

# Data Center Industry Overview and Insights

Day 3 – Resiliency, availability and  
performance

---

**Prepared for the Lloyd's Market Association (LMA)**

*Confidential: For internal use by LMA and Uptime Institute only*

# The Uptime Team



---

Doug Donnellan  
(Moderator)

---

Research Analyst,  
Uptime Institute



---

Chris Brown

---

Chief Technical Officer,  
Uptime Institute



---

Dr. Tomas Rahkonen

---

Research Director  
Sustainability (Europe),  
Uptime Institute

# Quick recap

## Day 1: Data centers in the modern economy

- The origins and evolution of data centers
- Scale, growth, and ownership
- Business models
- Delivery environment

## Day 2: Data center (and IT) technology

- IT building blocks
- Why AI is different
- Power and cooling
- Costs, forecasts and future pressure



# Quick recap

## Day 1: Data centers in the modern economy

- The origins and evolution of data centers
- Scale, growth, and ownership
- Business models
- Delivery environment

## Day 2: Data center (and IT) technology

- IT building blocks
- Why AI is different
- Power and cooling
- Costs, forecasts and future pressure

- How are these systems designed, operated and managed to prevent failure?
- What happens when they fail anyway?



# Day 3: Resiliency, availability and performance

1

## Availability and resilience

Achieving uptime and withstanding disruptions

2

## Metrics and regulations

What gets measured, reported and scrutinized by customers and regulators

3

## Operations and controls

Best practices and greatest challenges in maintenance, staffing and security

4

## Risks and outage analysis

Root causes, cascading failures, damages and prevention

- Run time: 90 minutes (with a short break)
- Ask questions at any time

# Availability and resilience

- Keeping services running when components fail
- Using redundancy to remove single points of failure
- Designing systems to limit disruption and recover quickly

# Achieving uptime and withstanding disruptions

## Availability

How often the service is up, reachable and usable when customers need it.

- Usually measured by uptime/total time
- 99.999% (“five nines”) availability = maximum downtime of 5.3 minutes/year

## Resilience

How well the system withstands disruption, absorbs failure and recovers.

Often assessed by:

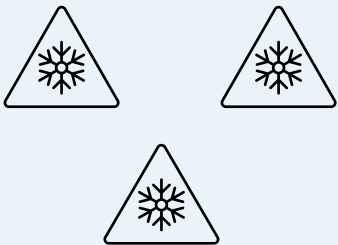
- Redundancy levels
- Recovery speed
- Failure containment

*Takeaway: Availability is the observable outcome; resilience is the capability that helps protect it.*

# Using redundancy to remove single points of failure

## N

- Sized to meet the expected peak load
- No additional redundant components



## N+1

- One additional component beyond what is needed to support the peak load

## N+2

- Two additional components beyond the required peak-load capacity

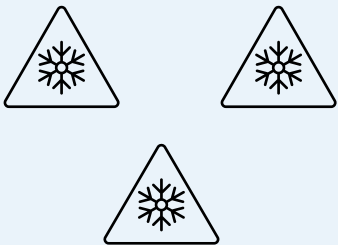
## 2N

- The full required system capacity is duplicated
- Each can support the entire load

# Using redundancy to remove single points of failure

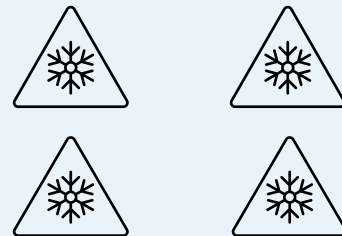
## N

- Sized to meet the expected peak load
- No additional redundant components



## N+1

- One additional component beyond what is needed to support the peak load



## N+2

- Two additional components beyond the required peak-load capacity

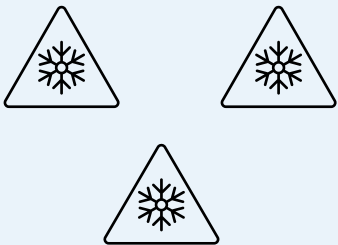
## 2N

- The full required system capacity is duplicated
- Each can support the entire load

# Using redundancy to remove single points of failure

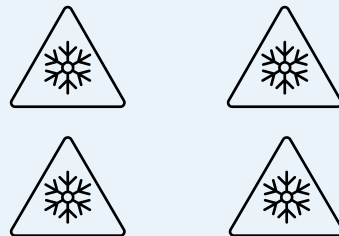
## N

- Sized to meet the expected peak load
- No additional redundant components



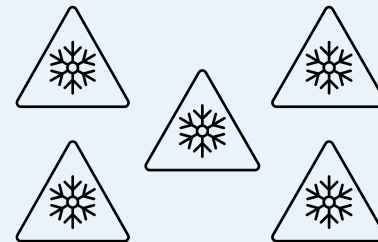
## N+1

- One additional component beyond what is needed to support the peak load



## N+2

- Two additional components beyond the required peak-load capacity



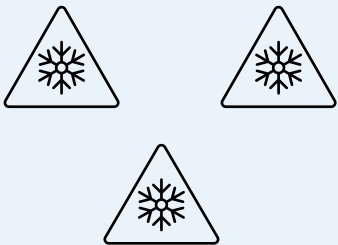
## 2N

- The full required system capacity is duplicated
- Each can support the entire load

# Using redundancy to remove single points of failure

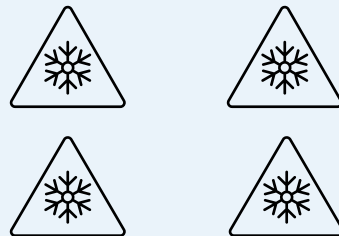
## N

- Sized to meet the expected peak load
- No additional redundant components



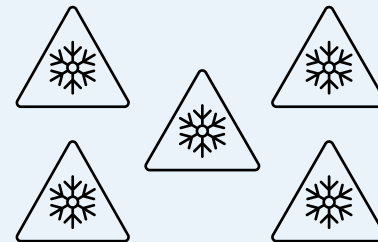
## N+1

- One additional component beyond what is needed to support the peak load



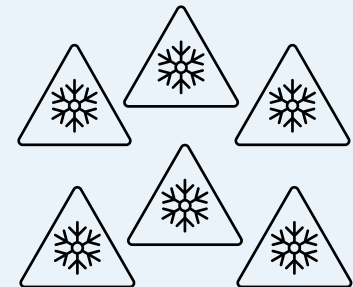
## N+2

- Two additional components beyond the required peak-load capacity



## 2N

- The full required system capacity is duplicated
- Each can support the entire load



- Note: having spare equipment is not the same as having a fully resilient system.
- Redundancy has to exist across the entire supporting path (pumps, electrical feeds, etc.)

