Uptime Institute | INTELLIGENCE

RISK & RESILIENCY

# The pandemic's impact on digital infrastructure

## July 2021 update

**Andy Lawrence,** Executive Director of Research, Uptime Institute

**The pandemic has accelerated some long-term trends toward greater use of digital services, remote working and remote operation. Overall, costs have been pushed up, but other impacts are less clear — some are even counter-intuitive. Many uncertainties remain.**

## CONTENTS

In our August 2020 report, **Post-pandemic data centers**, Uptime Institute Intelligence identified three phases of the COVID-19 pandemic as it applied to the operation of critical digital infrastructure:

- **Phase 1: Reaction** — An emergency response phase involving the purchase of personal protection equipment, increased sanitation efforts and enhanced staff/resource management.
- **Phase 2: Mitigation** — A phase in which new methods of operation are developed while the pandemic itself continues to require extra measures or causes sudden changes in status or major disruption.
- **Phase 3: Adaptation** — A post-pandemic phase where a "new normal" is established.

Uptime Institute's most recent research, based on work in five continents, suggests that much of the world is now in a hybrid state between Phase 2 (Mitigation) and Phase 3 (Adaptation) — and it may remain so for some time.

This means that many managers are undecided on how to proceed in several key areas. It also reflects society at large in many regions, and so is to be expected. Not only is the course of the pandemic unpredictable and uneven, but new variants of the coronavirus may elicit new questions and, as can research findings, sometimes prompt new government responses and medical advice.

In several countries, vaccine and testing capabilities have progressed rapidly and ahead

15-30 MINUTES TO READ

of expectations. But the global scale of the challenge means that post-vaccine normality — full Phase 3 — cannot be expected before 2022. Moreover, adaptation, as we discussed in our 2020 report, does not necessarily mean stability: new variants and new outbreaks will prompt responses, such as lockdowns and border closures, that can affect staff movements and supply chains.

**Continuing complexity**

Political and legal complexities add to the continuing uncertainty. Cross-border travel, which particularly affects support staff and third-party suppliers, remains difficult, and policies are not necessarily driven by epidemiological evidence. Insurance liabilities are unclear and legal guidance, particularly relating to staff and their medical issues, can vary by time and country. In short, the new normal is not yet normal by pre-pandemic standards — and it may not be for some time.

Some certainties, however, have emerged. First, operators of critical infrastructure are spending more to ensure resiliency and effective operation — partly to offset the threat of restricted or reduced staff availability in the future (see The pandemic has driven up operational costs).

Second, a long-term trend toward digital services and remote working or remote operation has been irreversibly accelerated. There is a surge in demand for data center services and an increased level of dependency on digital services.

Managers and investors are responding to all these factors by investing more in critical infrastructure — even in private enterprise-owned data centers, where capital investment has been suppressed in recent years.

*Note:* Uptime Institute has tracked the impact of COVID-19 in some depth. Most of our research is freely available in the form of recorded webinars and reports. The findings in this report are based partly on a global survey of data center operators, owners and managers conducted in the spring of 2021.

# Site policies are loose but will tighten

How should data center operators control access to their sites, now that cross-infection has become a persistent concern? Is it acceptable to insist that staff are vaccinated? Or that visitors are? Will testing, at least, become the norm?

Legal experts and human resources managers have found this area to be rife with difficulty. While the situation varies from country to country, there is often a general understanding that employee medical information is confidential. Employers who insist their staff be vaccinated, or who insist on knowing why an employee does not want to be vaccinated, could be open to lawsuits under employment, privacy or human rights laws. For this reason — coupled with the limited availability of vaccines in many countries — most data center companies, and their suppliers, are delaying making fixed policy decisions.

Uptime Intelligence research confirms that operators are taking a cautious approach. Only a tiny percentage (2% to 4%) of data center operators recently surveyed (globally) insist that staff or visitors are vaccinated. The rest seek a middle way, treating unvaccinated staff as an infection risk, not asking at all, or having no clear policy (see Figure 1). We think this may represent a relaxation from the earlier stage of the pandemic, when health questionnaires and tests were more rigorously applied.

The pragmatic approach will change over time, as the picture becomes clearer and commercial pressures build. By the end of 2021, when many more people will have had the opportunity to be vaccinated, the proportion of data center operators surveyed who say they will insist that staff are vaccinated jumps to almost 10%, and yet more will insist that visitors are vaccinated. The great majority of operators expect to have clear policies on vaccines and testing.

Over time, human resources experts and legal professionals think the balance will most likely tilt toward greater disclosure of medical information and, in turn, an increased requirement for staff and visitors to be vaccinated. This will be most easily applied to new employees.

