures caused user devices to disconnect from AT&T's network for over 12 hours. Around 92 million calls were blocked, including roughly 25,000 calls to emergency services. Financial impacts are estimated to exceed $100 million and AT&T may also face regulatory penalties. |
| **CDK Global** (North America) | Digital services | 5 | 2024 (Q2) | Cyberattack/ ransomware | Two separate ransomware attacks forced systems offline for two weeks, disrupting digital services for roughly 15,000 automotive dealerships. Estimated financial losses exceeded $3 billion, and a $25 million ransom was paid. |
| **Salesforce** (global) | Digital services | 5 | 2024 (Q3) | Configuration error/ software | A flawed database maintenance change removed critical application components, triggering outages across data centers in North America and Asia-Pacific. Core services for businesses and government agencies were disrupted, with financial losses from operational downtime likely reaching hundreds of millions of dollars. |
| **CrowdStrike** (global) | Digital services | 5 | 2024 (Q2) | Configuration error/ software | A faulty update to security software caused Windows systems to crash globally, leading to widespread disruptions across airlines, banks, hospitals and other critical sectors. The total estimated economic impact is more than $5 billion. |
| **Microsoft Azure** (US) | Cloud/internet giant | 5 | 2024 (Q2) | Configuration error/ software | A software configuration change accidentally blocked backend access between some of Azure's storage clusters and compute resources in the Central US region, disrupting services for more than five hours. This coincided with the unrelated CrowdStrike outage, causing confusion over which outage was affecting certain services. |
| **Digital Realty** (Singapore) | Digital services | 5 | 2024 (Q2) | Fire | A lithium-ion battery explosion caused a fire at a Digital Realty data center. The high temperatures and water damage from containing the fire disrupted services to major companies, such as Alibaba Cloud, ByteDance and Lazada, with the disruption lasting longer than one week. |
| **Ascension** (US) | Healthcare | 5 | 2024 (Q3) | Cyberattack/ ransomware | A ransomware attack forced the shutdown of critical systems, diverting ambulances, disrupting patient care, blocking access to medical information and potentially exposing data from an estimated 5.6 million people. The disruption lasted several weeks and contributed to a $1.8 billion operating loss for the fiscal year. |
| **Microsoft 365** (global) | Cloud/internet giant | 4 | 2024 (Q4) | Configuration error/ software | A backend infrastructure change mistakenly routed an influx of retry requests through servers, overloading them and making them unresponsive to users. Microsoft 365 services were unavailable for many businesses, and full service recovery took more than 24 hours. |
| **Barclays** (UK) | Financial services | 4 | 2025 (Q1) | Configuration error/ software | A software issue in Barclays' UK mainframe operating system caused a three-day outage, disrupting online banking, card transactions and ATM withdrawals. The outage coincided with the final deadline for tax returns and a major payday. Barclays has allocated up to £7.5 million for customer compensation. |

UPTIME INSTITUTE 2025

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

# Cost of outages

Outages are becoming more expensive. For the second consecutive year, just over half (54%) of respondents to Uptime's 2024 annual survey say their most recent significant outage exceeded $100,000 in total costs (see **Figure 15**). There has also been a slight uptick in outages costing over $1 million, rising by four percentage points since 2023.

A range of persistent and interrelated factors — including inflation, rising labor and hardware replacement costs, service level agreement (SLA) penalties and longer recovery times — are driving these high figures. The growing impact of malicious cyberattacks is also playing a role, particularly when extended downtime or ransomware payments push costs into the tens of millions.

At the same time, the increasingly critical nature of digital services is likely to drive these costs even higher, with some incidents triggering cascading effects across many customers and their services. The most prominent example of this is the CrowdStrike outage in 2024, estimated to have caused $10 billion in global financial impact — and widely described as the most significant IT service outage to date.

Rising expectations from customers, businesses and regulators are reflected in stricter SLAs and, in some cases, regulatory fines. These financial pressures reinforce the business case for continued service availability and investment in resiliency.

**Figure 15**

**Half of impactful outages cost more than $100,000**

Estimate the total cost of this downtime incident (from outage to full recovery), including direct, opportunity and reputation costs. (n=91)




*(Responses shown are only from those who reported experiencing either a significant, serious or severe outage in the past three years.)*
*(All figures rounded)*

UPTIME INSTITUTE GLOBAL DATA CENTER SURVEY 2024

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

# Summary

High availability and resiliency — defined as both preventing outages and recovering from them effectively — remain top priorities for digital infrastructure managers and operators. However, progress is not guaranteed. Uptime's research shows that resiliency gains are gradual, often challenging and costly — and that new threats are emerging, including cyberattacks, extreme weather events, electricity grid instability and system complexity.

Overall, the investments in resiliency, technological improvements and the diligence of operators tell a success story. These efforts have reduced the overall severity and frequency of outages relative to the overall growth in IT.

However, several trends emerging in 2025 may offset these gains. The industry-wide shift toward distributed architectures improves site-level resiliency but also introduces new points of failure — particularly in software, system configuration and network connectivity.

The rising complexity of these environments — driven by AI, automation, integration between IT and OT systems, and remote management — is increasing exposure to operational errors and cybersecurity threats.

Human error also remains a persistent risk, with a growing share of outages linked to failures to follow established procedures. As a result, allocating further resources to recruitment and training processes may significantly reduce downtime.

Additional external risks are becoming more prominent. Grid instability — driven by growing electrification and the variability of renewable energy sources — and the frequency of extreme weather events linked to climate change are increasingly relevant to long-term resiliency strategies, despite remaining largely beyond direct operator control.

While the industry is making progress, resiliency is neither automatic nor assured. Preventing outages in an increasingly complex, interconnected and high-stakes environment demands continuous investment, operational discipline and adaptive risk management.

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

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 Survey of IT and Data Center Managers

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.

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

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 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 2024*
*Annual outage analysis 2024*
*Publicly reported outages see increase in deliberate attacks*

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED

# 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. 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 Seattle, London, Sao Paulo, Dubai, Singapore, and Taipei.

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

© COPYRIGHT 2025 UPTIME INSTITUTE. ALL RIGHTS RESERVED