# Uptime Institute Data Center Site Infrastructure Tier Standard



Basic  
Capacity



Redundant  
Components



Concurrently  
Maintainable



Fault  
Tolerant

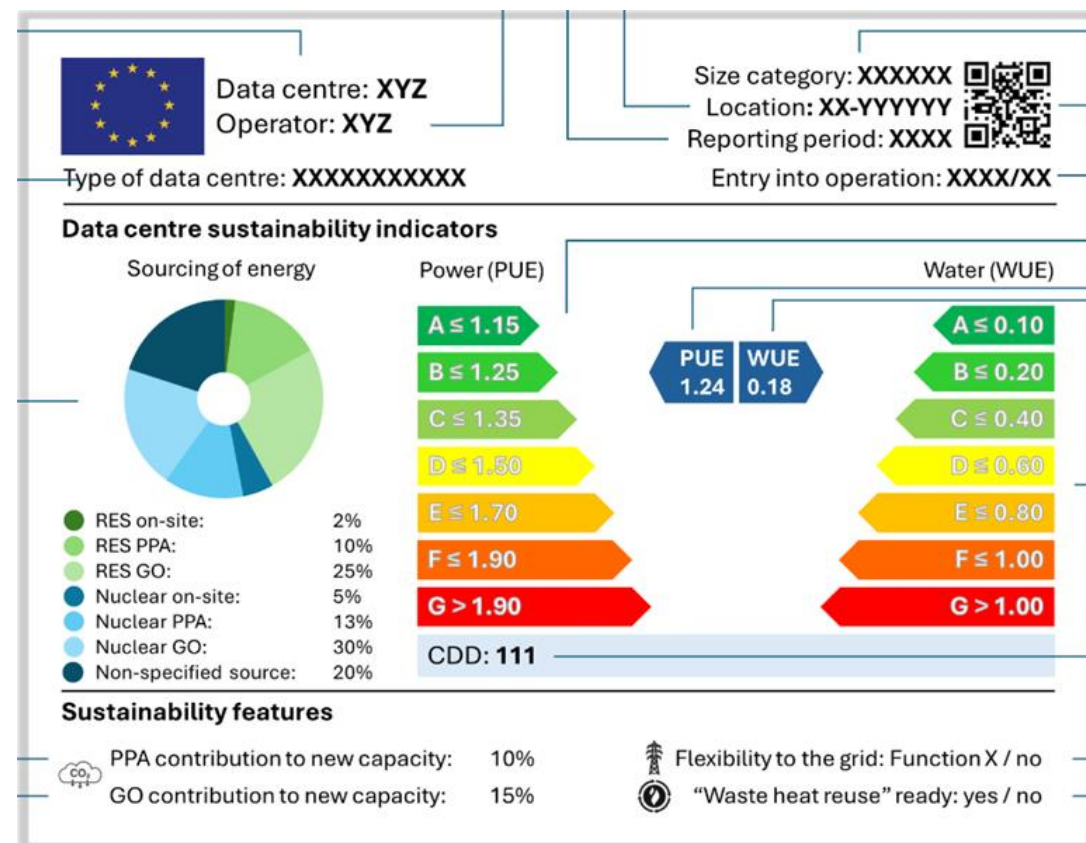
- ☐ Higher Tiers place greater emphasis on redundancy, maintainability and fault tolerance.
- ☐ A higher Tier is not automatically the appropriate choice for every facility
- ☐ Infrastructure design is only part of resilience.
- ☐ How the facility is staffed, maintained and operated also affects whether that design performs as intended

# Metrics and regulations

- Common data center metrics and data collection
- Meeting sustainability and resiliency requirements
- Critical National Infrastructure designation
- What's in an SLA

# Key data center metrics

| Metric                          | Definition                                                              | Purpose                                                                   |
|---------------------------------|-------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Power Usage Effectiveness (PUE) | Total facility energy / IT energy                                       | Indicates energy efficiency of the power and cooling that supports the IT |
| Water Usage Effectiveness (WUE) | Water consumed relative to IT energy use                                | Identifies exposure to water scarcity and cooling constraints             |
| Renewable Energy Factor (REF)   | The share of total power that is supplied from renewable sources.       | Helps estimate total carbon emissions from operations                     |
| Energy Reuse Factor (ERF)       | The proportion of the total energy consumption (heat) that is exported. | Shows how much data center waste heat that is reused                      |



EU Energy Efficiency Directive (EED) rating scheme label

# EU EED proposed Minimum Performance Standards

| Timeline                                    | Power usage effectiveness (PUE)                                                               | Water usage effectiveness (WUE)                              | Renewable energy factor (REF) |
|---------------------------------------------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------|-------------------------------|
| Existing data centers by 2030               | Operational PUE <1.5                                                                          | <0.4<br>(regardless of water origin: potable or non-potable) | 100%                          |
| Data centers commissioned in 2027 and later | Design PUE <1.3<br>(with operational PUE <1.4 to be achieved within three years of operation) | <0.4<br>(regardless of water origin: potable or non-potable) | 100%<br>(by 2030)             |

- Minimum performance standards for PUE, WUE and REF are under development
- May require ~40% of data centers in the EU to make significant upgrades (or relocate)
- Other countries and regions are likely to use the EED as a legislative model

