INTELLIGENCE UPDATE

Publicly reported outages see increase in deliberate attacks

Rose Weinschenk

27 Mar 2025

Major publicly reported outages in 2024 were longer and, therefore, more impactful than in previous years because of the growing number of ransomware attacks, according to data compiled by Uptime Intelligence. The data also shows an increase in the proportion of outages that were caused deliberately.

The latest data relating to major publicly reported outages (collected annually), supports the pattern seen in Uptime Intelligence analyses since 2022, which show outages are becoming less frequent as a proportion of overall workload. Major outages, however, are becoming more severe.

The impact of deliberate attacks has changed in recent years. They are increasingly likely to lead to an IT outage, rather than just a privacy breach (Uptime Intelligence tracks outages, but not security breaches that do not lead to an outage). Most attacks affect IT systems, rather than OT (operational technology) systems, and no major facility-related cybersecurity breaches are recorded in the data. However, the growth in malicious activity suggests that this is likely in the future.

Tracking outages: the methodology

Uptime Intelligence tracks outages in several ways, including self-reporting, surveys and media monitoring, to an incident database. The combined findings are analyzed in the *Annual outage analysis 2024* report (the 2025 edition of this report will be published in May 2025).

The new data discussed in this report tracks major outages reported publicly by the media and other sources. The data should be interpreted cautiously due to the methodology (the analysis that includes major public outages and excludes minor outages), but it presents a more qualitative insight into outage patterns than the more detailed survey data.

Table 1 shows the number of outage reports Uptime Intelligence collected from publicly available sources over the past nine years. In 2024, Uptime collected details from 119 such outages. Only outages that resulted in significant monetary loss, disruption or reputational damage are included.

Table 1 Publicly reported outages tracked by Uptime Intelligence (2016 to 2024)

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

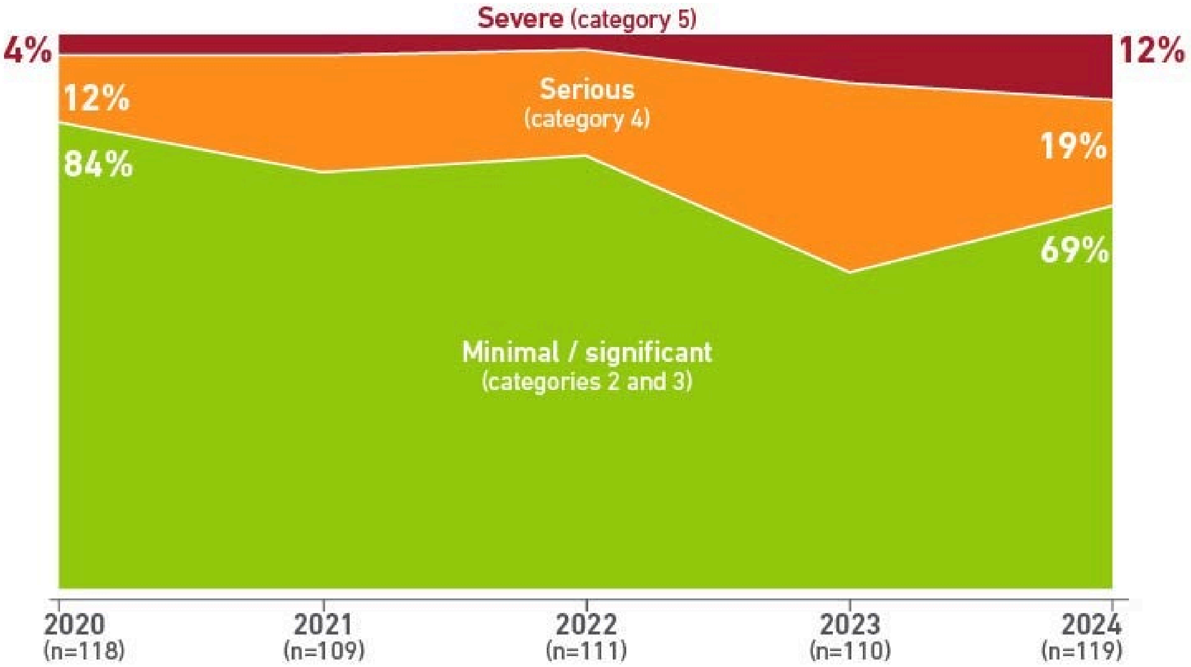
Uptime excludes Category 1 outages (small outages that cause minimal financial and other adverse effects) that have less detailed reporting and are often less accurate. The overall number of outages recorded is not meaningful, reflecting methodologies, media interest and underlying patterns.

