uptime INTELLIGENCE

Annual outages analysis 2023

The causes and impacts of IT and data center outages

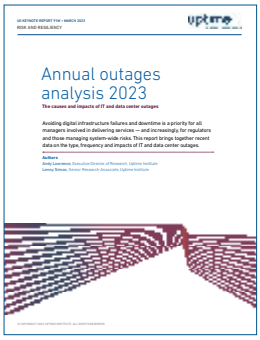
Avoiding digital infrastructure failures and downtime is a priority for all managers involved in delivering services — and increasingly, for regulators and those managing system-wide risks. This report brings together recent data on the type, frequency and impacts of IT and data center outages.

Authors
Andy Lawrence, Executive Director of Research, Uptime Institute
Lenny Simon, Senior Research Associate, Uptime Institute

Synopsis

The avoidance of outages is a priority for operators of mission-critical digital infrastructure. In recent years, this has also been a bigger issue for regulators and market authorities. This report brings together and analyzes recent Uptime Institute data on outage trends, causes, costs and consequences.

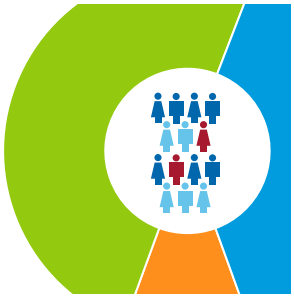
- Data relating to outages should be treated skeptically. All methodologies to track the frequency, severity and costs of outages are subject to uncertainty, partly because of a lack of transparency and reliable reporting mechanisms.
- There is evidence that outage rates have been gradually falling in recent years. Although most sites have experienced an outage in the past three years, only a small proportion are serious or severe.
- When outages do occur, they are becoming more expensive, a trend that is likely to continue as dependency on digital services increases. With more than two-thirds of all outages costing more than $100,000, the business case for investing more in resiliency — and training — is becoming stronger.
- Professional third-party digital infrastructure companies — cloud, colocation, telecommunications and hosting companies — account for a growing proportion of outages. This reflects the growing role and importance of these companies.
- Human error and management failures contribute to a considerable number of outages. More training and investment in management processes is required.



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

Introduction and terminology

This report on outage trends is one of an ongoing series from Uptime Institute Intelligence analyzing IT service resiliency. The analysis is based on data from a variety of sources, including publicly available information (e.g., information reported in news and social media), Uptime Institute Intelligence surveys (e.g., the Uptime Institute Global Survey of IT and Data Center Managers 2022 and the Uptime Institute Data Center Resiliency Survey 2023) and other data anonymized and aggregated from Uptime members and partners. Despite the limitations of these data sources, taken together, they provide insight into the trends, causes and impacts of outages over the course of the past year (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

In this report we use three primary sources:

- The Uptime Institute Annual Global Data Center Survey 2022. This was conducted in April and May 2022, with about 830 operator respondents. This may be referred to as Uptime's annual survey.
- The Uptime Institute Data Center Resiliency Survey 2023, conducted in January and February 2023, with 739 respondents. This is an annual survey.
- Public reported / tracked outages tracked by Uptime in 2022. 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.

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 INTELLIGENCE 2023

Many decades of innovation, investment and better management mean than, overall, critical IT systems, networks and data centers are far more reliable than they were. Major failures seem more common for several reasons: the high levels of critical IT in use; society's high dependency on IT; and increased visibility through news and social media.

For most data center and IT managers, small IT-level service outages are frequent irritants and a sign that attention and investment is needed. Significant, serious and severe outages (categories 3, 4 and 5) are the focus of this report. These outages can have serious consequences and require a full root-cause analysis, investment and corrective action to reduce the likelihood of a repeat occurrence.

The increasing use of cloud services has changed the characteristics of outages in recent years. Failures are more likely to be caused by software, systems or configuration errors — a reflection of the growing complexity of the IT and associated networking. These outages are also more likely to affect many IT services and organizations, reflecting system interdependency and the concentration of customers using single providers, often in a single availability zone. Cloud and internet service outages are more likely to be partial, sporadic or intermittent, again reflecting the distributed nature and overall complexity of digital services.

Outage frequency and severity

How common are outages? Is the number of outages increasing? The answers depend on who is asked and how they define outages. Even so, the survey evidence from Uptime Institute, with its large global panel of senior data center and IT managers, is relatively consistent.

Uptime's data suggests that the number of outages globally, increases year-on-year as the industry expands. This increase, along with the obvious public impact of some outages, inevitably attracts attention and headlines. This can give the false impression that the rate of outages relative to IT load is growing, whereas the opposite is the case. The frequency of outages is not growing as fast as the expansion of IT, or the global data center footprint.

In four separate surveys from 2020 to 2022, the proportion of managers and data center operators who experienced an outage at their organization in the past three years (category severity 3 to 5) fluctuated from 60% to 80%. (Note that Uptime uses "past three years" to ensure a more even trend line and a sufficient sample for understanding the causes.)

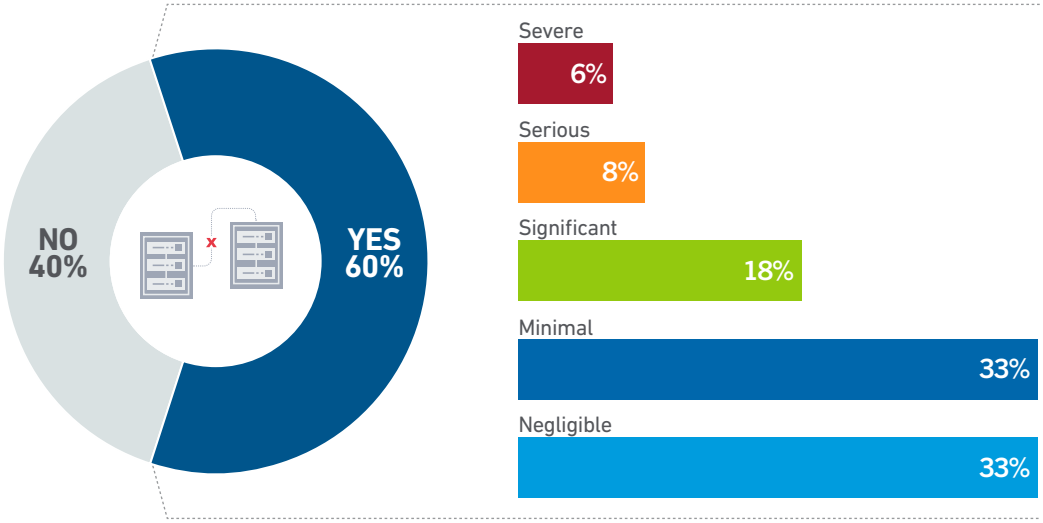
Overall, Uptime has tracked a steady decline in the outage rate per site (or per survey respondent). In 2022, 60% of operators that responded to the Uptime annual survey say they had an outage in the past three years (see **Figure 1**) — down from 69% in 2021 and 78% in 2020.

Uptime is reluctant to herald this as a breakthrough improvement for two reasons. First, the impact of the COVID-19 pandemic on business levels and IT and data center operations has made recent year-on-year comparisons difficult; second, there are some contradictory findings (not discussed in detail here) that require further research.

