Uptime Institute® INTELLIGENCE

RISK & RESILIENCY

UI Intelligence report 39

Post-pandemic data centers

Author
Andy Lawrence, Executive Director of Research, Uptime Institute

The COVID-19 pandemic will bring some long-term strategic changes to the management and day-to-day operations of data centers and mission-critical infrastructure services. The goal? To become more resilient to any future pandemics.

UII-39 v1.0 published August 6, 2020 last updated August 6, 2020

This Uptime Institute Intelligence report includes:

ABOUT UPTIME INSTITUTE INTELLIGENCE

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 intel@uptimeinstitute.com.

KEY FINDINGS

- A majority of data center owners and operators are planning to make their data centers more resilient, in readiness for the next pandemic.
- As with all industries, most data center owners and operators expect more remote working and plan to operate with fewer on-site workers.
- The pandemic will not drive a big shift to either public cloud or the edge, but it will likely help accelerate pre-existing trends.
- There will be a wave of investment in remote monitoring/management and automation, creating a surge of opportunities for vendors.
- Governments, regulators and IT clients will increasingly seek reassurance that data centers are designed and operated to maintain availability throughout any future pandemics.

Introduction

The COVID-19 pandemic will leave a lasting mark on the world and on most industries and businesses. Working patterns and behaviors may change forever, and with this, the infrastructure that supports them. Whole sectors appear to be shifting to remote working and delivery. Some companies have already announced permanent changes to their business model; some big planned investments, such as offices and airports, may never be made; governments have changed laws and increased powers. Suppliers in many industries are anticipating a wave of investment to facilitate remote working and reduce human on-site involvement.

The impacts on the data center industry look to be largely benign, but even so, there will be long-term changes. This report focuses on the following questions: What will be the long-lasting impact of the COVID-19 pandemic on the digital critical infrastructure industry? How, if at all, will the COVID-19 pandemic change the way data centers are built and operated?

In this report, we discuss over a dozen possible areas of impact. Some of the changes discussed were happening anyway, others represent a significant or accelerated shift. As ever, forward-looking predictions are never easy. The scale and pace of some changes may be contingent on unknowns outside the sector's sphere of influence. Although some practices will tail away over time, in this report we have attempted to identify lasting changes.

One question we did not consider is whether COVID-19 will drive up overall demand for data center capacity. This is a macroeconomic question, since even very strong industries will be slowed by deep recessions. At present, there are signs that the strong growth phase will continue.

There is an important assumption running through our analysis and, we believe, in the planning of most operators: COVID-19 will almost certainly not be the last pandemic — and it may only be one of many. Operators, therefore, are not making all these changes in response to COVID-19, but in anticipation of future pandemics. Therefore, this report is not about COVID-19 response, per se, but about changes being made in anticipation of future situations.

In recent months, 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 (see the **Appendix** for more information). Our findings in this report are based in part on a survey (The long-term impact of COVID-19 on data centers) conducted in July 2020, of over 300 data center operators, owners and managers. Further details on the survey are provided in the **Appendix**.

The impact life cycle

Uptime Institute has classed the responses in the data center industry to the COVID-19 pandemic into three present and future phases.

Phase 1: Reaction

The first phase might be termed ***reaction***. Operators were put on high alert, in emergency response mode. The biggest concerns were to understand the threats, the science and evidence; to identify and immediately implement responses; and to adopt best practices. The first priorities were to decrease the risk to staff and to maintain availability; to source appropriate personal protective equipment and decontaminants; to clean facilities; to re-organize project work and maintenance schedules to accommodate reduced staffing levels; and to overcome possible supply chain disruption.

For most, this phase lasted a few weeks to months and has already passed. While the vast majority came through this well, the suddenness of the crisis did lead to some outages (about one in 20 data centers had a pandemic-related outage). Others said they experienced IT service slowdowns — most likely due to changing demand patterns or server/network maintenance problems. Figure 1 shows the range of impacts data center operators experienced in the first months of the pandemic.