UPTIME INSTITUTE 2025

Although numerous factors may influence how outages are reported, it is those outages with a severe impact that inevitably draw media attention. Uptime Intelligence records all outages on a severity scale of 1 (insignificant) to 5 (severe). **Figure 1** shows the proportions of publicly reported outages categorized by severity over the past five years (2019 to 2024). The majority of outages continue to have a minimal or significant impact on the organization and its customers/users, but the proportion classified as severe has increased over the past two years.

There are several reasons for the rise in severe outages: a greater dependency on IT services and interdependence of systems; and increasingly complex systems can be more challenging to diagnose and restore. A new factor is the rise of ransomware attacks, which can lead to prolonged outages as systems are isolated and restored — or while a decision is made on whether to meet the attackers' demands.

Figure 1 Publicly reported outages of categories 2 to 5 severity (2020 to 2024)



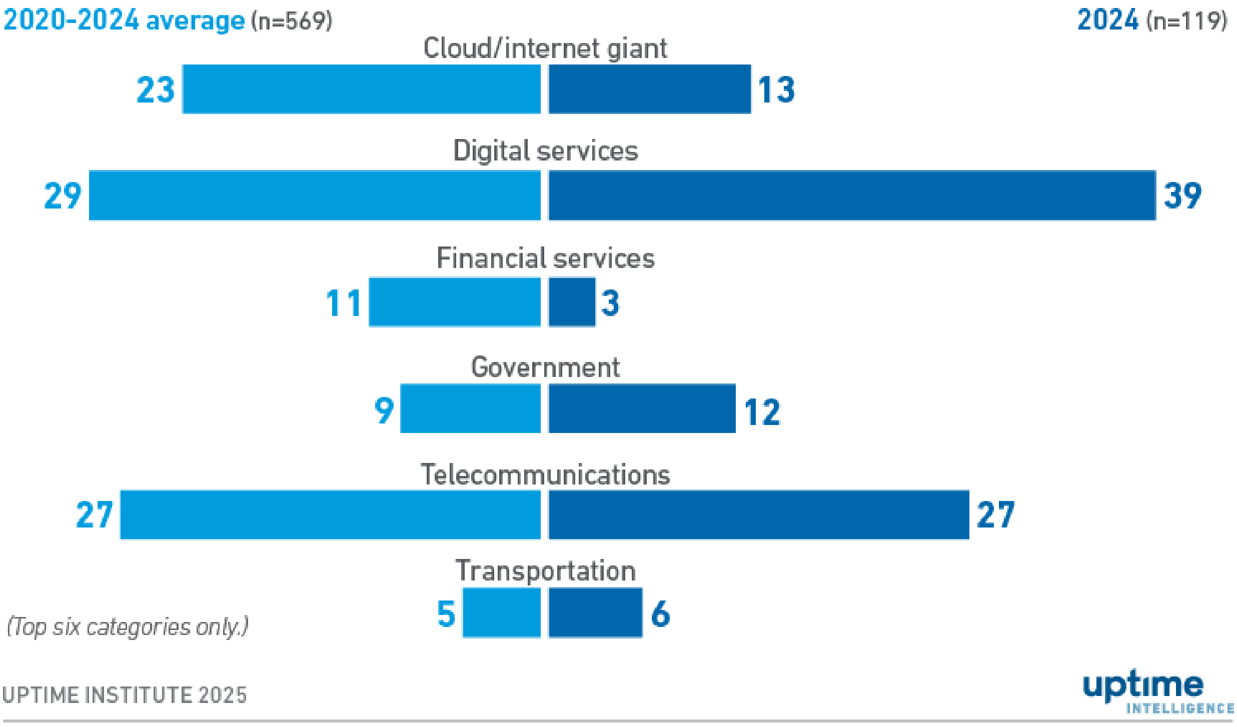
UPTIME INSTITUTE 2025

Digital service outages on the rise

Over the nine-year period that Uptime has been collecting data, an increasing proportion of IT services is dependent on a cloud, colocation provider or other hosted IT service. More outages, unsurprisingly, are now the result of problems in the infrastructure of these professional IT service organizations.

