Rillor

RESEARCH REPORT

What causes data-center outages: surveys and incident reviews

Uptime's 2025 survey puts power behind 45% of impactful outages. Published incident reviews show how faults in power, cooling and water spread, and what set recovery time.



Contents

01 Summary

02 Background

03 Method

04 Findings

05 Implications

06 Limits of this analysis

07 Sources

Summary

Surveys show how often data centers suffer impactful outages and which systems fail, and published incident reviews show how one fault gets past the protection meant to contain it.

- Half of the operators in Uptime Institute's 2025 survey reported at least one impactful outage, one significant enough to record, at their facility in the past three years, down from 74% in 2020 [1]. One in 10 said their most recent one was serious or severe [1].
- Power caused 45% of the most recent impactful outages in Uptime Institute's 2025 survey, down from 54% in 2024, with cooling at 14% and network at 11% [1]. Uptime's 2026 survey puts power and cooling together at more than two-thirds [5].
- Uptime's Data Center Resiliency Survey 2025 found uninterruptible power supply (UPS) failures behind 42% of power-related IT service outages, transfer switch failures behind 36% and generator failures behind 28% [1].
- In Uptime's pooled 2025 and 2026 survey responses, 70% of respondents whose cooling had no spare capacity (N) reported an impactful outage in three years, against 39% of those with fully duplicated cooling (2N), a correlation Uptime's authors caution is not causation [5].
- In cloud providers' own incident reviews from 2012 to 2023, protection failed when called on: generators that failed to provide stable voltage, cooling that shut down when its controls failed and 13 chillers that did not restart on their own after a voltage sag [15, 16, 17].
- Recovery time depended on what came after the fault: chiller restart order, where data replicas sat and backup sites that failed to take over [17, 18, 24].
- In July 2024, a transmission line fault led about 1,500 MW of data-center load to transfer to backup power at once, with no service outage reported, and grid operators had not anticipated it [21].
- In Uptime's 2025 survey, 87% of operators with an impactful outage in the past three years said better management, processes or configuration could have prevented it [1].

Background

A data center's power and cooling form one chain from the utility to the rack: grid supply, transfer switches, generators, UPS systems and batteries, then chillers and the controls that run them. An outage starts where a link fails and the one behind it does not take over.

Two kinds of public evidence describe that chain. In 2025 Uptime Institute asked more than 800 data center owners and operators what caused their most recent impactful outage, one "significant enough to record, even if the resulting costs were negligible" [1]. Those shares say which systems fail and little about how a failure spreads. Incident reviews do the reverse, tracing single events from trigger to recovery [15, 16, 17, 18, 19, 20, 21, 24].

Uptime warns that outages "are often under-reported or disclosed with limited details", and that "failures often involve multiple interdependent systems that can obscure the initial trigger" [1]. The load is changing too. Uptime's 2026 survey release reports more operators with peak rack densities of 30 kW or higher [2], and in November 2025 Uptime reported that in the worst cases GB200 NVL72 racks can see sudden power climbs from around 60 to 70 kW to more than 150 kW, against a maximum specification of 132 kW [10].

Method

What was examined. What causes data center outages, from survey data and published incident reviews, and what set the time to recover.

Sources. Uptime's 2025 survey report, its press releases and Journal articles [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14]. Incident reviews by Amazon Web Services [15, 16], Microsoft Azure [17] and Google Cloud [18, 19], and Cloudflare's post-mortem on a facility it leases [20]. The North American Electric Reliability Corporation (NERC) [21, 22, 23], the Monetary Authority of Singapore (MAS) [24, 25], CME Group's annual report and CyrusOne's statement as reported by DatacenterDynamics [26, 27], Korean press reports on a 2025 battery fire [28, 29, 30], three annual reports [31, 32, 33] and AWS's compute service level agreement [34]. All were viewed on 8 November 2026.

How. Uptime's Annual Outage Analysis reports are for subscribers, so only figures in its public survey report, press releases and Journal articles are used. The UPS, transfer switch and generator shares are credited to the Resiliency Survey 2025, as the survey report credits them [1]. Each incident comes from its own published account, the authors' own and not independently verified. Operators are named only as their own reviews or filings name them, or as Uptime does. The Daejeon facility is called a government-run data center, as The Korea Herald calls it [28]. Times are in the zone each review uses. "Derived" marks arithmetic on a source's numbers.

Incidents reviewed.