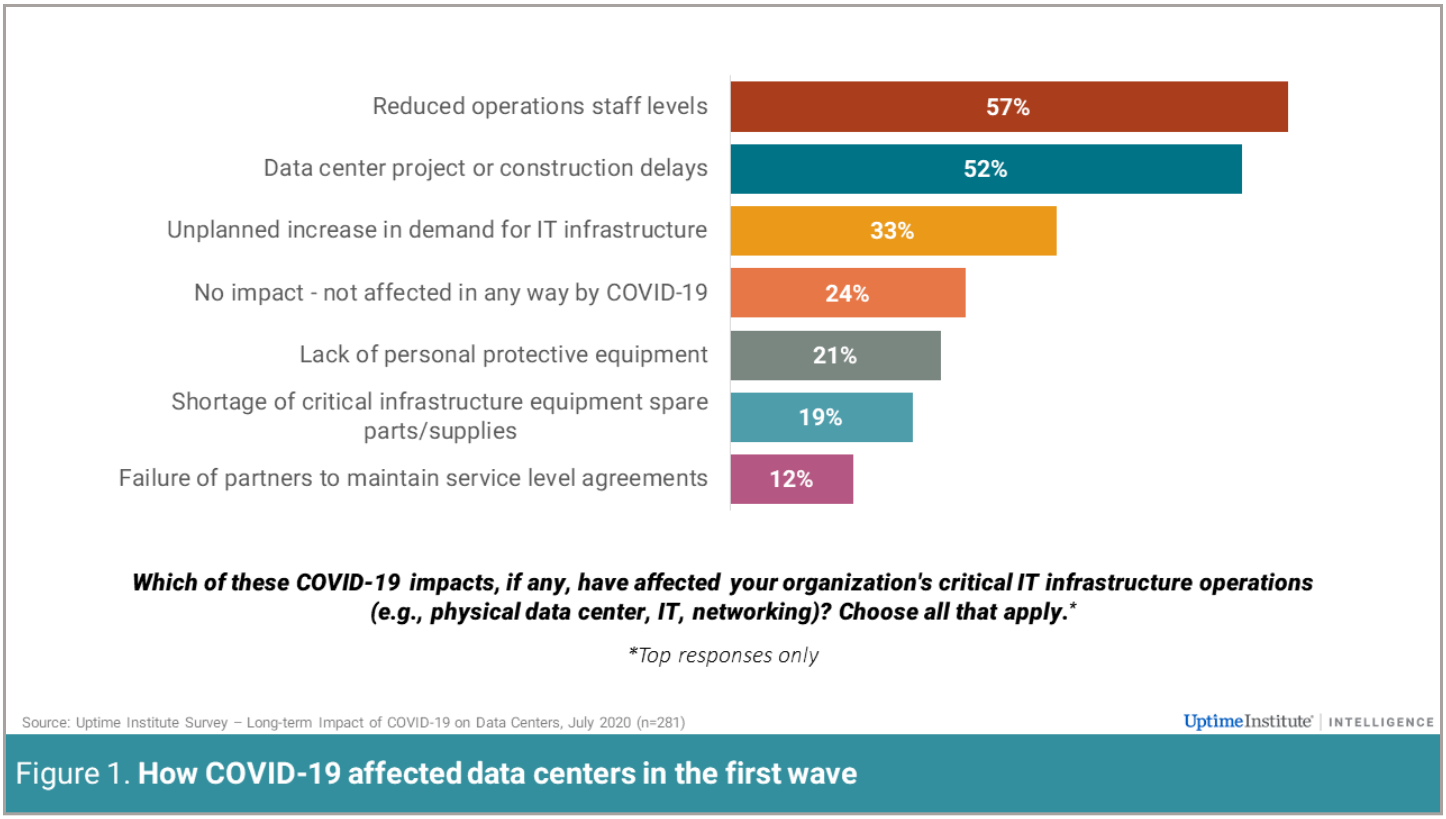


Figure 1. **How COVID-19 affected data centers in the first wave**

Phase 2: Mitigation

The second phase, ***mitigation***, is an interim "normal." At the time of writing — mid-2020 — most data center operators are in this period (which may last up to two years). The virus is still widespread, but the immediate threat to data center operations and service availability has been reduced. This may be due to overall virus containment or because new processes mitigate the risk to infrastructure.