# Data centers are critical infrastructure

- Digital Operational Resilience Act for financial services and data centers they use

Penalties for noncompliance include daily periodic payments of up to 1% of average daily global turnover



- Data centers are Critical National Infrastructure in the UK, with a focus on cybersecurity

CNI status can give new projects priority for electrical grid connections or fuel during extended outages

But governments can make CNI data centers meet strict reporting, resiliency, and risk concentration criteria



- Cybersecurity concerns are growing



# The Service Level Agreement (SLA)

- Sets expectations for service performance
- Defines what happens if those targets are missed (incl. compensation)

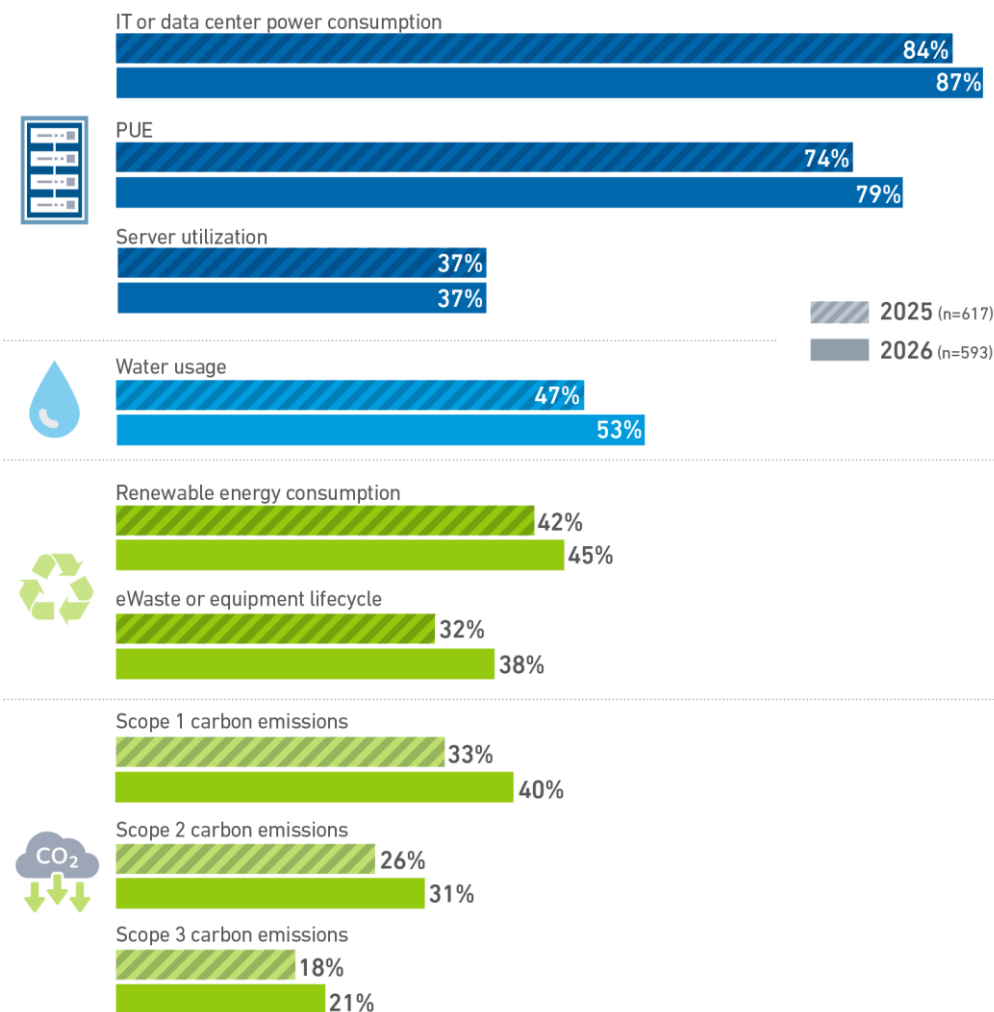
| SLA type              | Typical focus                             |
|-----------------------|-------------------------------------------|
| Internal / enterprise | Uptime and support targets                |
| Cloud                 | Availability of (many) different services |
| Colocation            | Stable power, temperature/humidity, etc.  |
| Managed hosting       | Server and service performance            |
| Network / carrier     | Connectivity and restoration              |

- While SLAs define the service commitment, operations determine whether it is achieved

# Data collection is lacking

- Current and future regulations require reporting of many data center metrics
- But many operators do not (or cannot) collect this data
- Those unprepared to meet these requirements are at risk (e.g., fines, reputational damage, etc.)

Which of the following IT or data center metrics does your organization collect for corporate sustainability purposes? Choose all that apply.



UPTIME INSTITUTE GLOBAL DATA CENTER SURVEY 2025-2026

# Operations and controls

- Risk assessments and testing
- Staffing challenges and opportunities

# Resiliency depends on operations

Resilient design



Resilient data center

# Resiliency depends on operations



# Design creates resilience capability, but operations preserve it

Documented procedures reduce improvisation during critical work

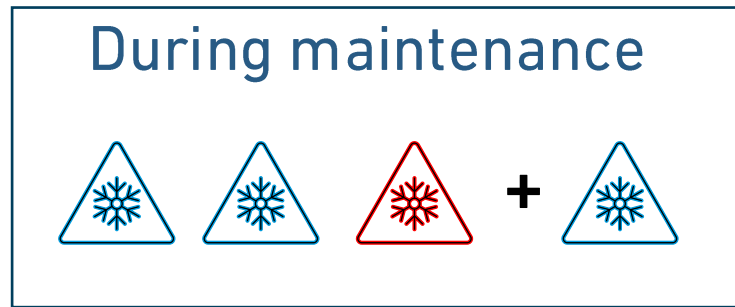
- **Standard Operating Procedure (SOP):**  
Normal operation
- **Method of Procedure (MOP):**  
Planned change
- **Emergency Operating Procedure (EOP):**  
Something has gone wrong

Effective procedures should be current, clear, accessible and practiced.