Date	Event	Account	Trigger
29 June 2012	AWS, one Availability Zone in US East	AWS [16]	Voltage spike during a storm
23 August 2019	AWS, one Availability Zone in Tokyo	AWS [15]	Bug in a cooling control system's failover
10 to 11 March 2021	OVHcloud SBG2, Strasbourg	Uptime [12, 13]	Fire, with two UPSs at the heart of the blaze, per firefighters
19 July 2022	Google Cloud, europe-west2-a	Google [19]	Redundant cooling failed in extreme heat
15 October 2022	Colocation facility in Pangyo	Uptime, from police reports [12]	Fire that started in a battery room

Date	Event	Account	Trigger
25 April 2023	Google Cloud, europe-west9	Google [18]	Cooling pipe leak into a UPS room, then fire
30 August 2023	Microsoft Azure, Australia East	Microsoft [17]	Lightning-induced voltage sag
14 October 2023	Data center hosting DBS and Citibank systems, Singapore	MAS [24]	Cooling system malfunction
2 November 2023	Leased facility near Hillsboro, Oregon	Cloudflare [20]	Utility feed event, then a transformer ground fault
10 July 2024	Data-center load, Eastern Interconnection	NERC [21]	Lightning arrestor failure on a 230 kV line
26 September 2025	Government-run data center, Daejeon	Korean press [28, 29, 30]	Fire during a lithium-ion battery relocation
27 November 2025	CME Group's data center operated by CyrusOne	CME [26], CyrusOne via DatacenterDynamics [27]	Chiller plant failure caused by human error

Findings

1. How often impactful outages occur

Survey year	Reported an impactful outage in the past three years	Respondents
2020	74%	494
2021	69%	730
2022	60%	730
2023	55%	781
2024	53%	768
2025	50%	754

Source: [1], Figure 10.

Uptime calls the 2025 figure the fifth consecutive year of decline and says the pace of improvement has slowed [1]. Rating their most recent impactful outage, 39% called it negligible, 34% minimal, 18% significant, 7% serious and 3% severe [1].

Among respondents whose outage was significant, 20% reported a cost above $1 million in both 2024 and 2025, and the share between $100,000 and $1 million rose from 33% to 37% [1]. Uptime's survey report names "inflation, rising labor expenses, hardware replacement, penalties for service level agreement (SLA) breaches, and reputational damage" as reasons [1]. Its July 2026 release says fewer operators again reported an impactful outage, one in ten outages is still serious or severe, and costs "continue to climb sharply", with no 2026 share given [2].

2. Power as the leading cause

Primary cause of the most recent impactful outage, 2025	Share
Power	45%
Cooling	14%

Primary cause of the most recent impactful outage, 2025	Share
Network	11%
IT systems (hardware or software)	9%
Fire suppression	6%
Information security-related	5%
Unknown	4%
Fire	2%
Third-party provider	2%
Colocation provider	1%

Source: [1], Figure 12, n=96, rounded.

With 96 answers, each respondent is about one percentage point (derived from [1]). The power share fell from 54% in 2024, reversing a rise since 2020 [1]. Uptime's 2022 survey put power at 44%, "greater than the second, third and fourth most common outage causes combined" [6]. The only public 2026 cause figure is power and cooling together at more than two-thirds [5].

Fire suppression rose six points from 2024, which Uptime puts down to "wider deployment of fire suppression systems and a higher rate of accidental discharges" [1]. Information security-related outages rose four points [1]. Uptime's 2026 outage release adds that external infrastructure failures are more prominent in publicly reported outages, and that third-party IT and data center service providers account for about two-thirds of the public outages it has tracked over nine years [3].

In June 2023, Uptime put the frequency of power-related outages partly down to "power system complexity and a dependence on moving parts", and noted that compared with other systems such as cooling, "power is more prone to fail completely, rather than operating at partial capacity" [6].

3. Inside power failures: UPS, transfer switches and generators

The 2025 survey report quotes the separate Resiliency Survey 2025: of IT service outages that stem from power, 42% came from UPS failures, 36% from transfer switch failures and 28% from generator failures [1]. The shares add to 106% (derived from [1]), and the public report does not give the question's form.

In June 2023, Uptime's Journal named the weak points. Loss of critical load from a UPS failure is often "due to batteries not being monitored closely enough by experienced technicians" [6]. Operators are advised to disconnect from the grid once a year, yet many avoid it, so "lurking failures in transfer switches and paralleling switchgears may go undetected" [6]. Long grid outages can exceed on-site fuel, and most US diesel generators are limited to 100 hours of full load a year [6]. The Resiliency Survey 2023 found more than 70% of organizations run pull-the-plug tests, while less than half of operators involve their utility [7]. In some designs, tests that open an isolation device can bypass the power-loss detection and the controls that switch to on-site power [7].