Figure 1

Most organizations experienced an outage in the past three years

On a scale of 1 (negligible) to 5 (severe), how would you classify the most impactful outage your organization has had in the past three years, either in your own facility or because of a third-party service provider? (n=730)



(All figures rounded)

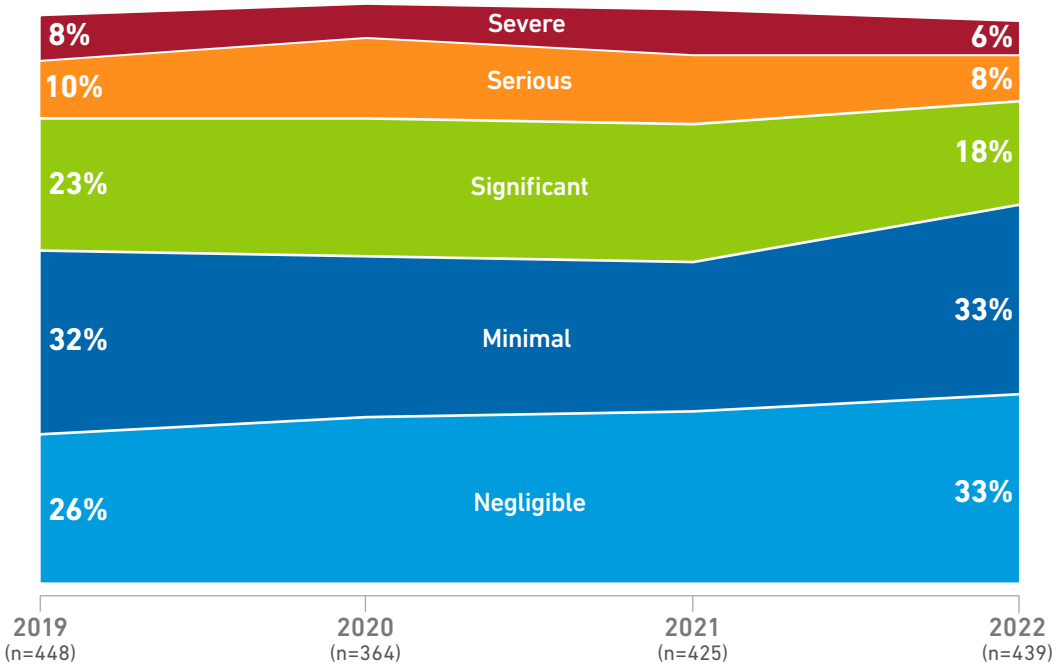
UPTIME INSTITUTE GLOBAL SURVEY OF IT AND DATA CENTER MANAGERS 2022

There are also signs that the impact of at least some outages is decreasing. Uptime classifies outages on a scale of 1 to 5, and those in the two most serious / severe categories (category 4 / category 5) historically account for about one in five of all outages (among survey respondents who had an outage in the past three years). In 2022, outages in the serious / severe categories fell to 14%, or one in six, among those organizations that had an outage in the past three years (**Figure 2**).

Figure 2

Proportion of outages classified as significant, serious or severe

On a scale of 1 (negligible) to 5 (severe), how would you classify the most impactful outage your organization has had in the past three years, either in your own facility or because of a third-party service provider?



(All figures rounded)

UPTIME INSTITUTE GLOBAL SURVEY OF IT AND DATA CENTER MANAGERS 2019-2022

What can be learned from this data on outage frequency and severity?

- Outage frequency is relatively consistent and, arguably, relatively high, despite the improvements to technology, software and physical redundancy technology. The frequency of outages and the associated financial and / or reputational costs justify the high concern from executives and authorities / regulators.
- Despite the headlines, there is no evidence that the number of outages is increasing relative to the overall rise in IT — and it may be falling slowly. (Uptime Institute is researching this further.)
- Data on outages is confused by two factors:

  1. The impact of the COVID-19 pandemic persists. While some operators reduced maintenance and operated at a high capacity, others operated at well below capacity and could conduct unscheduled extra maintenance.

  2. The reliance on premium and highly redundant data centers, often with one passive backup site, is shifting towards more complex, distributed architectures. Although the latter may ultimately prove more resilient, the industry is still learning how to handle failures in such large and complex networks.

- The frequency of outages (and their duration) strongly suggests that the actual performance of many providers falls short of service level agreements (SLAs). Customers should never consider SLAs (or 99.9x% availability figures) as reliable predictors of future availability.

Major public outages — the headline makers

In addition to our 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 including those that are different and more qualitative than survey data.

Table 3 shows the number of outage reports we collected from public sources over the past seven years. The numbers do not necessarily represent the underlying number of outages. In recent years, media and social media have reported increasing numbers of outages, even though many are trivial and some are inaccurate (or not attributed to the underlying operator). 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 2022, we collected the details of 111 outages.

Table 3

Publicly reported outages tracked by Uptime, 2016 to 2022

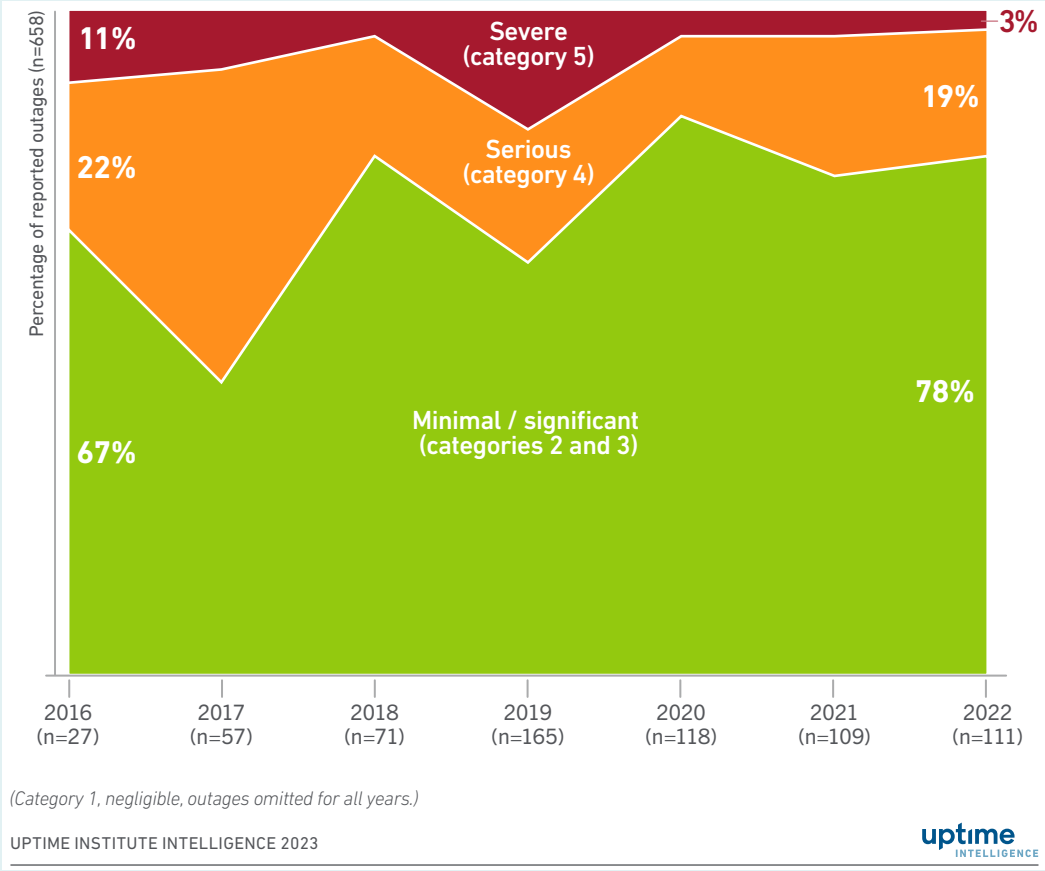
Publicly reported outages							
2016	2017	2018	2019	2020	2021	2022	Total
27	57	71	165	118	109	111	**656**

UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2023

Outages with the most severe impact inevitably attract media attention. **Figure 3** shows that the proportion (and indeed, the absolute number) of serious and severe outages has fallen over seven years of tracking. It is not clear if this is caused by changes in technology, data center practices or other factors — although the COVID-19 pandemic probably dampened the impact of outages in 2020.