# Maintenance can reduce (and introduce) risk

## Example N+1 facility



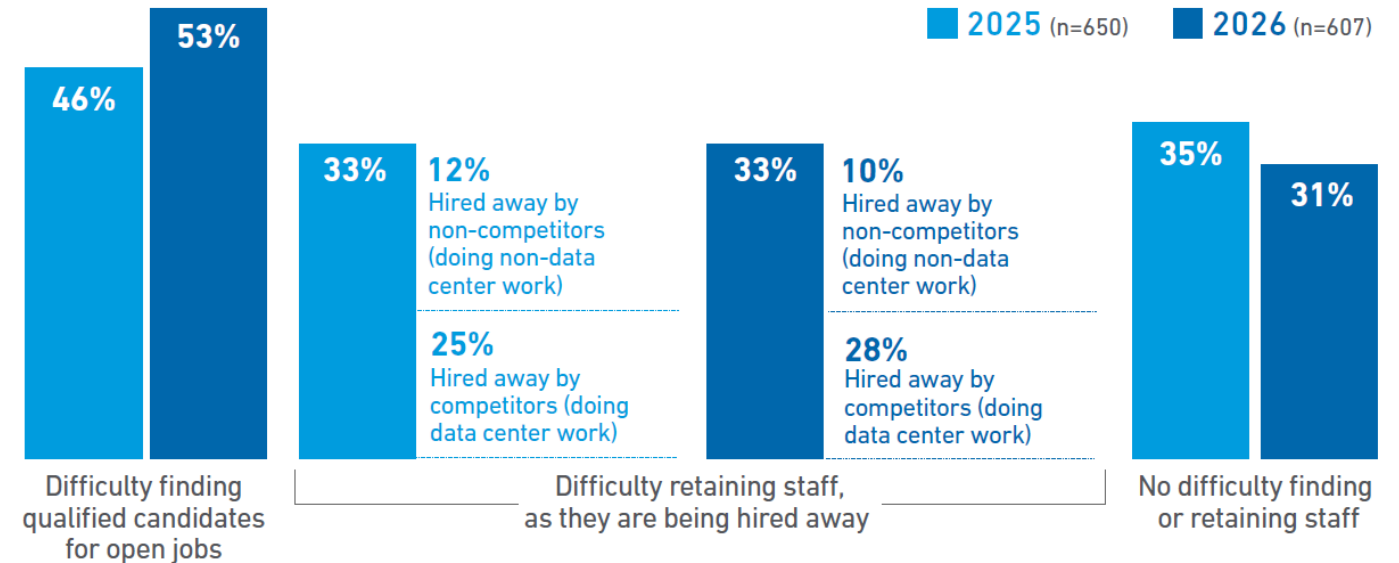
## Planned work can:

- Temporarily limit redundancy
- Change normal operating configurations
- Introduce contractors or temporary procedures

# People remain a critical control

- Qualified staff are increasingly difficult to recruit and retain
- Understaffing can increase workload, fatigue and dependence on contractors
- Training and documented procedures become more important as systems become more complex

Which of the following staffing conditions apply to your organization? Choose all that apply.



UPTIME INSTITUTE GLOBAL DATA CENTER SURVEY 2025-2026

uptime  
INTELLIGENCE

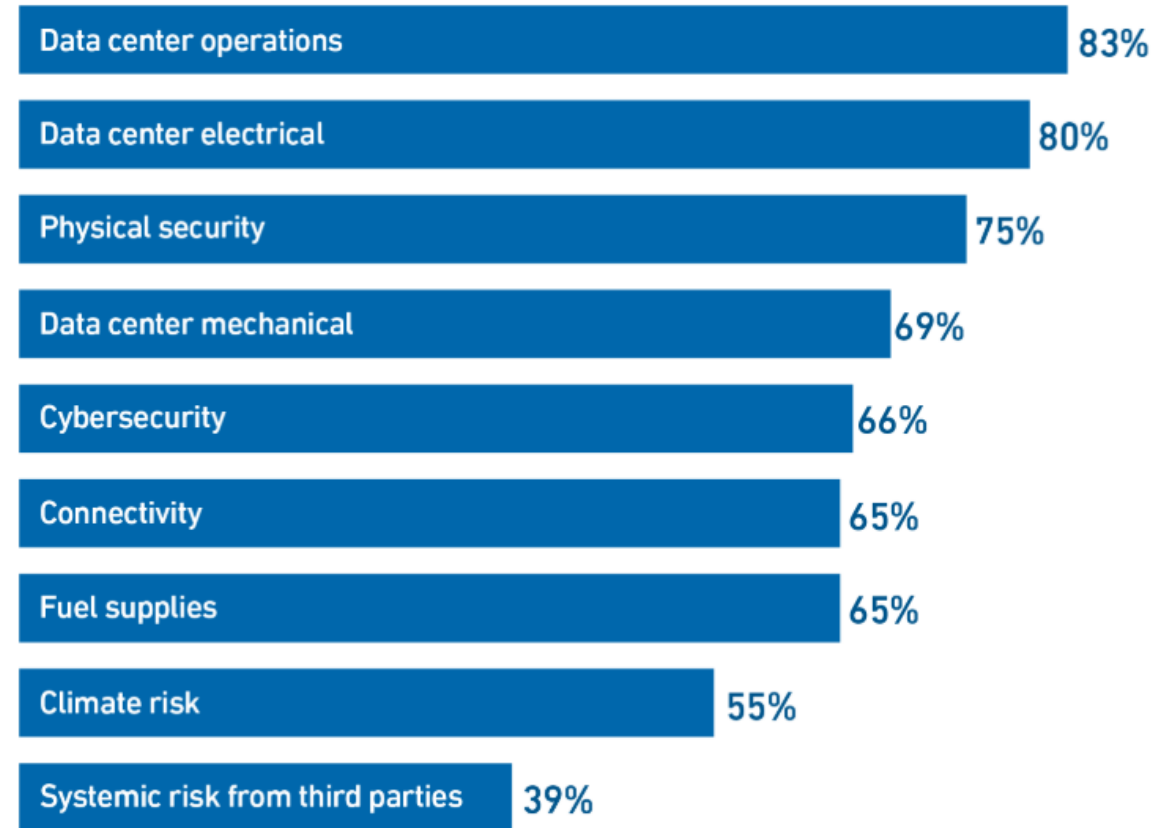
Takeaway: Reduced experience or staffing can increase the chances that threats are missed (or mishandled)

uptime®  
INTELLIGENCE

# Assessing risk and testing systems

- Most operators perform risk assessments, but approaches and scope vary
- Core infrastructure risks are commonly reviewed, but third-party systemic risks often receive less attention
- Not every threat is inside the facility or under the operator's control