US East, June 2012. A voltage spike at 7:24pm PDT during a storm in Northern Virginia started a transfer to generator power in two data centers [16]. In one, "each generator independently failed to provide stable voltage" [16]. Utility power failed again at 7:57pm, the UPS systems ran down and servers lost power at 8:04pm, and all racks had power again at 8:24pm [16]. The generators were less than two years old, tested weekly and load-tested in full that May [16]. AWS's fixes lengthen the time its switching equipment gives generators to reach stable power and add on-site staff to switch by hand before UPSs discharge [16].

Near Hillsboro, Oregon, November 2023. Cloudflare says the facility's operator started generators after a utility event at 08:50 UTC without telling it, and "none of our observability tools were able to detect that the source of power had changed" [20]. In its account, at about 11:40 UTC a transformer ground fault occurred, and the protective response also shut down all the generators [20]. Batteries meant to carry the facility for about 10 minutes "started to fail after only 4 minutes" [20]. Cloudflare says facility staff told it unofficially that the generators had to be restarted by hand, which happened at 12:48 UTC, after which faulty circuit breakers had to be replaced [20].

In November 2025, Uptime wrote that among power equipment, engine generators would be the most stressed if exposed to the full extent of training-cluster power swings, and gave an example of facility load stepping from 45% to 50% of design capacity to 80% to 85% within a second, on repeat, possibly "at the expense of reduced expected life or outright failure" [10].

4. Redundancy and outage rates

Uptime defines N as capacity sized to the expected peak load, N+1 and N+2 as one or two additional components, and 2N as the full capacity duplicated in two independent paths or systems [5]. In 2025, 42% of respondents named 2N as their usual power redundancy and 41% N+1 [1].

Uptime's October 2026 analysis pooled over 1,200 responses from 2025 and 2026 [5]. The share reporting an impactful outage rose from 39% with 2N cooling to 70% with N, and from 42% with 2N power to 68% with N [5]. Outages in categories 3 to 5, broadly those with a meaningful financial impact, came to around 8% to 11% with 2N and about 19% to 22% with N [5].

Against N, likelihood of a category 3 to 5 outage in three years	N+1	N+2	2N
Cooling	About 36% lower	About 53% lower	About 63% lower
Power	About 23% lower	About 37% lower	About 44% lower

Source: [5].

Against N+1, 2N cooling was 42% less likely to have an outage [5]. The authors write that "correlation is not causation", that the analysis cannot isolate redundancy from operational maturity, maintenance, equipment condition and design, and that the N samples are small [5]. Uptime's 2025 report adds that "physical redundancy alone, however, can be insufficient protection against outages" [1].

Three incidents show why. A control failure in Tokyo "caused multiple, redundant cooling systems to fail" [15]. Google reported "a simultaneous failure of multiple, redundant cooling systems" in its europe-west2-a zone during extreme heat [19]. In Australia East, halls that needed four chillers had seven, and one voltage sag stopped chillers across several data centers [17].

5. Cooling controls and chiller restart

Tokyo, August 2019. At 12:36 PM JST, a small percentage of EC2 servers in one Availability Zone shut down from overheating [15]. A bug in the third-party control system, triggered as it failed away from one control host, left it unresponsive [15]. The design called for maximum cooling on control failure, but in part of the data center the cooling shut down, and purge failed too, both traced to the programmable logic controllers [15]. With "minimum visibility", the team reset each unit by hand [15]. Cooling returned at 3:21 PM, the vast majority of instances recovered by 6:30 PM, and some were retired after hardware failures [15]. AWS disabled the failover mode and began work so purge can bypass the controllers [15].

Australia East, August 2023. A lightning strike about 18 miles away caused a voltage sag that shut down chillers for multiple data centers, and 13 failed to restart [17]. Engineers restarted them one data center after another, and by the last five the chilled water was too hot to allow restart [17].

Time (UTC)	Event
08:41, 30 August	Voltage sag
08:43	13 chillers fail to restart

Time (UTC)	Event
11:34	Decision to shut down affected infrastructure
12:12	Five chillers restarted by hand
15:10	Power restored to all hardware
05:00, 31 August	All virtual machines recovered
20:00, 3 September	All databases online

Source: [17].