Figure 3

Proportion of publicly reported outages that were serious or severe, 2016 to 2022



This data suggests that each year there will probably be 10 to 20 serious, high-profile IT outages across the world that cause major financial loss, business and customer disruption, reputational loss and, in extreme cases, loss of life.

Outage causes

Understanding the causes of outages is critical to preventing them and to guide resiliency investments. Most outages have several causes and, as we have noted in surveys, knowledge and understanding of outages may depend on an individual's perspective.

Uptime's annual global survey provides a robust, consistent data set from a group of respondents who often have detailed knowledge of data center operations — but not all respondents from this group have detailed knowledge of all their organization's IT outages and their causes. Some of Uptime's other surveys, which may include a wider group of respondents, may show different causes and outage rates. All data should be treated cautiously.

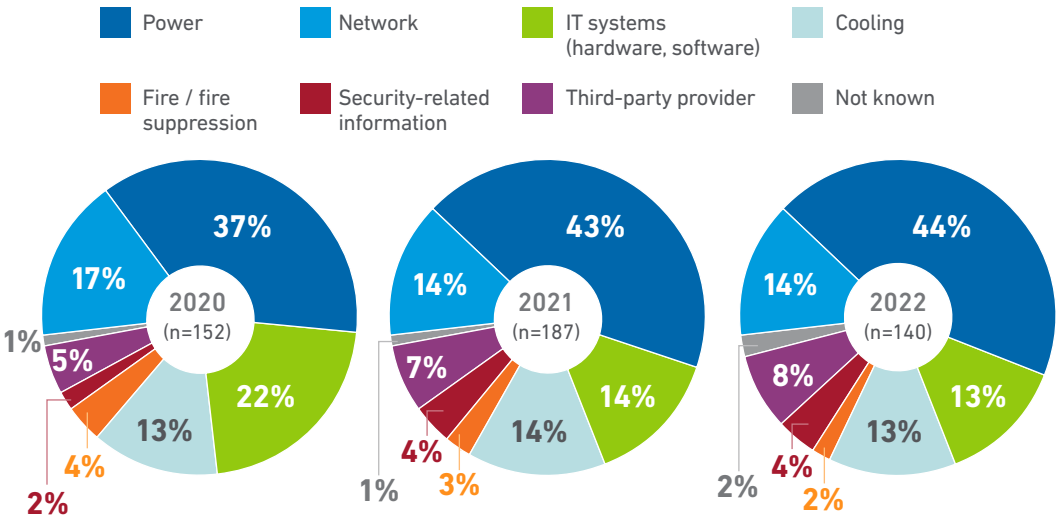
Uptime's 2022 annual survey findings are remarkably consistent with previous years. They show that on-site power problems remain the biggest cause of significant site outages by a large margin (see **Figure 4**). As in previous years, all other outage causes are far less common. However, three other common causes stand out as particularly troubling: cooling failures, software / IT system errors and network issues. The frequency of problems at

third-party providers — for example, software as a service (SaaS), hosting and cloud providers — is creeping up, reflecting a greater use of cloud, SaaS and colocation. Further underlying causes are discussed below.

Figure 4

Leading causes of significant outages

What was the primary cause of your organization's most recent impactful incident or outage?



(All figures rounded)

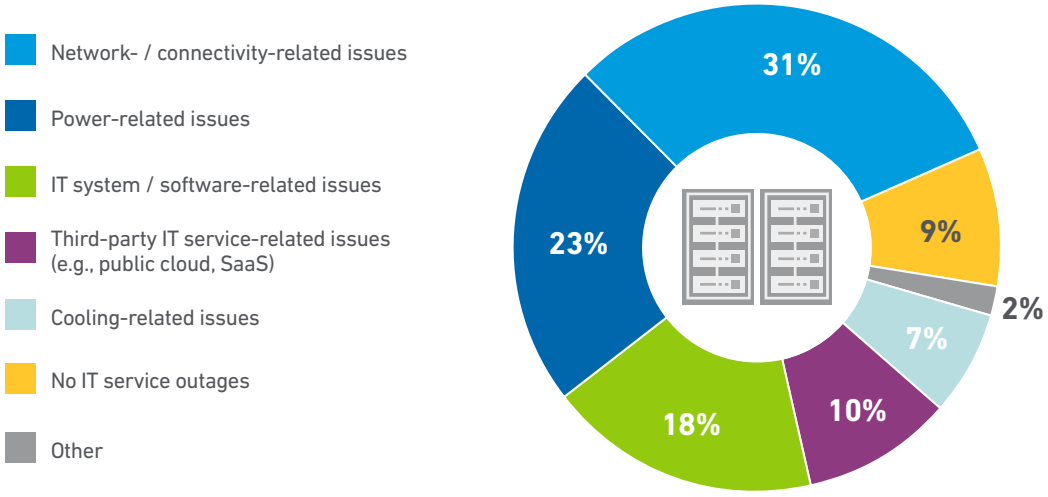
UPTIME INSTITUTE GLOBAL SURVEY OF IT AND DATA CENTER MANAGERS 2020-2022

For a more general view of outage causes, Uptime Intelligence's annual resiliency survey 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 show that network-related outages are more common, and some way ahead of power (**Figure 5**).

Figure 5

Most organizations had some IT service outage in the past three years

Which of the following issues has been the most common cause of an IT outage that may have affected your organization over the past three years? (n=406)



UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2023

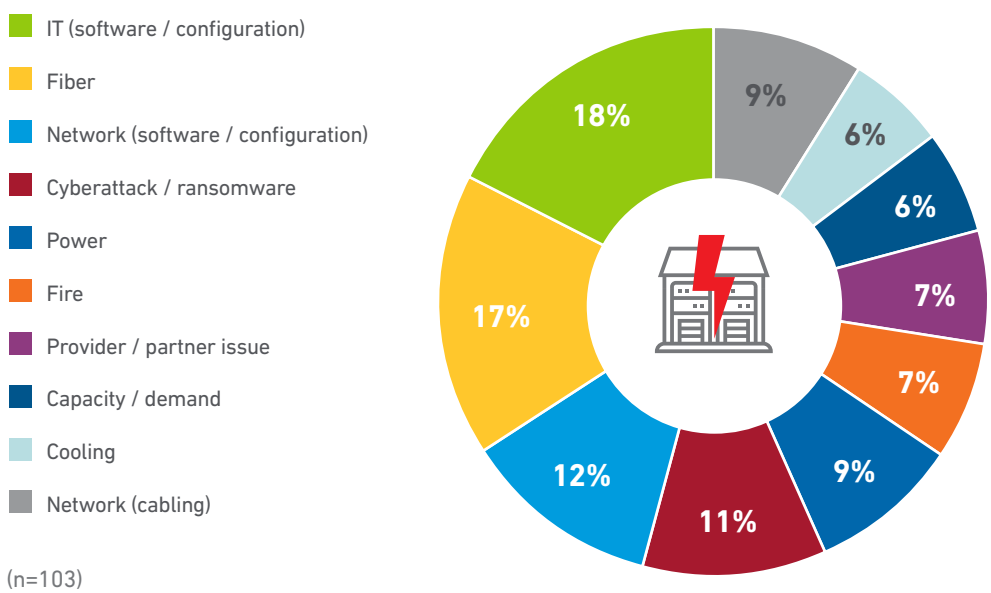
Ransomware confirmed as a major public outage cause

Publicly recorded or reported outages — those that receive media attention — show a diversity of causes, but there is usually some consistency from year to year. In the past two years, cyberattacks and ransomware have become a regular and growing cause of outages and accounted for 11% of publicly reported / recorded outages in 2022, rising from 8% in 2021 (**Figure 6**). High profile victims included a data center operator and an international newspaper.