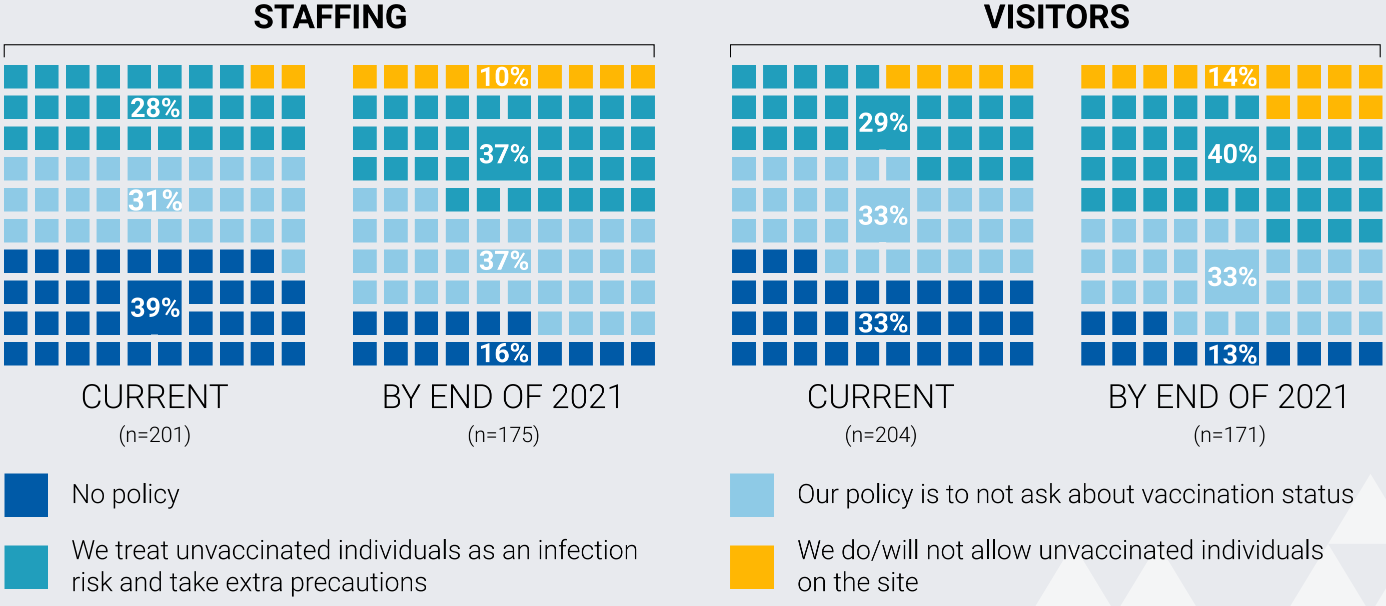
Employers are certainly under pressure to have their staff tested and/or vaccinated — especially if they travel to other sites. This may be because medical insurance requires vaccination (or even exempts COVID-19 as a covered condition); because customers demand that any visitors are vaccinated; or because of the legal exposure if an infected employee passes the virus to a partner/customer or fails to disclose information. During the pandemic, employees of services companies have caught COVID-19 while visiting data centers and, equally, some have tested positive while visiting sites.

FIGURE 1

## Vaccination and visitor policies vary

What is your organization's current policy on allowing unvaccinated individuals data center access? What do you think it will be by the end of 2021?

(TOP RESPONSES ONLY)



Uptime Institute | INTELLIGENCE

SOURCE: UPTIME INSTITUTE COVID-19 IMPACT GLOBAL SURVEY 2021

# It's official: Data center workers are critical

During the early stages of the pandemic in 2020, countries scrambled to decide which workers were "key" or "critical" and, therefore, exempt from some lockdown restrictions or eligible for free or easily available tests. The initial picture was confused. Different countries have different ways of defining what "critical infrastructure" means and different ways of applying exemptions. Data center staff sometimes fell into a gray area.

The situation now is more clear. In most countries, or states, those jobs that have key worker status are well defined, and this usually includes anyone involved in managing and maintaining mission-critical infrastructure — which includes digital infrastructure. Processes for confirming key worker status, sometimes through trade bodies or employer letters, are also established.

But complications and uncertainties remain. First, there are still rules and categories that may apply in certain situations and be applied differently from country to country. There are differences between, for example, health workers and other key workers; this may determine access to vaccines and travel. And second, there may still be differences between a critical infrastructure worker at a named power plant (for example) and a private enterprise-owned data center. The former site may be formally listed as part of the national critical infrastructure and all support workers, even international, may be allowed access.