Microsoft found that added load had left the chillers "susceptible to a timing defect in the Chiller Management System", changed the restart order to a load-based sequence that gives every hall partial cooling, and wrote that staffing at the time "would have been sufficient to prevent impact" with that sequence [17].

europe-west2-a, July 2022. Google's zone lost cooling through "a simultaneous failure of multiple, redundant cooling systems combined with the extraordinarily high outside temperatures" [19]. It terminated 42% of preemptible VMs across the region to cut heat, then powered the data center down [19]. Uptime, writing on the European heat wave of 18 and 19 July 2022, when Heathrow passed 40°C, wrote that "most susceptible are air-cooled mechanical compressors in direct-expansion (DX) units and water chillers without economizers" [9].

Singapore, 2023, and Aurora, Illinois, 2025. MAS told Parliament that a cooling malfunction at the data center hosting DBS and Citibank systems raised temperatures until the banks' systems shut down [24]. CME's annual report says that on 27 November 2025 "our largest data center owned and operated by CyrusOne experienced a critical cooling failure caused by human error", and that CME halted its markets, which opened the next day on a delayed basis [26]. CME leases that data center from CyrusOne in Aurora, Illinois [26]. CyrusOne, as reported by DatacenterDynamics, described "a chiller plant failure affecting multiple cooling units" at its CHI1 facility and brought in temporary cooling [27].

6. Water, batteries and fire

In 2021, Uptime reported that its member database of over 8,000 incidents since 1994 recorded 11 fires, all contained, and that accidental discharge of suppression systems had caused significantly more serious disruption than fires [14]. In January 2023 Uptime counted 14 publicly reported, high-profile outages caused by fire or fire suppression since 2020 [12].

europe-west9, April 2023. At 16:46 US/Pacific on 25 April, "a cooling system water pipe leak occurred in one of the data centers in the europe-west9 region", in a non-Google portion of the facility, and the water entered a UPS room and led to a fire [18].

Time (US/Pacific)	Event
16:46, 25 April	Cooling water pipe leak
19:14	Smoke detected
20:08	Engineers alerted to the battery room water leak and fire
22:45	Building fire suppression water supply runs out
23:04	One building shut down on the fire marshal's order
04:11, 26 April	Battery room fire reported extinguished

Source: [18].

The fire took nearly 16 hours to extinguish, which delayed recovery, and customers lost no data [18]. Google's listed actions include a water intrusion risk analysis for all data centers that host Google Cloud and evaluating drip trays in multi-story locations with water on floors above [18].

Pangyo, October 2022. Uptime reported that, according to police reports, a fire at a colocation facility operated by SK Inc. C&C "started in a battery room before spreading quickly to the rest of the building", taking tens of thousands of servers offline and affecting KakaoTalk and Naver [12]. The cause was disputed: Kakao pointed to the lithium-ion batteries, and SK released what it said were battery management records showing no deviation, which some local media reports contradicted [12].

Strasbourg, March 2021. OVHcloud's 2 MW SBG2 was destroyed, and firefighters placed two UPSs at the heart of the blaze, one worked on that morning [13]. Uptime reported that the French investigation bureau found the lack of an automatic extinguisher system, delayed electrical cutoff and building design contributed to the spread, and put the estimated cost to the operator at more than €105 million, less than half insured [12].

Daejeon, September 2025. The Korea Herald reported on 28 September 2025 that the government-run data center housed 647 government systems, 96 of them confirmed directly damaged, and that a UPS battery disconnected for relocation was identified as the source [28]. The Interior Ministry said the batteries had been in place a year past their recommended 10-year lifespan [28]. Korea JoongAng Daily reported on 10 October

2025 that, per witnesses in the police investigation, auxiliary power to the battery system stayed on, logs showed about 90% charge against manufacturers' guidance to discharge below 30% before transport, and 709 systems were disrupted [29]. The Asia Business Daily reported on 7 September 2026 that the Board of Audit and Inspection found 18 violations and improper practices, and that the relocation went to two firms not registered for electrical construction and was done with only one of eight battery racks powered down [30].

Uptime wrote that lithium-ion batteries present a greater fire risk than valve-regulated lead-acid ones, that fire-resistant battery compartments, required at Tier IV, can reduce the risk of facility-wide outages, and that water and foam are likely to perform better than gas in a major thermal runaway [12]. It noted in October 2026 that IT-agnostic direct liquid cooling designs do not guarantee every rack redundant supply and return manifolds [11].