Ransomware attacks often lead to a lengthy shutdown of large parts of an organization's digital infrastructure. Because of contamination and loss of integrity, organizations often need to rebuild systems and data bases; data loss is common. The incorporation of industry-standard operating systems into mechanical and electrical equipment, and the greater use of remote monitoring, is increasing the risk of security breaches in data centers considerably.

Figure 6

Causes of publicly reported outages, 2022



(n=103)

(Category 1, negligible, outages omitted.)

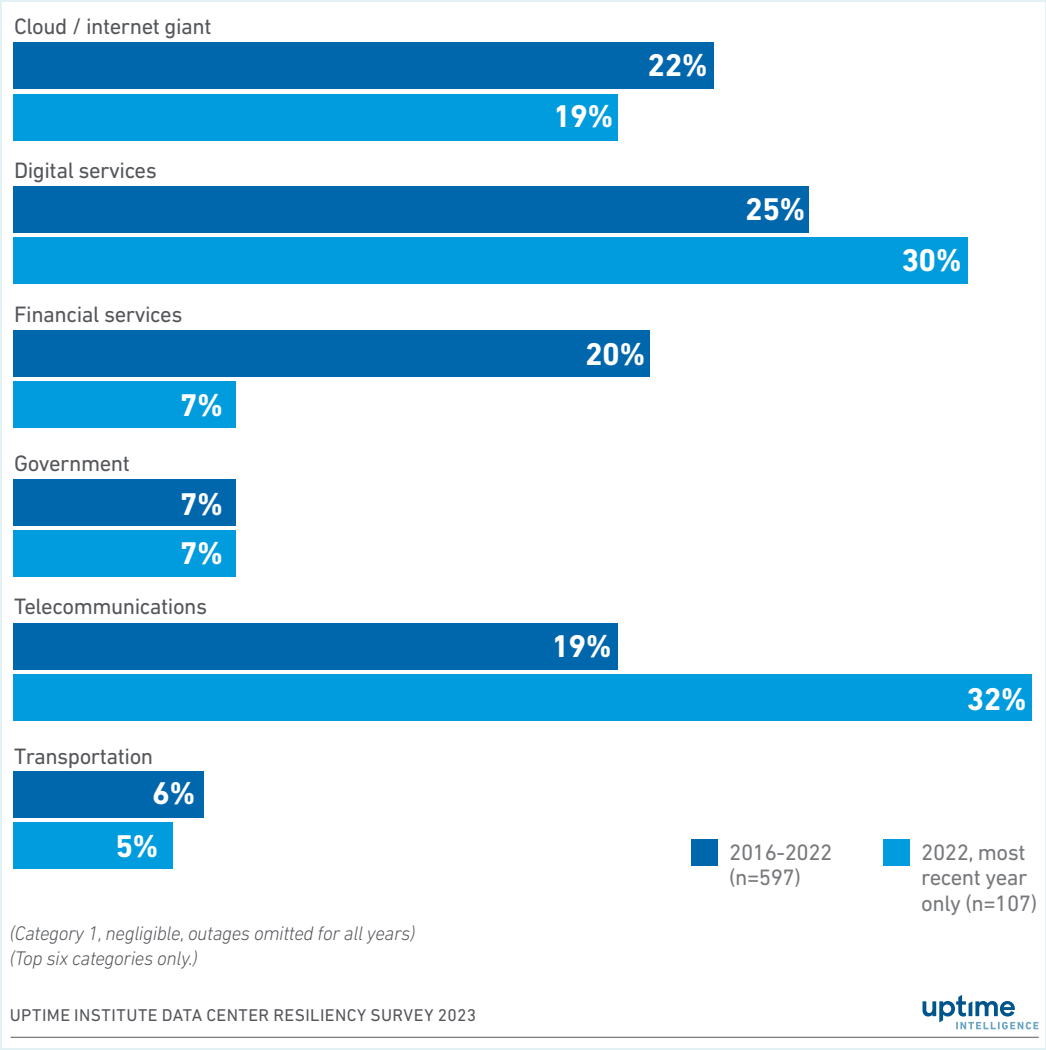
UPTIME INSTITUTE INTELLIGENCE 2023

Public outages: commercial operators in the limelight

The more that workloads are outsourced to external third-party providers, the more these operators account for high profile, public outages. Over seven years, third-party, commercial operators of IT and / or data centers (cloud / internet giant, digital services, telecommunications, etc.) accounted for two-thirds (66%) of public outages tracked since 2016 (see **Figure 7**). This percentage has crept up year by year — in 2021 the combined proportion of outages caused by these commercial operators was 70%, and in 2022 it was 81%. Of these, outages of telecommunications services show the largest increase, while reported cloud service outages fell. This is partly caused by the high dependency of almost all services on telecommunications — but it is also because telecommunications services have moved from expensive, proprietary systems to more commodity-based components and architectures.

Figure 7

Publicly reported outages by sector, 2016 to 2022



Cloud and third-party provider reliability

Cloud services are designed to operate with low failure rates. Large (at-scale) cloud and IT service providers (such as Amazon Web Services, Microsoft Azure and Google Cloud) incorporate layers of software and middleware; balance capacity across systems, networks and data centers; and reroute workloads and traffic away from failures and troubled sites. Overall, these architectures provide high levels of service availability at scale. Despite this, no architecture is fail-safe, and many recorded failures can now be attributed to the difficulties of managing such complex, at-scale software, data and networks.

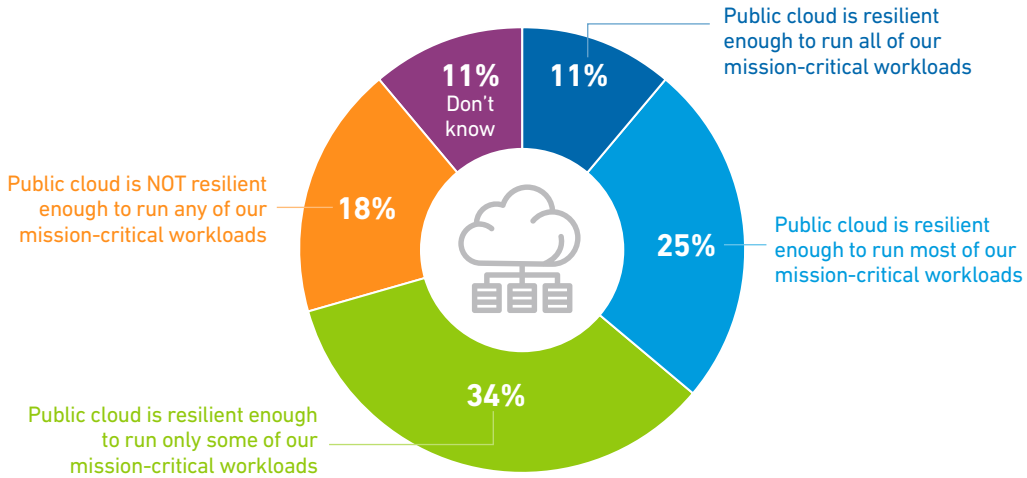
Cloud, hosted and many other internet-based services and workloads play an increasing role in critical corporate IT. The reliability (and transparency) of public cloud services has come under scrutiny in recent years due to some high-profile outages and the growing interest in running critical services in a public cloud. Concentration risk — over dependency on a few major services or underlying components or data centers — is also a concern.