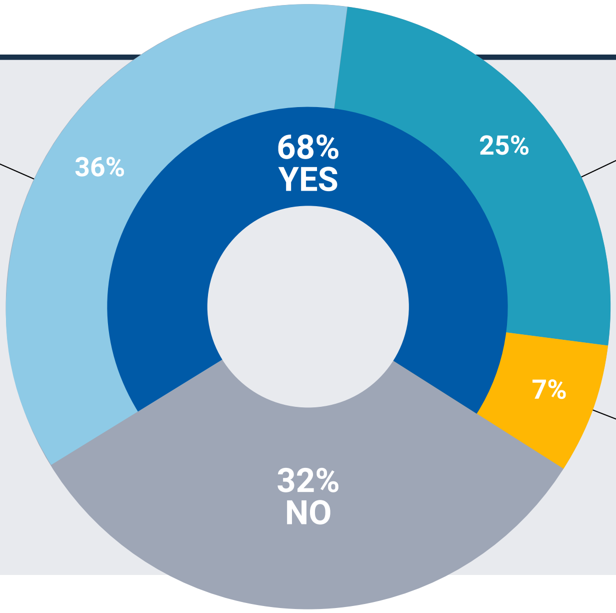
> "The new normal is not yet normal by pre-pandemic standards — and it may not be for some time."

Cross-border travel may mean further restrictions apply, from which data center staff may not be exempt. The US, for example, may not allow noncitizens entry unless it can be shown it is in the US national interest. More usually, there may be a requirement to show proof of vaccination, COVID-free status, details of critical work, or to self-isolate upon arrival or return. This is creating considerable uncertainty and making cross-border support work extremely difficult. It is affecting some maintenance services and forcing a supply chain re-think (see Figure 2).

FIGURE 2

**Most have experienced disruptions due to COVID-related travel restrictions**

Between early 2020 and the present, have you suffered any disruptions or delays caused by workers or visitors being unable to travel to your site due to travel/lockdown restrictions?



Uptime Institute | INTELLIGENCE
SOURCE: UPTIME INSTITUTE COVID-19 IMPACT GLOBAL SURVEY 2021 (n=194)

# The COVID outage paradox

In the 12 months from early March 2020 to April 2021, COVID-19 made a big impact on how and where IT was used. This had a surprising — and in some ways paradoxical — impact on IT service availability and the number and severity of outages recorded.

At the beginning of the pandemic, data center managers were bracing themselves. Scheduled maintenance was often postponed, again and again. Critical equipment was caught up in supply chain delays. Staff shifts needed to be split into teams that must never meet; many staff members fell ill or were forced to isolate. A jump in outages seemed inevitable.

### Outages were infrequent

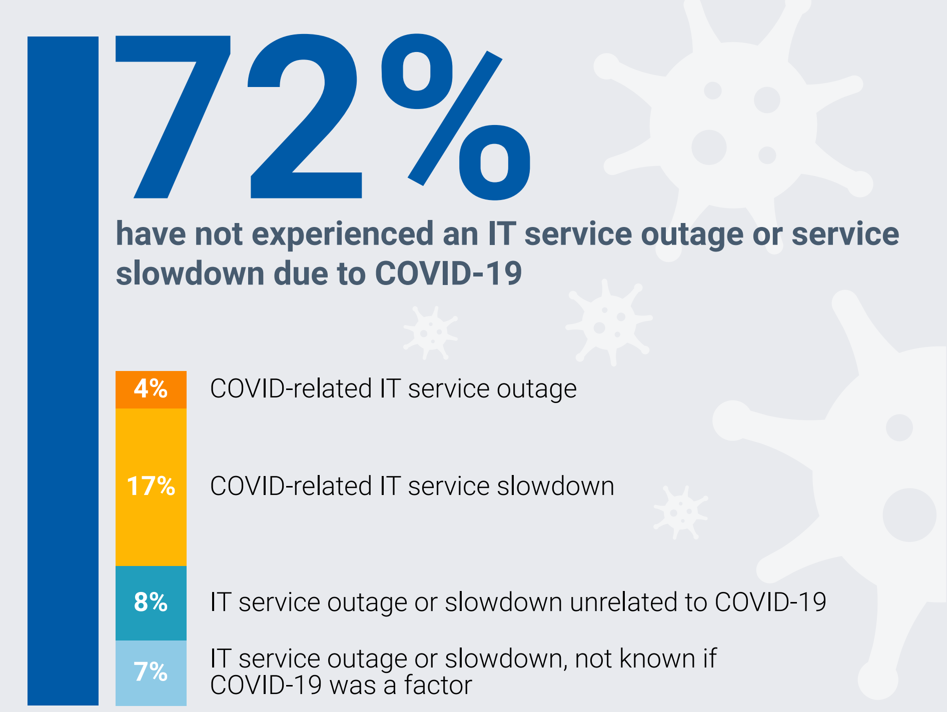
This did not materialize, however. In three separate surveys conducted by Uptime Institute during the period, operators reported relatively low numbers of outages attributable to COVID. In the latest research, covering the 12-month period to April 2021, only around 4% recorded a COVID-related outage (see Figure 3). Overall, the level of outages recorded was around the same as in most years (according to Uptime Institute data) or lower. There was a slight increase if COVID-related service slowdowns were included, but these are likely to have included network-related congestion or other issues on the public internet.