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



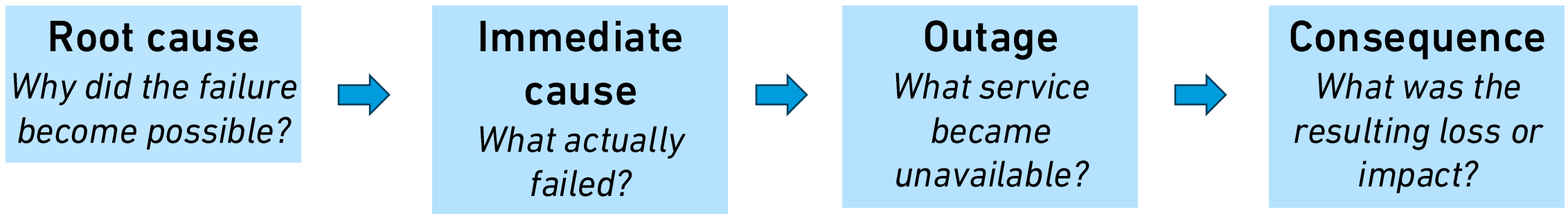
UPTIME INSTITUTE DATA CENTER RESILIENCY SURVEY 2026

# Risks and outage analysis

- Outage frequency and severity
- Root cause analysis
- Prevention and mitigation
- The impact of outages

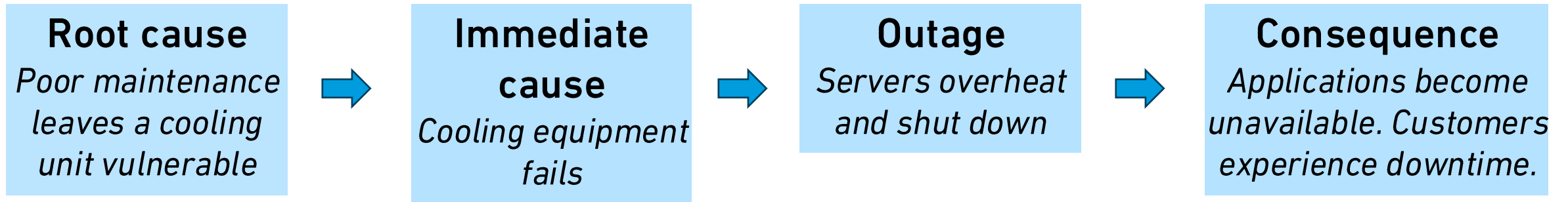
# An outage is the event — not necessarily the underlying cause

- A data center outage is an unplanned loss or material degradation of IT service availability.
- It may affect part of a facility or service or, in extreme cases, requires the entire data center to shut down.



# An outage is the event — not necessarily the underlying cause

- A data center outage is an unplanned loss or material degradation of IT service availability.
- It may affect part of a facility or service or, in extreme cases, requires the entire data center to shut down.



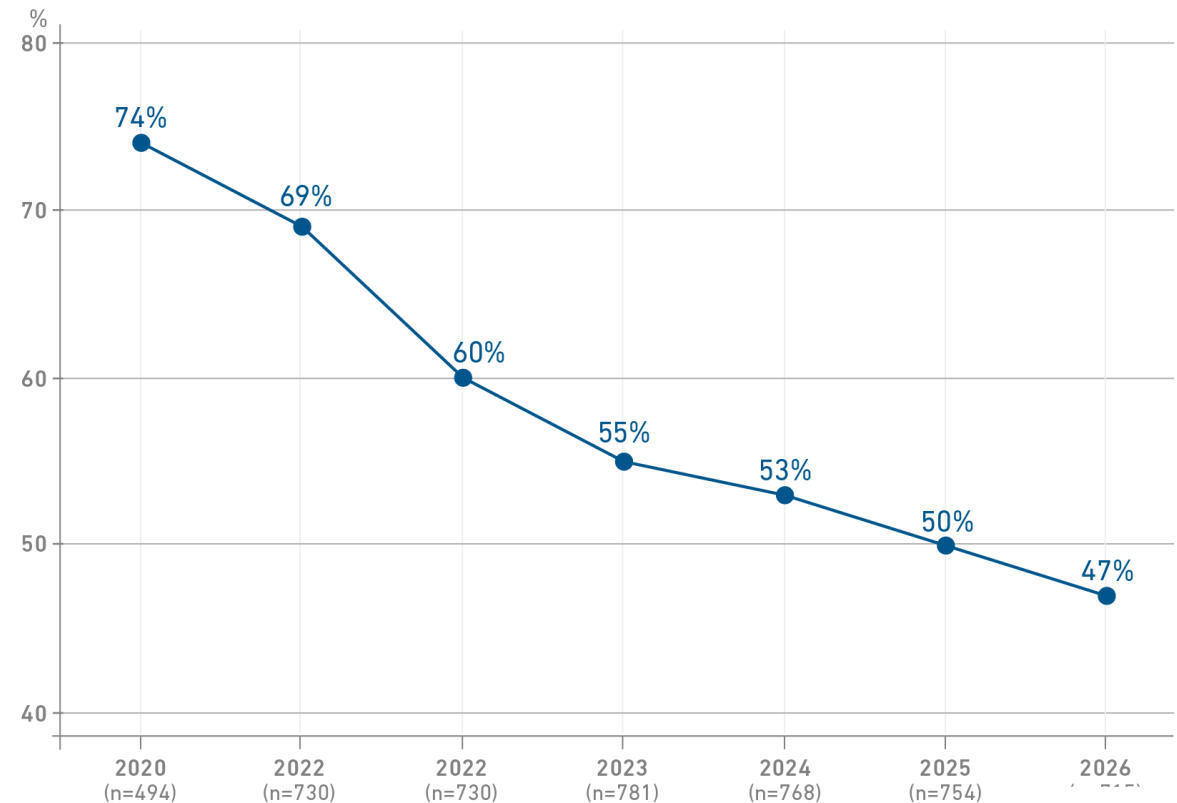
# Uptime Institute Outage Severity Rating