Figure 8 shows that many enterprise managers are concerned about the resiliency of public cloud services. Only about one in 10 respondents say public cloud services are resilient enough to run all their workloads. And a growing proportion — now nearly a fifth (18%) say the cloud is not resilient enough to run any of their workloads. About a third (34%) say the cloud is only resilient enough to run some workloads. Overall, these are not the results (or the trends) that cloud providers want to see, but these numbers are unlikely to change dramatically until they can offer greater reassurances on transparency — and perhaps new SLAs that give mission-critical customers more control and compensation.

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, run most of them, run only some of them, or is public cloud not resilient enough to run any of your organization's mission-critical workloads?



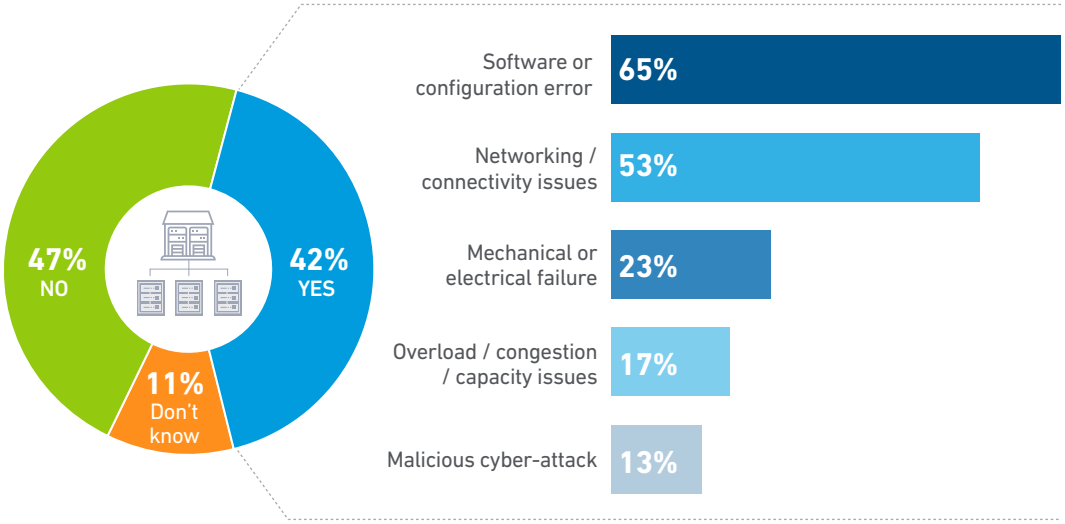
UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2023

Of course, concern over cloud resiliency may be partly caused by the number of cloud service outages that make the headlines. In our 2023 resiliency survey, 42% of respondents said their organization suffered an outage in the past three years that was caused by a problem with a third-party supplier — a marginal increase over 2022 (39%). The breakdown of causes of these third-party outages, as perceived by the customers affected, is shown in **Figure 9**.

Figure 9

Most common causes of major third-party outages

Has your organization experienced a major outage(s) caused by a problem with a third-party IT provider over the past three years (n=186)? If so, what are their most common causes? Choose no more than three (n=78)



UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2023

Power outages

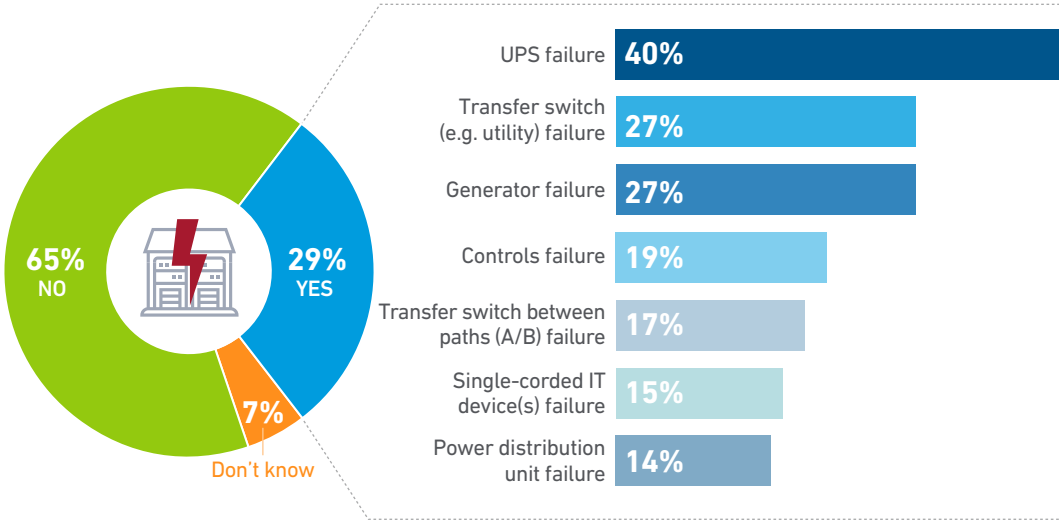
Power-related outages have long been the scourge of data center management. A power event is usually sudden, binary (on / off), can be site-wide and can have an immediate impact on service delivery. Although diagnosis and restoration of power can be quick, it can take many hours to restart IT systems and fully synchronize databases. The loss of equipment can mean data centers operate outside SLAs until full replacements are installed.

In the 2023 resiliency survey, less than a third of operators said they experienced a major outage at their site caused by a power problem in the past three years (see **Figure 10**). In 2023, there were only small changes from 2022. The single biggest cause of a power outage, by some distance, is a UPS failure (a grid failure is considered to be a backup or lower-cost power source, not a primary power source). Generator and transfer switch failures were experienced by just over a quarter of operators.

Figure 10

Most common causes of major power-related outages

Has your organization experienced a major outage(s) caused by a problem with a power system over the past three years (n=393)? If so, what are their most common causes? Choose no more than three (n=113)?



UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2023

Uptime engineers report that static UPSs fail for several reasons:

- Fans fail frequently because they are usually inexpensive and constantly in operation. A single fan failure does not take a unit down, 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.

UPS problems are more likely with age, so supply chain / replacement problems may lead to more failures. Operators of data centers without trusted concurrent maintainability designs (the ability to bypass any item of equipment for maintenance without interrupting overall service) can be more likely to postpone maintenance or replacement.

Generators are reliable, but require regular scheduled maintenance, fuel checks and testing. Automatic transfer switch (ATS) units are generally robust, but failures may occur with active controls or with a loss of direct current (DC) power to those controls. Other less common failures are caused by mechanical issues, such as bearings wearing out or a jammed switch.