These findings match Uptime Institute's analysis of publicly recorded outages for 2020, which shows a marked drop in the number of major outages reported.

Why is this? There are two factors at play: First, 2020 was the year in which the COVID-19 outbreak caused a lot of businesses to reduce/suspend commercial operations (although, of course, a lot moved online). This depressed some business activity, meaning fewer outages and reduced disruption in some areas (the transportation sector, for example, usually accounts for a small but significant number of serious failures each year). Also, many service interruptions occur during maintenance, upgrades and transition — but in 2020, much of this was delayed.

FIGURE 3

Few have experienced COVID-related service interruptions



UptimeInstitute® | INTELLIGENCE
SOURCE: UPTIME INSTITUTE COVID-19 IMPACT GLOBAL SURVEY 2021 (n=206)

A second reason is that the pandemic shifted a lot of business activity onto internet-based collaboration tools. While manufacturing, transport, retail and other systems were doing less business and suffered fewer major issues, outages of services such as Zoom, Teams and Facebook made headlines. These disruptions were less marked because of the less-critical nature of the service and the distributed, cloud-based architecture on which they are based. This tended to result in fewer binary outages — that is, slowdowns and interruptions rather than complete failures.

## The pandemic has driven up operational costs

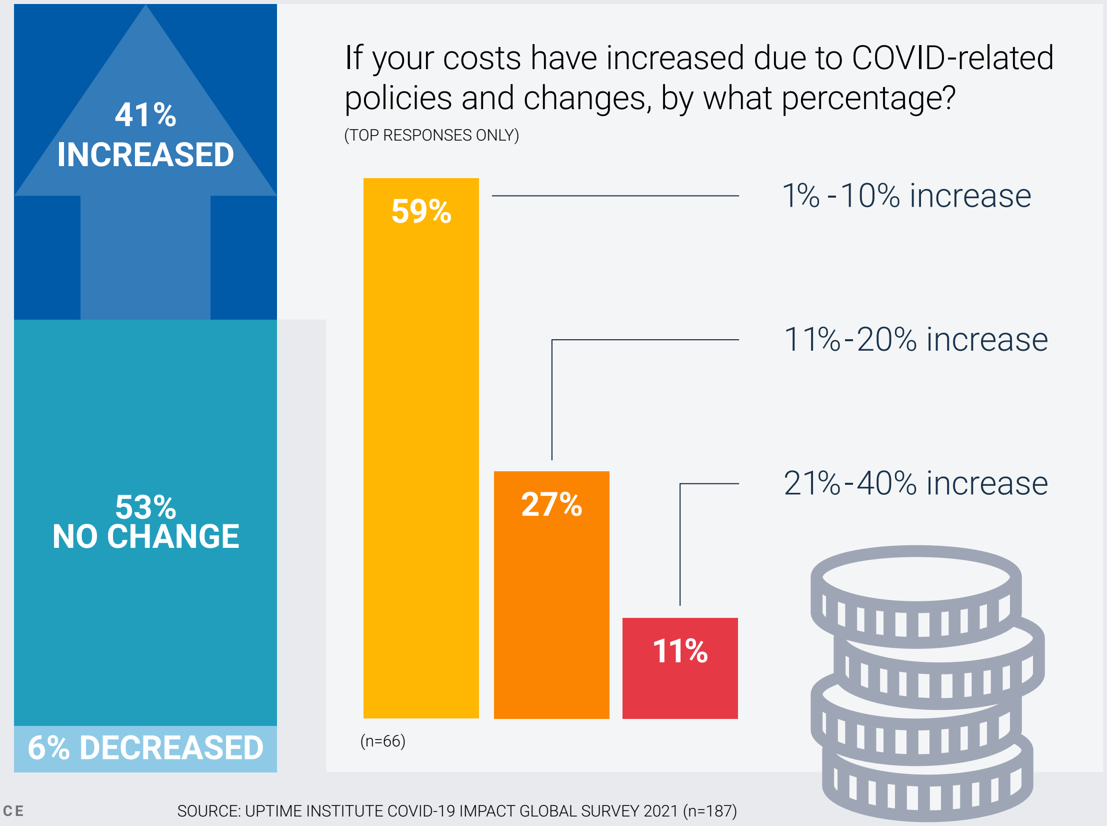
As the pandemic began to make an impact in early 2020, it became clear that data center operators were going to have to spend more if they were to provide the services on which their customers were increasingly reliant. Short-term needs included protective equipment, deep cleaning and, it seemed likely, more spending to support extended shifts and more support staff. Initially, this increase appeared temporary — but the evidence now suggests it may be more enduring, if not permanent.