| 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. |

# Outages are becoming less frequent, but are still a challenge

- Fewer operators say they had an impactful outage in the past three years – maintaining a strong trend.
- As external risks intensify, and new systems are introduced at scale, the improving trend is not guaranteed to continue.

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

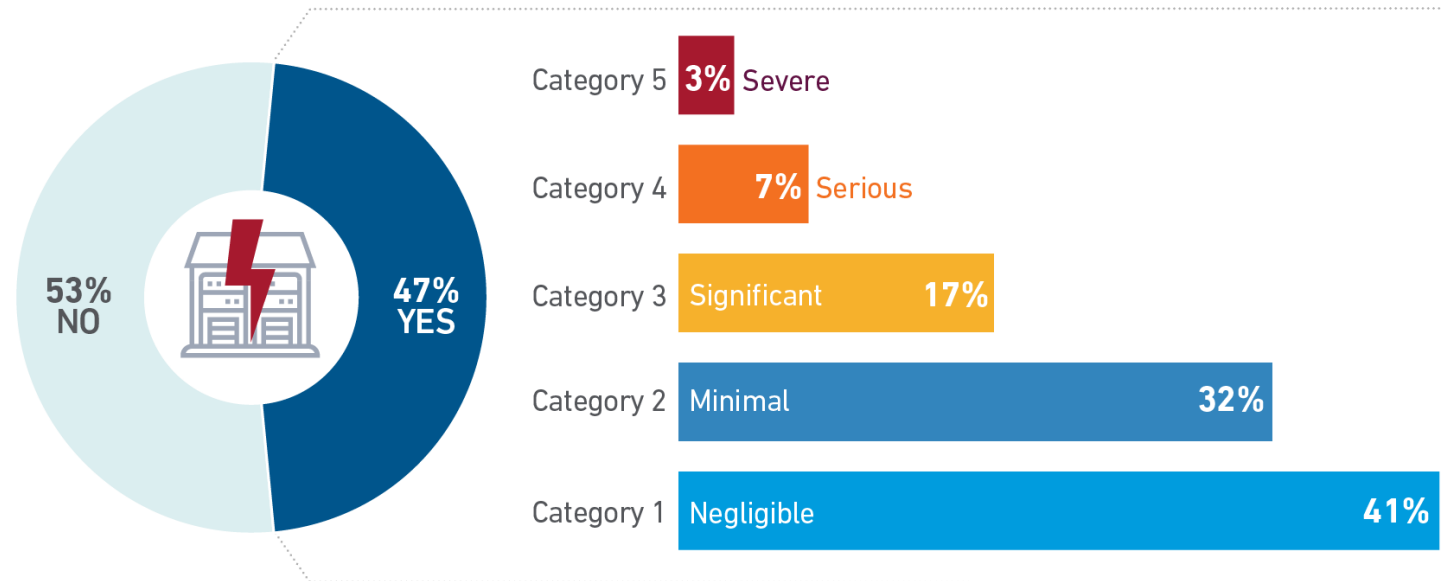


UPTIME INSTITUTE GLOBAL DATA CENTER SURVEY 2025-2026

# Major outages remain despite improving reliability

- Most operators who did have an outage in the past three years say it had little impact.
- But 1 in 10 outages are still serious or severe.
- These outages may have greater consequences than in the past as reliance on digital services grows.

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=715)