Networking outages

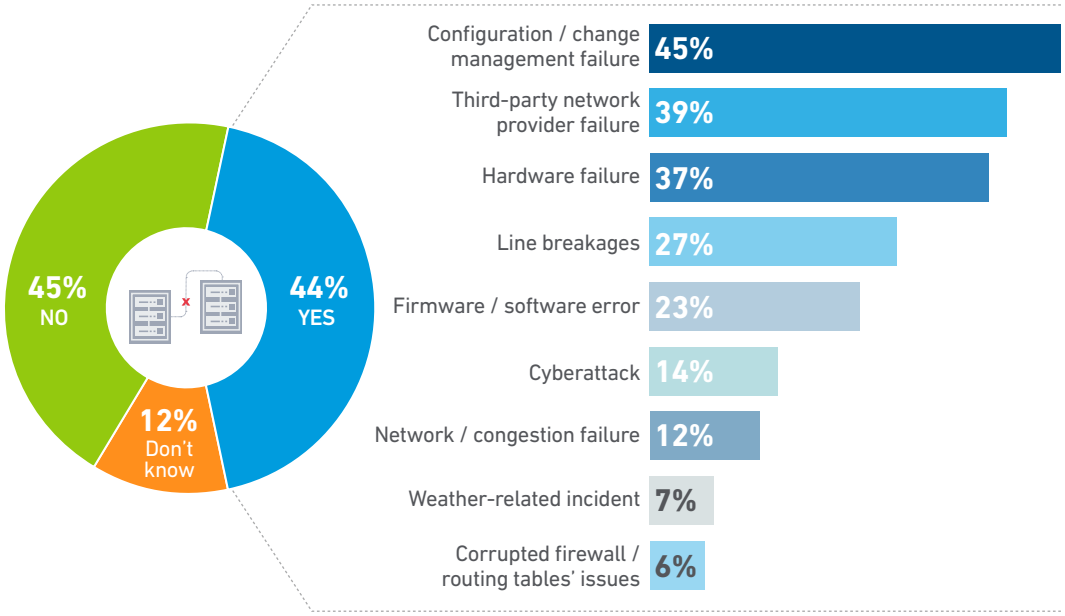
In recent years, networking issues have caused an increasing portion of IT outages. The 2023 Uptime resiliency survey finds the two most common causes of networking- / connectivity-related outages are configuration / change management failure (45% of respondents) and third-party network provider failure (39%) — very similar numbers to previous years (see **Figure 11**).

Neither of these two underlying causes are surprising. In earlier times, networking was far less dynamic and flexible, with routers, switches and cabling equipment largely left alone during normal operation. But in modern, dynamically switched and software-defined environments, programs to manage and optimize networks are constantly revised or reconfigured. Errors become inevitable, and in such a complex and high throughput environment, frequent small errors can propagate across networks, resulting in cascading failures that can be difficult to stop, diagnose and fix. The high number of network / software failures has clearly contributed to a rise of telecommunications failures in publicly reported outages.

Figure 11

Most common causes of major network-related outages

Has your organization experienced a major outage(s) caused by network / connectivity issues over the past three years (n=406)? If so, what are their most common causes? Choose no more than three (n=174)



UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2023

Networks are complex, not only from a technical point of view, but also operationally. While enterprise data centers may be served by only one or two telecommunications providers, multicarrier colocation hubs are usually served by many. Some of these links may, further down the line, share cables or facilities — adding possible overlapping points of failure or capacity pinch points. Ownership, visibility and accountability can also

be complicated. This contributes to 39% of survey respondents having experienced an outage in the past three years caused by a third-party networking issue — something over which they had little control.

The majority of those who avoided network-related downtime attribute it to more controllable factors: redundancy and resiliency in the network.

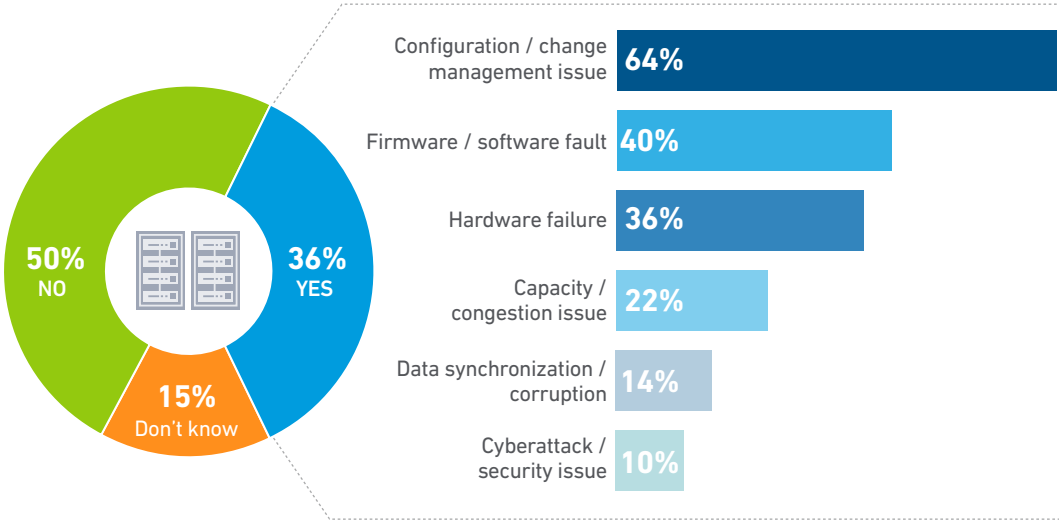
System and software outages

More than a third of operators experienced a major outage at their site caused by a system or software problem in the past three years (see **Figure 12**). As with the high number of network-related issues, system and software outages are partly caused by the complexity and scale of modern systems, and the growing role that software plays in ensuring availability across distributed data center sites. Problems with database synchronization, load balancing and traffic management can cause partial or complete downtime of services that are running in more than one data center or availability zone.

Figure 12

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

Has your organization experienced a major outage(s) caused by an IT systems or software failure over the past three years (n=385)? If so, what are their most common causes? Choose no more than three (n=136)



UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2023

Software problems are mostly caused by configuration changes, upgrades, patches and other changes, which cause instability and unforeseen errors. If these are propagated across networks, the problem can be difficult to contain. But hardware and software faults and failures that cause outages are less common, although these numbers appear to be rising. About one in 10 organizations said they had suffered an outage caused by cyberattacks, such as ransomware and distributed denial of service (DDoS) attacks, lower than in previous years. When these events do occur, however, they can be extremely serious and expensive.

For all outage causes, resiliency and redundancy are always cited as the main methods to avoid them — this is not surprising and justifies decades of high investment and mission critical design. But effective processes, staff competency and effective management are also commonly cited means to avoid outages.

The human factor

Uptime tends to research human error in a different way than other causes: we view it as one causal factor in outages — rarely a single or root cause. When viewed this way, Uptime estimates (based on 25 years of data) that human error plays a role in two-thirds to four-fifths of all outages.

Analyzing human error — with a view to preventing it — has always been challenging for data center operators. The cause of a failure can lie in how well a process was taught, how tired, well trained or resourced the staff are, or whether the equipment itself was unnecessarily difficult to operate. Factors such as tiredness may ultimately be caused by insufficient staff levels or long shifts.

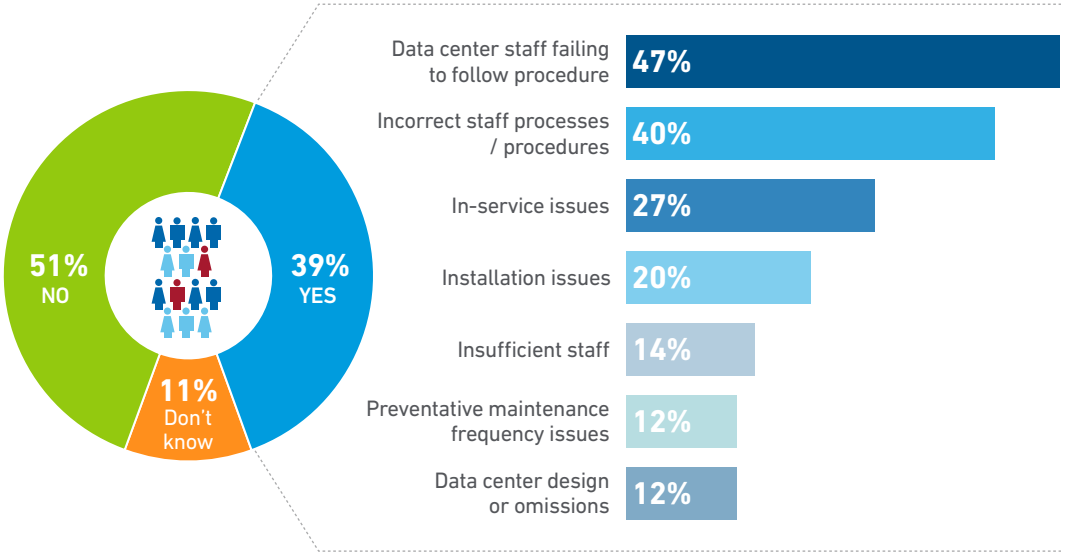
There are also definitional questions: if a machine fails due to a software error at the factory, is that human error? Human error can also often play a role in outages that are attributed to other causes.