7. Grid faults and transfers to backup power

NERC's January 2025 review describes an event with no reported service outage [21]. At about 7:00 p.m. Eastern on 10 July 2024, a lightning arrestor failed on a 230 kV line in the Eastern Interconnection, and the line's auto-reclosing produced six faults in 82 seconds [21]. About 1,500 MW of "exclusively data center-type load" disconnected through customer-side protection [21]. "The data centers transferred their loads to their backup power systems in response to the disturbance," NERC wrote [21]. About 1,260 MW did not return for hours, and grid operators had to bring voltage back down [21].

A typical scheme counts three voltage disturbances in about one minute, then keeps the load off the grid until staff transfer it back by hand [21]. NERC's July 2025 white paper reports an ERCOT event of about the same size, which involved many types of load [22]. Its alert of 9 September 2025 reports multiple events of 1,000 MW or more of unexpected large-load reduction, mostly in 2024 or 2025, recommends post-disturbance voltage and frequency recovery requirements for large loads, and asks entities to describe their voltage and frequency ride-through requirements [23].

Grid events started three other chains: the 2012 storm [16], the 2023 sag in Australia East [17] and the Oregon utility event [20]. Uptime wrote that "a loss of grid power often reveals weaknesses elsewhere, including equipment maintenance regimens and staff training" [6].

8. What set recovery time

Incident	Fault cleared	Service recovered	What extended recovery
Tokyo 2019	Cooling after 2 h 45 min (derived) [15]	Vast majority by 6:30 PM JST [15]	Manual reset, hardware retired [15]

Incident	Fault cleared	Service recovered	What extended recovery
europe-west2-a 2022	Cooling impact 4 h 8 min [19]	14 h 15 min after cooling, long tail 16 h 52 min more [19]	Long-tail VMs that needed manual reconciliation, and zonal failover automation problems [19]
europe-west9 2023	Fire out after nearly 16 hours [18]	Region primarily recovered at 19:00 on 26 April, after Spanner quorum at 12:47 [18]	Two of three Spanner replicas in one building [18]
Australia East 2023	Hardware power at 15:10 [17]	Full mitigation 20:00 on 3 September [17]	Storage and database dependencies [17]
Singapore 2023	Not stated [24]	Early on 15 October [24]	Backup sites failed to take over [24]
Oregon 2023	Clean power at 22:48 UTC [20]	Incident ended 04:25 UTC on 4 November [20]	Full bootstrap of the facility: configuration servers took 3 hours, then each server 10 minutes to 2 hours, in parallel with some services in sequence [20]

Replica placement spread one building's loss across a region. Google's regional Spanner "should have had one replica in each of the three buildings in the region. Instead, it had two of its three replicas in two different clusters in the building that was powered down", which interrupted control-plane services region-wide [18]. 79% of regional Persistent Disk volumes had a replica there and became read-only while Spanner was offline [18].

Australia East's full mitigation came about four days and 11 hours after the sag (derived from [17]), held back by dependencies on recovering storage and database services, while zone-redundant storage "remained 100% available" [17].

In Singapore, DBS could not fully recover at its backup data center because of a network misconfiguration, and Citibank because of connectivity issues [24]. Up to 810,000 attempts to reach the two banks' digital platforms were estimated to have failed, and about 2.5 million payment and ATM transactions could not be completed [24]. MAS requires critical systems to be restorable within 4 hours [24]. Both banks ran annual recovery exercises, which did not surface these issues [24].

Cloudflare restored most of its control plane at a disaster recovery facility by 17:57 UTC, and each server it rebuilt took 10 minutes to 2 hours [20]. In 2012, a bottleneck in AWS's server booting process extended recovery [16].

9. What contracts attach to outages

- Digital Realty says "substantially all" of its customer agreements carry service level commitments, and failures could bring "service level credits against customer rent payments, legal liability and monetary damages, regulatory sanctions, or, in certain cases of repeated failures, the right by the customer to terminate the agreement" [31]. It warns that outages may outlast its backup power [31].
- Equinix has service level commitments to most customers and has settled with affected customers regardless of contractual limits on liability [32]. In some leased buildings the landlord is responsible for the power connections, UPSs and generators, so Equinix could depend on the landlord and the utility to restore power [32].
- CoreWeave, a GPU cloud that leases its space, has provided service credits or refunds, could face terminations, and may or may not control infrastructure such as generators [33].

The one published credit schedule among the sources is a cloud SLA. AWS commits to 99.99% monthly uptime at the region level, with credits of 10%, 30% or 100% as uptime falls below 99.99%, 99.0% and 95.0% [34]. That allows about 4.3 minutes of downtime in a 30-day month (derived from [34]). Credits are the "sole and exclusive" remedy and carry no refund [34].