One important area where spending was expected to increase was remote

FIGURE 4

**For many, COVID-19 has increased data center costs**

In the period from early 2020 to the present, do you think the cost of your monthly data center operations has increased, decreased, or remained the same as a result of your organization's COVID-related policies and changes?



If your costs have increased due to COVID-related policies and changes, by what percentage?

(TOP RESPONSES ONLY)

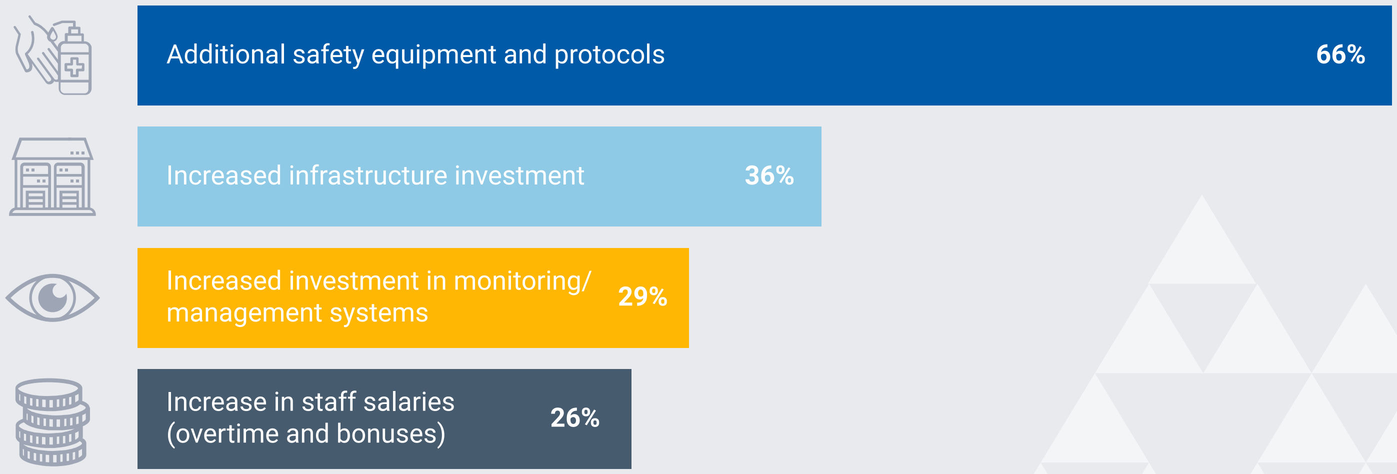
SOURCE: UPTIME INSTITUTE COVID-19 IMPACT GLOBAL SURVEY 2021 (n=187)

FIGURE 5

## Cost increases due to COVID: Where the money is being spent

Which of the following has contributed to the increase in data center operations costs as a result of your COVID-related policies and changes? (Choose all that apply)

(TOP RESPONSES ONLY)



UptimeInstitute® | INTELLIGENCE

SOURCE: UPTIME INSTITUTE COVID-19 IMPACT GLOBAL SURVEY 2021 (n=70)

monitoring and automation, which would enable data centers to be operated with fewer people on-site.

In a global Uptime Intelligence survey in July 2020, 90% of operators said they would increase their use of remote monitoring as a result of the pandemic, and 73% said they would increase their use of automation. Many also expected to spend more on infrastructure and resiliency as a direct result of the pandemic.

Expectations often do not translate into action. However, in our most recent survey there is some evidence that spending on infrastructure, monitoring and staff have increased because of the pandemic (see Figure 4 ). About four in 10 (41%) operators surveyed say spending has risen as a result of the pandemic, and only one in 20 (6%) say it has fallen. Most say spending rose by less than 20%, although a few outliers saw much bigger increases.

> "There is justifiable concern that future pandemics will require the same or greater levels of isolation by staff."

Our data suggests that while the pandemic may subside in many countries during 2021 and 2022, the spending increase is likely to be sustained. Spending on protective equipment and extra staff may fall back, but capital technology investments, whether in increased automation/monitoring or site resiliency, may take years to peak and then require ongoing operational support (see Figure 5).

Asked about future spending, about a third (35%) expect spending to increase in the next two years, compared with less than one in 10 (8%) who think it will drop. The increase is expected to parallel current trends, with around 45% thinking the rise will be less than 10% and a similar number expecting it will be between 10% and 20%.