In our recent surveys on resiliency, we have tried to understand the makeup of some of these failures related to human error. **Figure 13** shows that human error-related outages are mostly caused either by staff failing to follow procedures (even where they are agreed upon and codified) or by the procedures themselves being faulty.

Figure 13

Most common causes of major human error-related outages

Has your organization experienced a major outage(s) caused by human error over the past three years (n=378)? If so, what are their most common causes? Choose no more than three (n=146)



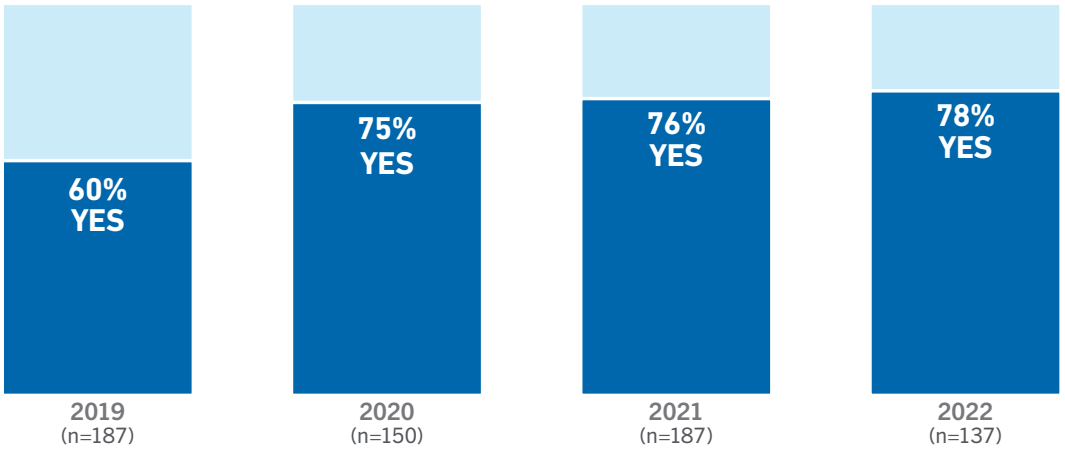
UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2023

Separately, in global annual surveys from 2019 to 2022, the great majority of managers and operators said that their most recent and impactful outage could have been prevented with better management and processes (**Figure 14**).

Figure 14

Most operators still view downtime as preventable

Would your organization's most recent impactful downtime incident have been preventable with better management / processes or configuration?



UPTIME INSTITUTE GLOBAL SURVEY OF IT AND DATA CENTER MANAGERS 2022

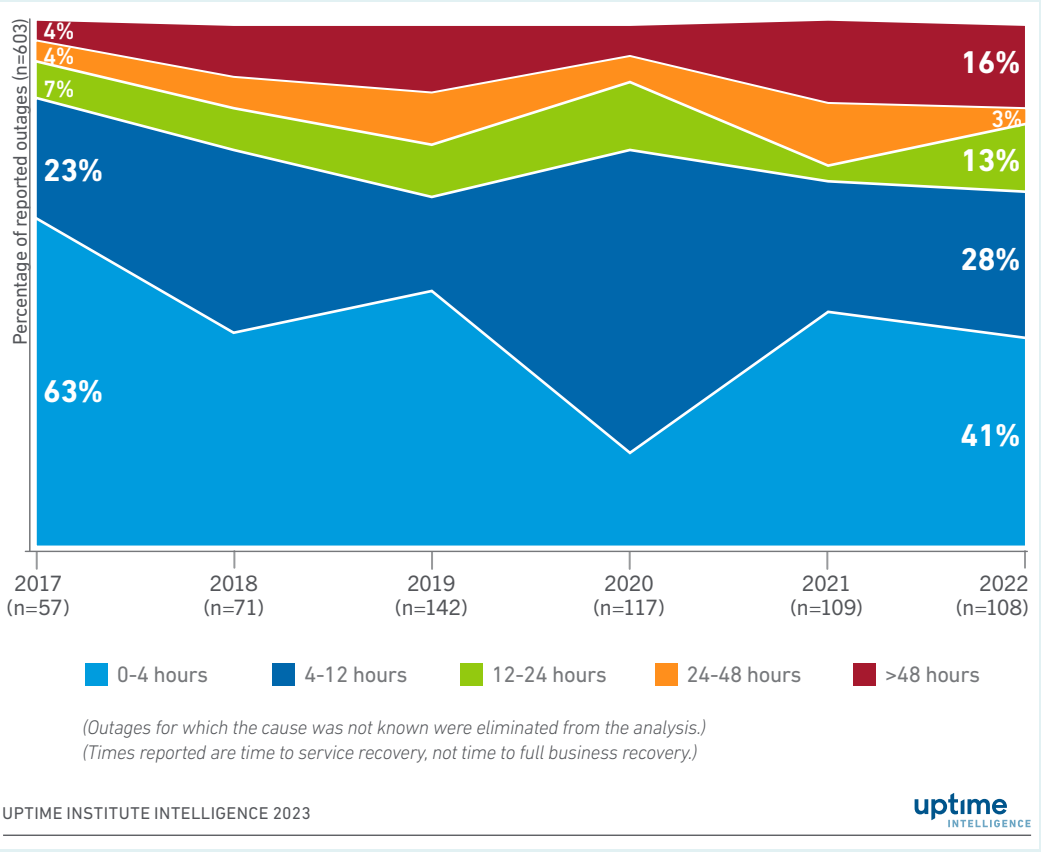
All these findings underscore a key tenet of Uptime's advice to owners and operators: good training and well thought-out and rehearsed processes play key roles in outage reduction and can be implemented without great expense.

Public outages: is duration increasing?

The longer an outage, the more likely it is to be expensive, disruptive and damaging. It is also more likely to receive media attention. Data from publicly reported outages shows that, even from this group of high-profile outages, the majority (70%) are resolved within 12 hours, and most are rectified far more quickly. Since 2019 (data before this year is less reliable), however, there is one disturbing trend: the number of outages that have not been fully recovered after 48 hours is rising (**Figure 15**).

There may be several reasons for this rise, for example fires (slightly up), and the complications of synchronizing distributed data and management systems. But clearly, major ransomware attacks, which usually require the shutdown of all potentially affected systems, are becoming more common.

Figure 15 Durations of publicly reported outages, 2017 to 2022



Recent serious / severe outages

Most years, there are 15 to 20 outages that Uptime classifies 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 2022 and early 2023 are shown in **Table 4**. The list is largely made up of telecommunications, cloud and / or digital services companies, where outages can affect many users. The government and healthcare sectors also stand out as being highly vulnerable to serious or severe outages.