Of the 12 sectors tracked, the top six sectors that have experienced outages are reported in **Figure 2**. Telecommunications, digital services, and cloud/internet giants have the highest average number of major publicly reported outages across the five years, as would be expected given their size and significance. However, there were some key changes in 2024: cloud/internet giant outages fell considerably in 2024, compared with their five-year average. Digital service outages, which include colocation provider outages, rose sharply above their five-year average.

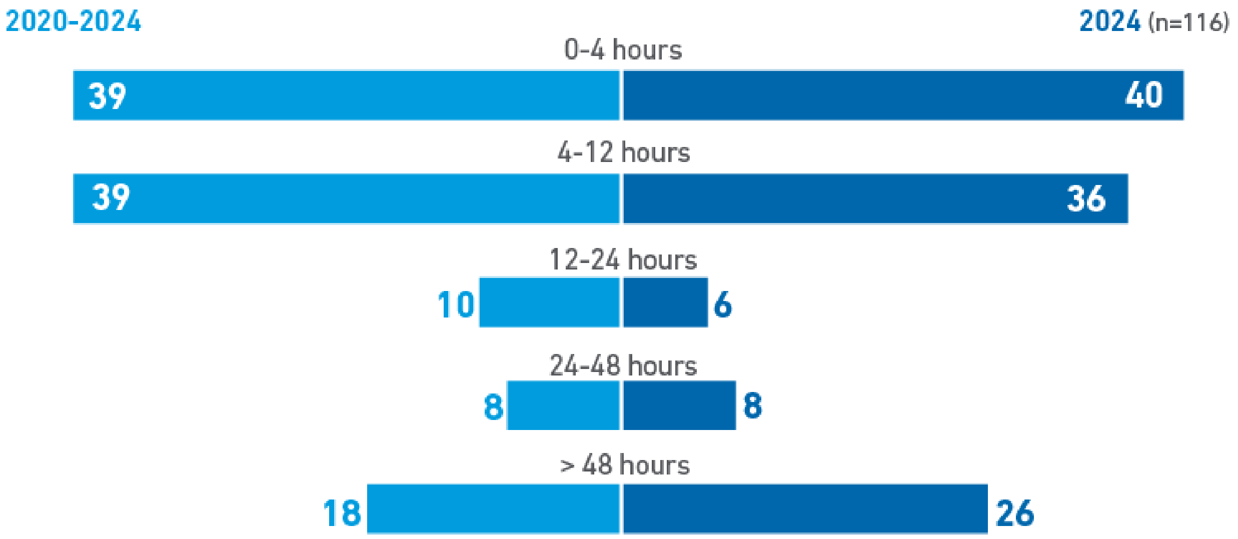
Figure 2 Publicly reported outages of categories 2 to 5 severity by sector (2020 to 2024)



Outage duration increasing

The number of outages in each duration category in 2024 was similar to their five-year averages, with one exception: outage durations of more than 48 hours have increased (**Figure 3**). Analysis of the underlying data suggests that this is mainly because of a higher number of ransomware/cyberattacks and other types of deliberate attacks (such as cable cuts).