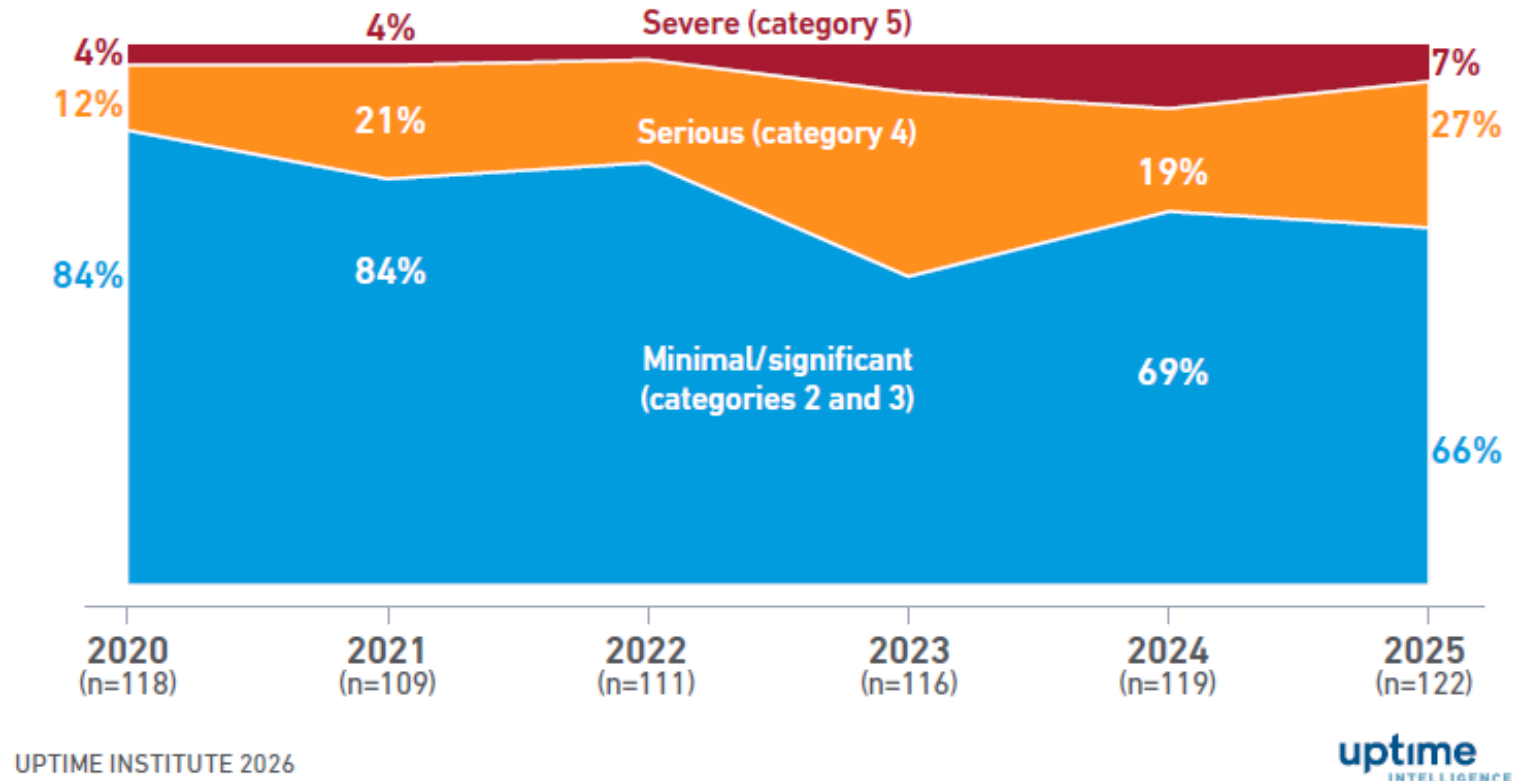


(Responses for "Don't know" not included.)

UPTIME INSTITUTE GLOBAL DATA CENTER SURVEY 2026

# Public outage data also shows growing severity

- One in three public outages tracked in 2025 were in the highest impact categories
- Category 4 incidents rose while Category 5 outages declined slightly
- On average, 15-20 high-profile organizations will suffer a major outage with financial, reputational and other consequences.



# Most severe outages in 2025:

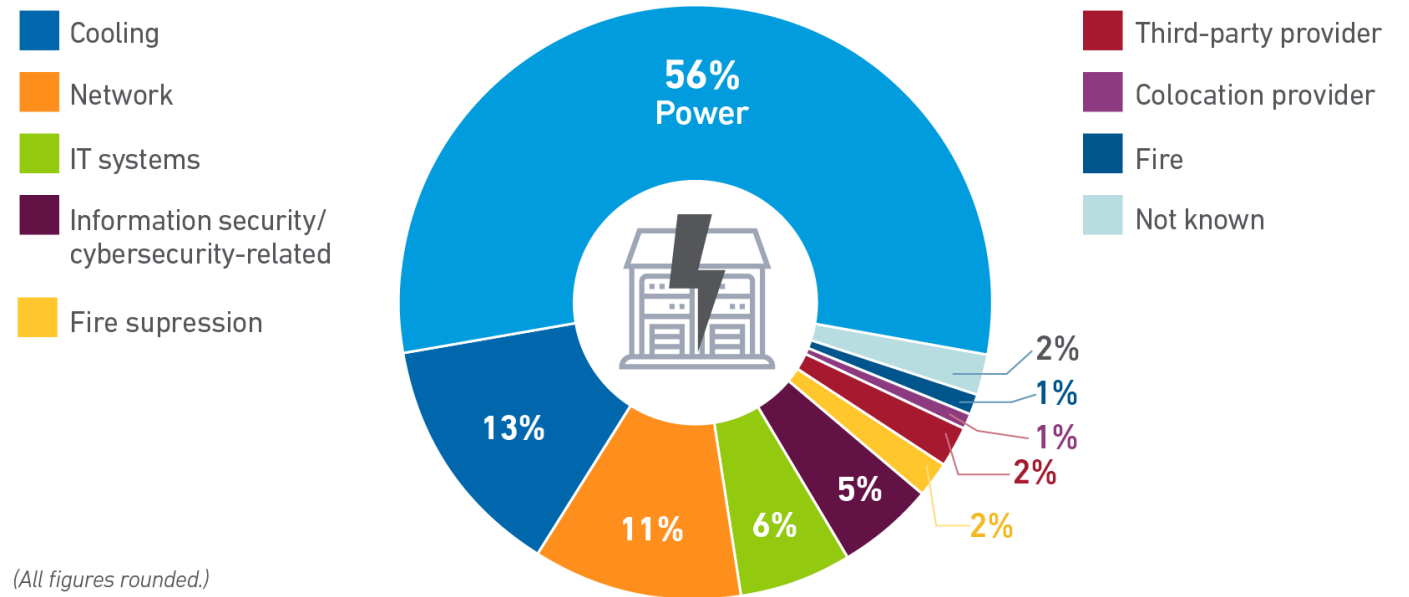
| Company                   | Industry           | Severity rating | Year (quarter) | Cause                         | Impact                                                                                                                                                                                                                                                                                                  |
|---------------------------|--------------------|-----------------|----------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Barclays                  | Financial services | 5               | 2025 (Q1)      | Configuration error/ software | A mainframe software failure disrupted online banking and payments during the UK tax filing deadline, resulting in outages lasting multiple days. More than half of transactions failed, leading to millions of pounds in compensation payouts.                                                         |
| Marks & Spencer           | Retail             | 5               | 2025 (Q2)      | Cyberattack/ ransomware       | A ransomware attack encrypted core systems, halting online sales for 46 days and exposing customer data. The incident cost an estimated £300 million in lost sales and led to a sharp decline in market value.                                                                                          |
| Government of South Korea | Government         | 5               | 2025 (Q3)      | Lithium-ion battery fire      | A lithium-ion battery entered thermal runaway during removal from an IT facility, triggering a fire that disrupted hundreds of systems including emergency services. It resulted in permanent loss of hundreds of terabytes of government data as well as injuries to personnel.                        |
| Jaguar                    | Manufacturing      | 5               | 2025 (Q3)      | Cyberattack/ ransomware       | A ransomware attack using stolen employee credentials forced Jaguar to shut down manufacturing and dealership systems for five weeks. Estimated losses reached £1.9 billion, with widespread supply chain disruption. The UK government provided financial support to mitigate broader economic impact. |
| Ingram Micro              | Digital services   | 5               | 2025 (Q3)      | Cyberattack/ ransomware       | A ransomware attack forced Ingram Micro to shut down core systems, halting order processing and logistics operations. Attackers accessed systems via compromised VPN credentials and threatened to leak 3.5TB of stolen customer data.                                                                  |