Table 4 Ten major outages in 2022 and 2023

Company name	Industry	Severity rating	Year (quarter)	Cause	Impact
Federal Aviation Administration (US)	Government	5	2023 (Q1)	Software configuration / database error	All US flights were grounded. Thousands of flights were cancelled or delayed.
Kakao (South Korea)	Digital services	5	2022 (Q4)	Battery fire in data center	Most of South Korea suffered an 8-hour service disruption. CEOs resigned. Government investigations and multiple class-action lawsuits were initiated.
KDDI (Japan)	Telecommunications	5	2022 (Q3)	Networking system / configuration error	More than 39 million users experienced service disruptions for 86 hours. Critical services were affected across multiple industries.
Google (global)	Cloud / internet giant	4	2022 (Q3)	Software update issue	Google search engine and applications that rely on it, such as Google Maps and Google Images, were offline or degraded for about 40 minutes worldwide.
CommonSpirit Health (US)	Healthcare	4	2022 (Q4)	Ransomware / cyberattack	The second largest non-profit hospital network in the US suffered IT service disruptions across multiple locations for more than a week, and a major data breach. Costs exceeded $150 million.
Amazon Web Services (US)	Cloud / internet giant	4	2022 (Q3)	Power loss / transfer switch failure	A major AWS availability zone went offline, affecting thousands of businesses. There were cascading errors for third-party services when the zone came back online.
National Health Service (UK)	Healthcare	4	2022 (Q3)	Heatwave / cooling failure	One of the largest NHS hospitals in London (UK) suffered major disruption to all services. The outage cost the NHS £1.4 million.
Microsoft (Europe / global)	Cloud / internet giant	4	2022 (Q3)	Power loss / switchover failure	Customers, mostly in Western Europe, suffered extended service delays and access failures for Microsoft 365 applications.

UPTIME INTELLIGENCE 2023

Cost of outages

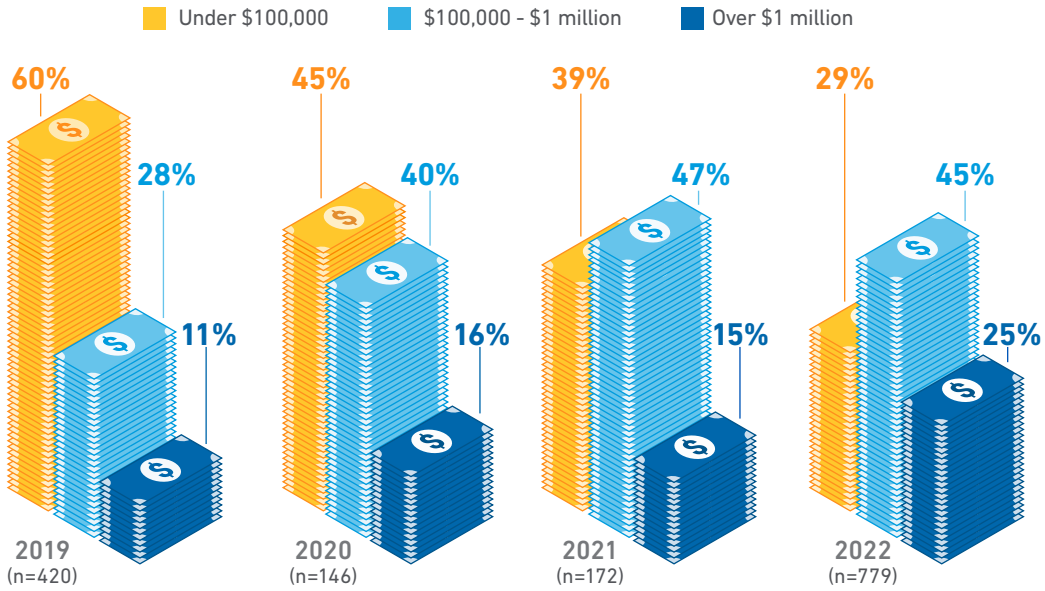
Trend data from Uptime research over several years regarding outage frequency or how organizations rate their severity, clearly shows that outages are costing more. In Uptime's 2022 global survey, a quarter of respondents said their most recent outage cost more than $1 million in direct and indirect costs, continuing a clear trend of increasing costs (see **Figure 16**). A further 45% said their most recent outage cost between $100,000 and $1 million.

With more than two-thirds of all outages costing more than $100,000, the business case for investing more in resiliency (and training) is becoming stronger.

Figure 16

The proportion of single major outages costing over $100,000 is increasing

Please estimate the total cost of your most recent downtime incident (from outage to full recovery) for your organization, including direct, opportunity and reputation costs, using the following options.



(All figures rounded)

UPTIME INSTITUTE GLOBAL SURVEY OF IT AND DATA CENTER MANAGERS 2019-2022

Why is the cost of outages increasing? This can be attributed to a variety of factors, ranging from inflation, fines, SLA breaches and the cost of labor, call outs and replacement parts, but the biggest single reason is the growing dependency of corporate economic activity on digital services and on the data center. The loss of a critical IT service often translates directly and immediately into disrupted business and lost revenue.

We do not calculate an average cost of outages, because the insights gained are rarely useful — businesses and outage impacts vary widely. Each year, a few large outlier outages are so costly that they can distort the overall picture. Some result in compensation, fines and lost business, with costs adding up to millions or even tens of millions of dollars. In 2022, Uptime Intelligence is aware of several outages that cost more than $150 million.

The trend toward higher costs resulting from outages is likely to continue as dependency on digital services increases. Stronger SLAs, expected by some businesses because of this growing reliance, could make outages even more costly, as will more and higher regulatory fines and compensation for customers who experience a service disruption. This, in turn, justifies further analysis of the causes and costs of outages and the continued or increased investment in resiliency.

Summary

High availability and resiliency (which means outage prevention and effective recovery) is a priority for all involved in the digital infrastructure supply chain. It is sometimes assumed that progress in this area is as reliable as Moore's law has been in the past three decades. This is not the case: Uptime's data shows that progress is gradual, hard won and — when failures occur — increasingly expensive.

Moreover, some trends could undermine progress being made in equipment reliability and improving processes and management.

First, a broad shift to distributed architectures, in which more IT functions run on standard IT systems, often distributed or replicated across many sites, reduces the impact of some localized failures. But this may also cause, at least during an extended transition, more network, software or systems issues.

Second, the transition to renewable energy and distributed energy generation and storage will, many believe, reduce the reliability of the grid. While grid failures are not considered a primary source of outages, they will put stress on data center power systems and management processes.

Third, the role of experienced and well-trained staff, who follow proven management processes, is critical to achieving resiliency. However, a skills shortage in many geographies makes it hard to find enough experienced staff.

Prevention of outages is an ongoing challenge that requires constant monitoring and attention, investment and analysis. Key considerations include: building for and increasing redundancy, testing, constant reviewing of changing threats and technologies, and perhaps above all, investing in staff and training.

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 in this report. This represents the most statistically significant dataset relating to outages in the critical digital infrastructure industry.

Uptime Institute Data Center Resiliency Survey

This global survey specifically focuses on outages and resiliency-related issues. 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 data. 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.
- We limit failures to those that had a noticeable impact on end users — a major fire during data center commissioning, for example, may never be registered. We have also eliminated all category 1 outages — 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 it was never disclosed.
- Finally, while we include IT system failures, we do not generally include cybersecurity breaches, except those that can lead to complete service interruptions.

About the authors

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

Lenny Simon

Lenny Simon is a Senior Research Associate at Uptime Institute covering global trends, sustainability and technologies in critical digital infrastructure. Before joining Uptime, he was an analyst at GreenMax Capital Advisors and worked in the Office of the Mayor of New York City.

lbrandes-simon@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**