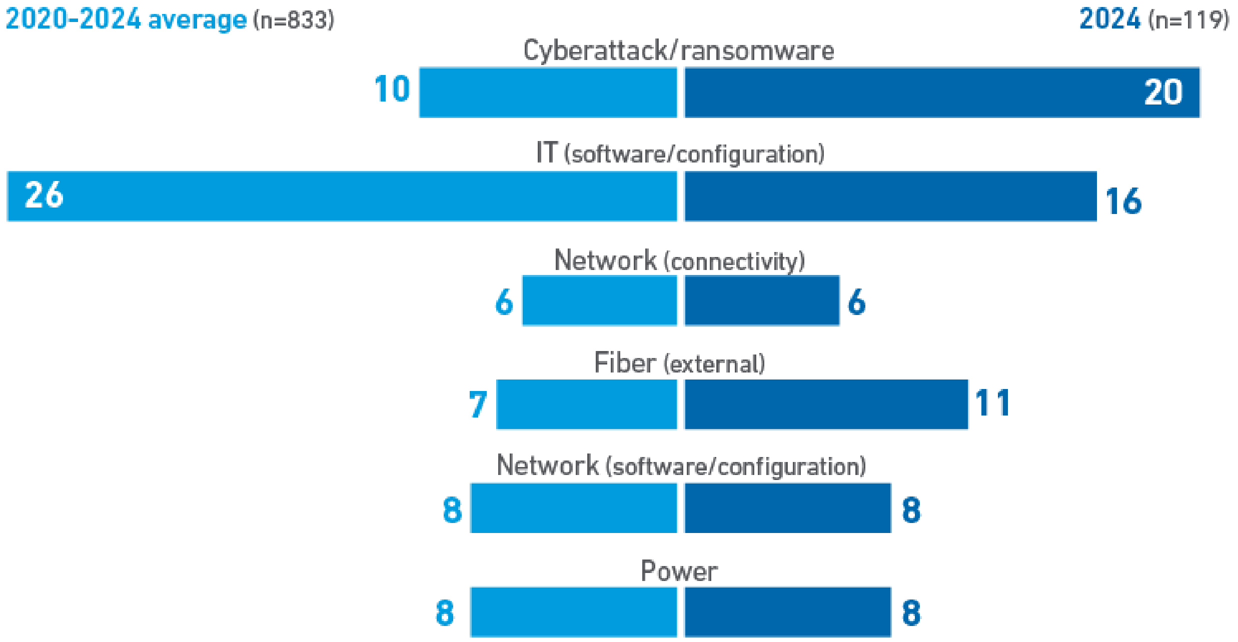
Figure 3 Durations of publicly reported outages with categories 2 to 5 severity (2020 to 2024)



UPTIME INSTITUTE 2025

The number of major outages caused by cyberattacks (from data analyzed by Uptime Intelligence) has almost doubled in the past three years (see **Figure 4**). These outages last longer due to the time-consuming recovery process, which may involve rebuilding systems using clean, uncorrupted data. While the downtime associated with a typical outage, caused by IT software/configuration for example, is slightly more than one day, the average downtime for cyberattacks/ransomware was found to be about 25 days.

Figure 4 Outages with categories 2 to 5 severity by source (2020 to 2024)



UPTIME INSTITUTE 2025

Physical attacks more common

Physical attacks on digital infrastructure are also rising. Not all fiber cuts are deliberate but have become more common compared with previous years. Fiber cuts accounted for 11 major outages in 2024, up from 9 in 2023. External fiber breaks/cuts was also the second most likely category to have an outage lasting over 48 hours (after cyberattacks). Deliberate fiber cuts require planning, expertise and resources, yet a clear financial reward is not always apparent, suggesting that the motivation may be political or ideological.

In 2024, all proven incidents of physical vandalism (aside from cyberattacks) were split between fiber cuts and copper wire theft, and most of these incidents resulted in more than 48 hours of downtime. The number of vandalism incidents (not including cyberattacks) has tripled since 2023, increasing from 1.8% to 5% of all incidents. Deliberate attacks and cyberattacks combined caused 50% of all outages lasting more than 48 hours.

Uptime Intelligence View

While owners and operators need to continue planning resiliency around infrastructure failures, resiliency measures should place more emphasis on the prevention of deliberate attacks.

Cyberattacks have become more widespread and complex to resolve as critical infrastructure directly impacting day-to-day life becomes increasingly digitized. Since a surge in cybercrime during the pandemic, cybercriminals have become more organized and technologically advanced.

ABOUT THE AUTHOR

Rose Weinschenk

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

RWeinschenk@uptimeinstitute.com

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.