MAS does not oversee data centers and expects banks "to establish contractual agreements with data centre providers that incorporate MAS' requirements on system availability" [25].

10. Patterns across the incidents

Protection that failed on demand. Generators tested weekly failed to provide stable voltage when called on [16]. Cooling designed to run at maximum on control failure shut down [15]. Chillers that should have restarted needed people on the roof [17]. Batteries meant to last about 10 minutes began failing after 4 [20]. A fire suppression water supply ran out [18].

Tests that missed the failure. The Singapore banks' annual exercises did not surface the faults that delayed recovery [24]. Pull-the-plug tests that open an isolation device can, in some designs, bypass the power-loss detection and the switch to on-site power they are meant to test [7].

Little visibility. AWS had "minimum visibility" into its cooling in Tokyo [15], and Cloudflare could not see that its facility had moved to generator power [20].

People and procedures. In June 2022, Uptime estimated from 25 years of data that human error plays some role in about two-thirds of outages, and called it "rarely a single or root cause" [8]. Its 2025 outage release says that of major outages caused by human error, 85% stem from staff failing to follow procedures or from flawed processes and procedures [4], and the 2026 release says failure to follow procedures remains the leading driver of human error-related outages [3]. In the 2025 survey, 87% of operators with an impactful outage in the past three years said better management, processes or configuration could have prevented it [1]. CME attributed its cooling failure to human error [26].

Interactions between systems. On 13 May 2026, Uptime's Andy Lawrence said he expects failures to stem less from a single point of failure and more from "complex interactions between systems" [3].

Implications

For buyers placing GPU systems in a facility. The surveys point at power first and cooling second [1, 5], and the reviews show where to look.

- How the transfer to generator is tested, with the utility involved, and the last result [6, 7].
- Fuel on site, resupply and generator runtime limits [6], and how generators handle repeated load steps [10].
- UPS design, battery chemistry and monitoring, and whether battery rooms are compartmented [6, 12].
- What the cooling controls do when they fail, and whether purge can bypass them [15].
- Whether chillers restart on their own after a voltage sag, in what order, and who restarts them by hand [17].
- Water pipes above or beside UPS and battery rooms [18].
- The hall's power and cooling redundancy, in N terms [5].

For platform leads. Recovery was set as much by replica placement, backup sites and rebuilds as by the facility [17, 18, 20, 24]. Replicas across buildings, zone-redundant storage and failover exercises that remove a whole facility address the delays recorded [17, 18, 20].

For risk and procurement teams. Colocation filings describe credits, liability and termination for repeated failures, and give no credit percentages [31, 32]. A tenant that leases its space may not control the generators that serve it [32, 33].

Limits of this analysis

- Survey figures are self-reported, the 2025 cause question had 96 answers, and Uptime says outages are under-reported [1].
- The Annual Outage Analysis reports are for subscribers and were not used. The 2026 survey's only public cause figure is power and cooling together [5].
- The incident reviews are their authors' accounts, chosen because they were published. For the Oregon facility, only its customer's account was reviewed [20].
- Cloudflare calls its account of events after the generators started informed speculation, partly from what facility staff told it unofficially [20].
- The Daejeon facts come from press reports, and their system counts differ [28, 29, 30]. The Pangyo cause was disputed [12].
- The redundancy figures are correlations, and the samples for N sites are small [5].
- No source reviewed reports outage rates by Tier level, for colocation against enterprise sites, or for liquid-cooled facilities.
- NERC names neither the data centers nor the state [21]. CME and CyrusOne give no outage length [26, 27].

Sources

1. Uptime Institute Global Data Center Survey 2025. Douglas Donnellan, Andy Lawrence, Daniel Bizo, Owen Rogers and others, Uptime Institute, July 2025, viewed 8 November 2026. https://datacenter.uptimeinstitute.com/rs/711-RIA-145/images/2025.Annual.Survey.Report.pdf

2. Uptime Institute 16th Annual 2026 Global Data Center Survey (press release). Uptime Institute, 28 July 2026, viewed 8 November 2026. https://uptimeinstitute.com/about-ui/press-releases/16th-annual-2026-global-data-center-survey-deployment-of-high-density-racks-rising-fast-operators-face-continued-recruiting-and-retention-pressures

3. Uptime Announces Annual Outage Analysis Report 2026 (press release). Uptime Institute, 13 May 2026, viewed 8 November 2026. https://uptimeinstitute.com/about-ui/press-releases/uptime-announces-annual-outage-analysis-report-2026