These increases, coming year on year, are not insignificant and are on top of an overall increase in new data center/digital infrastructure investment. As a result, data centers should be more resilient in the years ahead, and perhaps a little less susceptible to problems with a critical component — humans. But operational costs are unlikely to fall.

## Remote tools are becoming essential

The remote management of IT and networks and automated provisioning have been cornerstones of cloud computing. Despite that, suppliers of remote data center monitoring and analysis have had to argue hard for their value proposition, often without results. Adoption of data center infrastructure management (DCIM) software tools has risen only slowly, over a period of two decades.

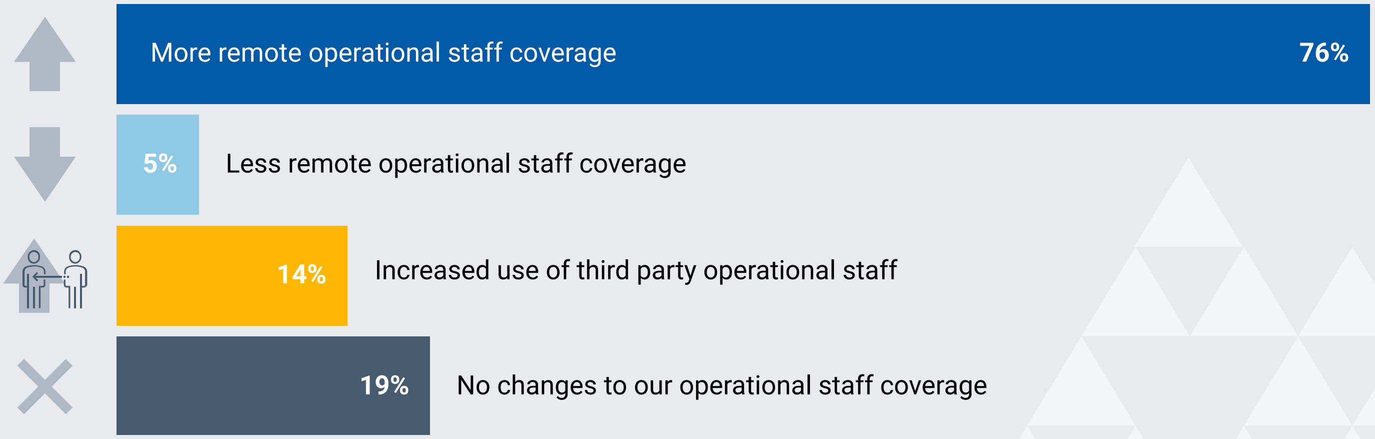
The pandemic looks to have decisively changed that. As with most other businesses, many data center staff who were not needed on-site were encouraged, or forced, to work from home or at an isolated location (see Figure 6). Many have not returned.

This shift to more remote working means that more management/monitoring tools are needed — four of five data center operators say they have already increased their investment in this area — confirming

FIGURE 6

**Remote staff coverage has increased for most**

How has your operational staff coverage transformed over the course of the COVID-19 pandemic? (Choose all that apply)



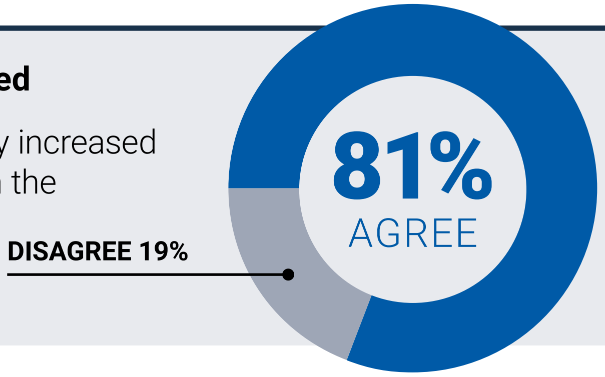
Uptime Institute | INTELLIGENCE

SOURCE: UPTIME INSTITUTE COVID-19 IMPACT GLOBAL SURVEY 2021 (n=177)

FIGURE 7

**Remote monitoring/management use has increased**

Because of the COVID-19 pandemic, we have already increased our use of remote monitoring/management or are in the process of doing so.



UptimeInstitute® | INTELLIGENCE

SOURCE: UPTIME INSTITUTE COVID-19 IMPACT GLOBAL SURVEY 2021 (n=188)

that planned expenditure is already happening (Figure 7).

It is not just COVID-19 that is driving uptake of management and monitoring software. There is justifiable concern that future pandemics will require the same or greater levels of isolation by staff. Remote management software, and even automation, are seen as critical tools for enabling continued operation. Growing concerns about extreme weather events (more common/severe due to climate change) are also driving investment.