- Severe outages attract the most scrutiny and reporting.
- Rare events (e.g., lithium-ion battery fires) can have extreme consequences
- Cyberattacks are a growing concern, and can affect critical systems
- Some threats remaining hidden or underreported until damage is done

# Power issues remain the top cause of impactful outages

- Since 2020, power issues account for the highest share of impactful outages.
- Separate Uptime data shows UPS and genset failures are the primary underlying causes.
- Root cause analysis of outages is difficult – many interrelated factors are involved.

What was the primary cause of your data center's most recent impactful incident or outage? (n=85)



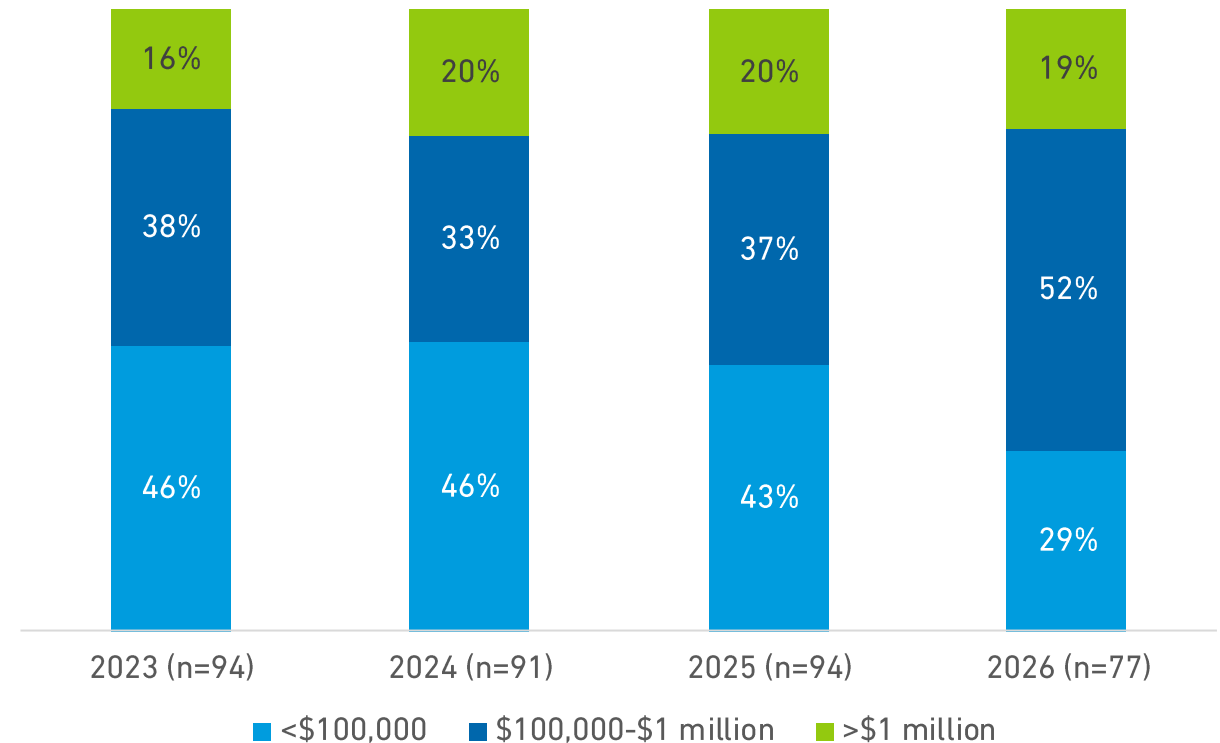
(All figures rounded.)

UPTIME INSTITUTE GLOBAL DATA CENTER SURVEY 2026

# Outage costs continue to rise

- Outages have become more expensive for the third consecutive year.
- Nearly one in five outages still cost over \$1 million.
- This trend will likely continue due to higher costs of equipment, greater workload concentration, and more reliance on digital services

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



# Key points from Days 1-3

## **Data centers are critical infrastructure**

- Failures can affect many customers, services and businesses at once.

## **Resilience is more than design: operations**

- Maintenance, testing and people all determine real-world performance.

## **Loss severity depends on concentration and recovery**

- What matters is not only what fails, but how much depends on it and how quickly service can be restored.

## **Exposure is system-wide**

- Facility, IT, suppliers, contracts, customers and dependencies all shape the risk.

Visit [www.uptimeinstitute.com](https://www.uptimeinstitute.com) for more information.



Uptime Annual Survey  
Executive Summary



Uptime Intelligence  
Free Trial Request

**uptime**<sup>®</sup>  
**INTELLIGENCE**

Uptime Institute is the Global Digital Infrastructure Authority.  
Uptime Institute is headquartered in New York, NY, with offices  
in Seattle, London, Sao Paulo, Dubai, Singapore, and Taipei.

©2025 Uptime Institute, LLC. All Rights Reserved.

**Uptime Institute**  
405 Lexington Avenue  
New York, NY 10174