4. Uptime Announces Annual Outage Analysis Report 2025 (press release). Uptime Institute, 6 May 2025, viewed 8 November 2026. https://uptimeinstitute.com/about-ui/press-releases/uptime-announces-annual-outage-analysis-report-2025

5. Survey findings link higher redundancy to lower outage risk. Owen Rogers and Douglas Donnellan, Uptime Institute Journal, 14 October 2026, viewed 8 November 2026. https://journal.uptimeinstitute.com/survey-findings-link-higher-redundancy-to-lower-outage-risk/

6. Data center operators will face more grid disturbances. Jacqueline Davis, Lenny Simon, Daniel Bizo and Max Smolaks, Uptime Institute Journal, 28 June 2023, viewed 8 November 2026. https://journal.uptimeinstitute.com/data-center-operators-will-face-more-grid-disturbances/

7. Are utility companies needed for pull-the-plug testing? Douglas Donnellan, Uptime Institute Journal, 20 September 2023, viewed 8 November 2026. https://journal.uptimeinstitute.com/are-utility-companies-needed-for-pull-the-plug-testing/

8. Outages: understanding the human factor. Andy Lawrence, Uptime Institute Journal, 8 June 2022, viewed 8 November 2026. https://journal.uptimeinstitute.com/outages-understanding-the-human-factor/

9. Extreme heat stress-tests European data centers, again. Daniel Bizo, Uptime Institute Journal, 27 July 2022, viewed 8 November 2026. https://journal.uptimeinstitute.com/extreme-heat-stress-tests-european-data-centers-again/

10. Electrical considerations with large AI compute. Daniel Bizo, Uptime Institute Journal, 19 November 2025, viewed 8 November 2026. https://journal.uptimeinstitute.com/electrical-considerations-with-large-ai-compute/

11. IT-agnostic DLC systems: key considerations. Daniel Bizo, Uptime Institute Journal, 29 October 2026, viewed 8 November 2026. https://journal.uptimeinstitute.com/it-agnostic-dlc-systems-key-considerations/

12. Major data center fire highlights criticality of IT services. Max Smolaks and Daniel Bizo, Uptime Institute Journal, 11 January 2023, viewed 8 November 2026. https://journal.uptimeinstitute.com/major-data-center-fire-highlights-criticality-of-it-services/

13. Learning from the OVHcloud data center fire. Andy Lawrence, Uptime Institute Journal, 29 March 2021, viewed 8

November 2026. https://journal.uptimeinstitute.com/learning-from-the-ovhcloud-data-center-fire/

14. Datacenter Fire Frequency. Andy Lawrence, Uptime Institute Journal, 5 April 2021, viewed 8 November 2026. https://journal.uptimeinstitute.com/datacenter-fire-frequency/

15. Summary of the Amazon EC2 Issues in the Asia Pacific (Tokyo) Region (AP-NORTHEAST-1). Amazon Web Services, 25 August 2019, updated 28 August 2019, viewed 8 November 2026. https://aws.amazon.com/message/56489/

16. Summary of the AWS Service Event in the US East Region. Amazon Web Services, 2 July 2012, viewed 8 November 2026. https://aws.amazon.com/message/67457/

17. Post Incident Review (PIR): Services impacted after power/cooling issue, Australia East (Tracking ID VVTQ-J98). Microsoft Azure status history, event of 30 August 2023, viewed 8 November 2026. https://azure.status.microsoft/en-us/status/history/?trackingId=VVTQ-J98

18. Multiple Google Cloud services in the europe-west9-a zone are impacted (incident report). Google Cloud Service Health, full report 23 June 2023, viewed 8 November 2026. https://status.cloud.google.com/incidents/dS9ps52MUnxQfyDGPfkY

19. Multiple Cloud products experiencing elevated error rates, latencies or service unavailability in europe-west2 (incident report). Google Cloud Service Health, full report 29 July 2022, viewed 8 November 2026. https://status.cloud.google.com/incidents/fmEL9i2fArADKawkZAa2

20. Post mortem on the Cloudflare Control Plane and Analytics Outage. Matthew Prince, Cloudflare blog, 4 November 2023, viewed 8 November 2026. https://blog.cloudflare.com/post-mortem-on-cloudflare-control-plane-and-analytics-outage/

21. Incident Review: Considering Simultaneous Voltage-Sensitive Load Reductions. North American Electric Reliability Corporation, 8 January 2025, viewed 8 November 2026. https://www.nerc.com/globalassets/our-work/reports/event-reports/incident_review_large_load_loss.pdf