"Two-thirds of organizations surveyed say they have increased investment in their infrastructure."

Digitization and greater use of telemetry are often precursors to greater levels of automation. This is likely to be the case in the data center, especially as artificial intelligence capabilities improve and proliferate.

Nearly two-thirds of operators surveyed say that, in 2021, they have either already increased the automation of their facilities or are planning to do so. This will likely lead to greater spending in the short and medium term but may enable staff reductions or redeployment in the long term.

# Operators shore up supply chains

In recent decades, most industries have become globalized — and some more than others. The mission-critical data center industry is heavily dependent on components shipped from across the world, some of which (such as microchips) may be produced in only one or two regions.

Most data centers do not have dual sourcing or local sourcing policies, which means that the unavailability of, for example, a chip made in Taiwan, or a heat-exchanger made in Germany, can threaten continued operations.

"[The pandemic prompted] many operators to re-examine their dependencies on previously reliable but ultimately fragile supply chains."

The pandemic is one of three of the biggest recognized threats to the supply chain — the others being political instability or trade disputes and increased frequency/severity of extreme weather due to climate change.

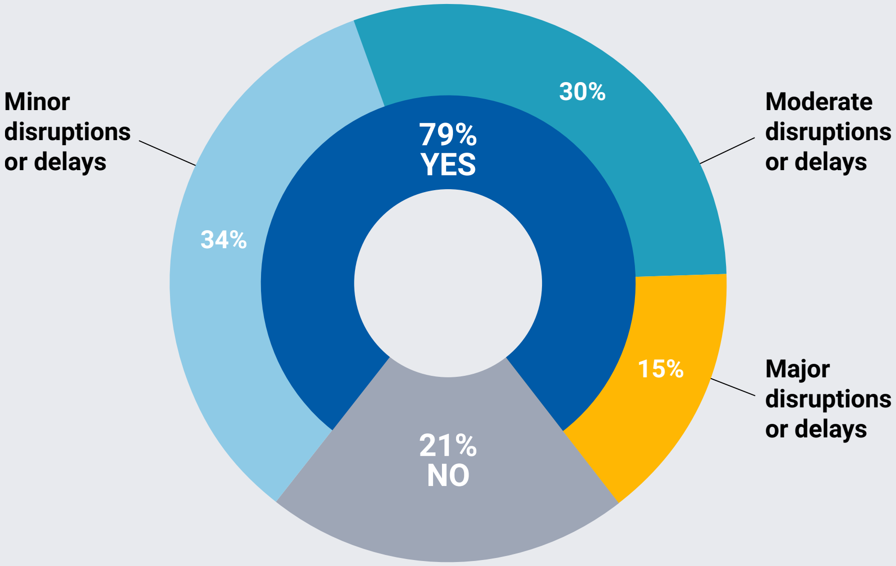
In 2020, the pandemic was the biggest threat for most data centers, prompting many operators to re-examine their dependencies on previously reliable but ultimately fragile supply chains. As Figure 8 shows, nearly half of all data center operators surveyed reported moderate or major disruption to the supply of parts and materials due to COVID during the 12 months leading up to April 2021.

The response to these threats is to move away from the more efficient approach of just-in-time delivery of parts and services, to the more expensive and more cumbersome just-in-case approach. The latter approach means holding bigger inventories of parts on-site and adding extra, and especially local, suppliers (Figure 9).

FIGURE 8

**Most have suffered supply-chain disruptions due to COVID-19**

Between early 2020 and the present, have you suffered any disruptions or delays to the supply of parts or materials due to COVID-19?