22. Characteristics and Risks of Emerging Large Loads (white paper). NERC Large Loads Task Force, July 2025, viewed 8 November 2026. https://www.nerc.com/globalassets/who-we-are/standing-committees/rstc/3_doc_white-paper-characteristics-and-risks-of-emerging-large-loads.pdf

23. Level 2 Alert: Large Load Interconnection, Study, Commissioning, and Operations. North American Electric Reliability Corporation, 9 September 2025, viewed 8 November 2026. https://www.nerc.com/globalassets/programs/bpsa/alerts/2025/nerc-alert-level-2--large-loads.pdf

24. Oral reply to Parliamentary Questions on banking services disruption of DBS and Citibank on 14 October 2023. Monetary Authority of Singapore, 6 November 2023, viewed 8 November 2026. https://www.mas.gov.sg/news/parliamentary-replies/2023/oral-reply-to-parliamentary-question-onbanking-services-disruption-of-dbs-and-citibank

25. MAS' Response to Media Queries on DBS Bank and Citibank's Recent Banking Services Disruptions. Monetary Authority of Singapore, 19 October 2023, viewed 8 November 2026. https://www.mas.gov.sg/news/media-releases/2023/mas-response-to-media-queries-on-dbs-bank-and-citibank

26. CME Group Inc. Annual Report on Form 10-K for 2025. U.S. Securities and Exchange Commission, filed 26 February 2026, viewed 8 November 2026. https://www.sec.gov/Archives/edgar/data/1156375/000115637526000009/cme-20251231.htm

27. Cooling issue at data center halts futures trading for CME Group. DatacenterDynamics, 28 November 2025, viewed 8 November 2026. https://www.datacenterdynamics.com/en/news/cooling-issue-at-data-center-halts-futures-trading-for-cme-group/

28. Government struggles to restore services after data center blaze. The Korea Herald, 28 September 2025, viewed 8 November 2026. https://www.koreaherald.com/article/10585032

29. Police investigation reveals auxiliary power remained on during NIRS data center fire. Korea JoongAng Daily, 10 October 2025, viewed 8 November 2026. https://www.koreajoongangdaily.com/korea/police-investigation-reveals-auxiliary-power-remained-on-during-nirs-data-center-fire/12229464

30. Board of Audit and Inspection: "National Information Resources Service Fire Was Man-Made... Unregistered Contractor Used for Illegal Subcontracting". The Asia Business Daily, 7 September 2026, viewed 8 November 2026. https://view.asiae.co.kr/en/article/2026090710145353550

31. Digital Realty Trust, Inc. Annual Report on Form 10-K for 2025. U.S. Securities and Exchange Commission, filed 13 February 2026, viewed 8 November 2026. https://www.sec.gov/Archives/edgar/data/1297996/000110465926015365/dlr-20251231x10k.htm

32. Equinix, Inc. Annual Report on Form 10-K for 2025. U.S. Securities and Exchange Commission, filed 11 February 2026, viewed 8 November 2026. https://www.sec.gov/Archives/edgar/data/1101239/000110123926000032/eqix-20251231.htm

33. CoreWeave, Inc. Annual Report on Form 10-K for 2025. U.S. Securities and Exchange Commission, filed 2 March 2026, viewed 8 November 2026. https://www.sec.gov/Archives/edgar/data/1769628/000176962826000104/crwv-20251231.htm

34. Amazon Compute Service Level Agreement. Amazon Web Services, last updated 25 May 2022, viewed 8 November 2026. https://aws.amazon.com/compute/sla/

About this report

Published by Rillor on 12 November 2026. Superintelligence (SI) tools assist research and drafting, and every figure cites its source. Rillor builds and secures SI systems, supplies the data they learn from and delivers the infrastructure they run on. We apply SI to financial and compute markets.

Cite as: Rillor. What causes data-center outages: surveys and incident reviews. 12 November 2026. https://rillor.com/insights/data-center-outage-causes

Notices

Rillor is not a registered investment adviser or commodity trading advisor and does not provide investment or trading advice. Research, forecasts, data and software described on this site are for research and engineering use. Nothing here is an offer or recommendation to buy or sell any security, commodity interest or digital asset. Past or simulated results do not indicate future results.

Work with Rillor

Send the GPU systems you plan to run, the block size and cooling you need, and the month you need power. Contact us at rillor.com/contact?type=capacity or contact@rillor.com. More on data-center capacity: rillor.com/compute/capacity