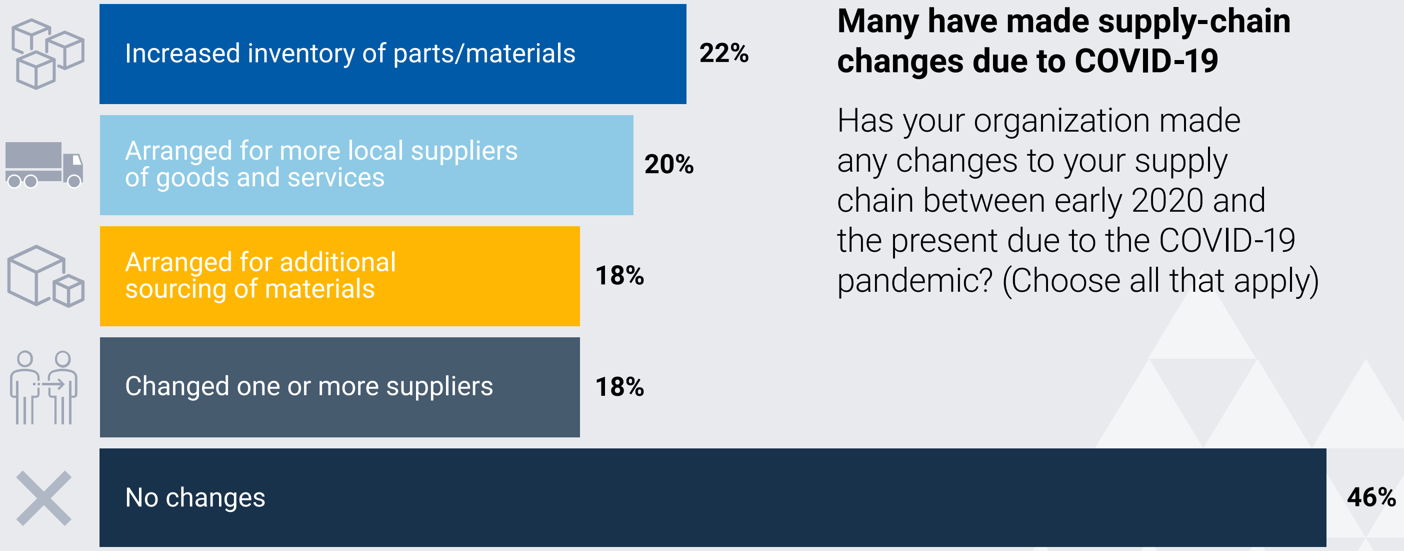


SOURCE: UPTIME INSTITUTE COVID-19 IMPACT GLOBAL SURVEY 2021 (n=192)

FIGURE 9

**Many have made supply-chain changes due to COVID-19**

Has your organization made any changes to your supply chain between early 2020 and the present due to the COVID-19 pandemic? (Choose all that apply)



SOURCE: UPTIME INSTITUTE COVID-19 IMPACT GLOBAL SURVEY 2021 (n=192)

# Other impacts and summary

All major, seismic events have a long-lasting legacy (it is said the bubonic plague in the 14th and 15th centuries triggered the Renaissance). The COVID-19 pandemic has accelerated the adoption of digital, internet-based services and underlined the need for end-to-end resiliency.

Another long-term and serious global challenge — climate change — is having (and will increasingly have) a similar impact: Both extreme weather and the need to reduce the transportation of people and goods are driving demand for more virtual services and greater resiliency of the digital infrastructure they rely on.

As discussed in our detailed 2020 report, **Post-pandemic data centers**, there has been a surge in demand for cloud-based services — already a very strong trend. More than six in 10 organizations recently surveyed say they have accelerated or increased their adoption of cloud services as a result of the pandemic.

> "More than six in 10 organizations recently surveyed say they have accelerated or increased their adoption of cloud services as a result of the pandemic."

However, this is part of a wider picture. Our research indicates that many have also invested more in their digital infrastructure recently — both in automation and in resiliency generally (two-thirds of organizations surveyed say they have increased investment in their infrastructure).

All these developments — impacts on staffing and resources, supply chain changes, use of remote management, automation and cloud — can be classified as risk-reduction strategies.

Clearly, most management teams have grasped that while the threat from COVID-19 is being controlled in many geographies, the level and number of risks from other sources will be ever-present. As a result, the risk-averse, highly prepared mission-critical digital infrastructure industry is in the process of becoming better prepared for whatever may come next.

# ABOUT THE AUTHOR

**Andy Lawrence** is Executive Director of Research at Uptime Institute and a founding member of Uptime Institute Intelligence. Mr. Lawrence has spent three decades analyzing developments in IT, emerging technologies, data centers and infrastructure; and advising companies on their technical and business strategies. **Contact:** alawrence@uptimeinstitute.com

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.**

## ABOUT UPTIME INSTITUTE

Uptime Institute is an advisory organization focused on improving the performance, efficiency and reliability of business critical infrastructure through innovation, collaboration and independent certifications. Uptime Institute serves all stakeholders responsible for IT service availability through industry leading standards, education, peer-to-peer networking, consulting and award programs delivered to enterprise organizations and third-party operators, manufacturers and providers.

Uptime Institute is recognized globally for the creation and administration of the Tier Standards and Certifications for Data Center Design, Construction and Operations, along with its Management & Operations (M&O) Stamp of Approval, FORCSS® methodology and Efficient IT Stamp of Approval.

Uptime Institute – The Global Data Center Authority®, a division of The 451 Group, has office locations in the US, Mexico, Costa Rica, Brazil, UK, Spain, UAE, Russia, Taiwan, Singapore and Malaysia. Visit uptimeinstitute.com for more information.

**All general queries:**
Uptime Institute
5470 Shilshole Avenue NW, Suite 500
Seattle, WA 98107 USA
+1 206 783 0510
info@uptimeinstitute.com