In this phase, the processes that were established in the reactive phase have become established — these include more remote working, blue/red operations teams, reduced maintenance, and some adjustments/innovations in the supply chain. Most of these are process-based and do not involve long-term investments or strategic changes. Some examples of these activities are presented in Figure 2.

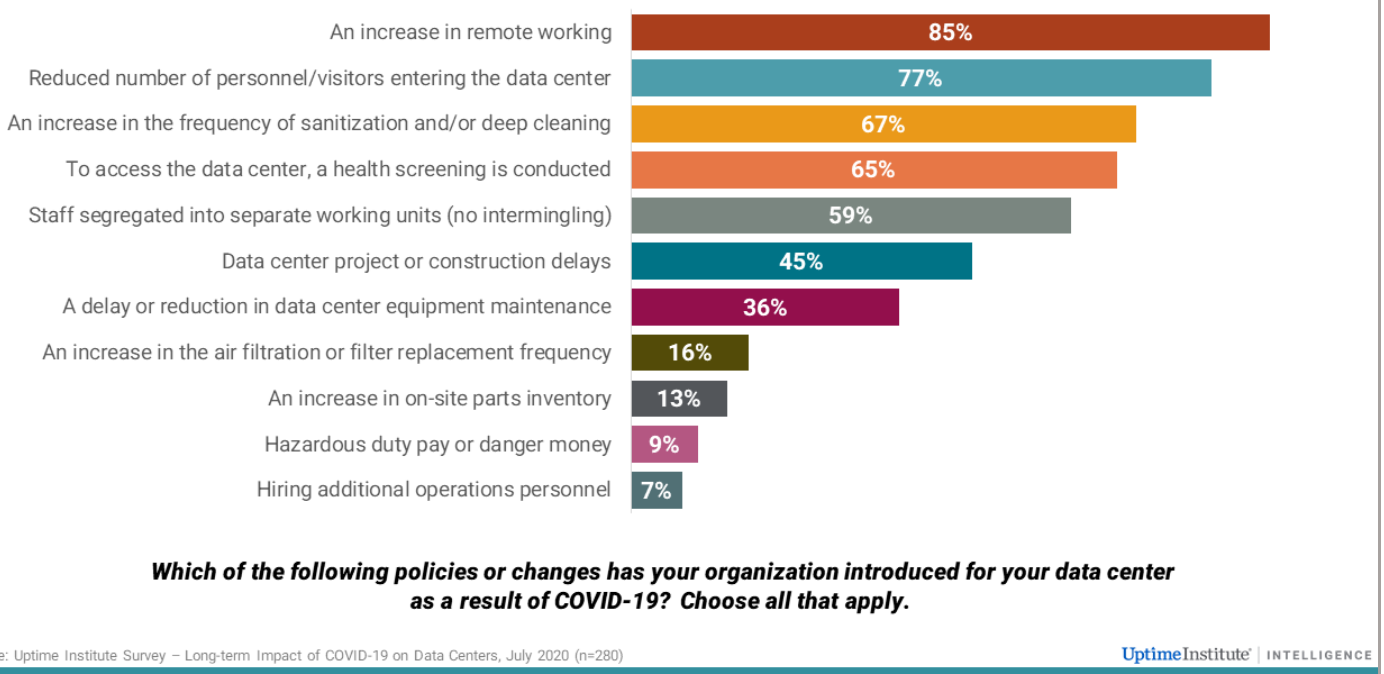


Figure 2. **Managing through the pandemic: Operational changes adopted by data centers**

During this mitigation phase, many delayed projects are being gradually restarted, but as a managed risk; investment is continuing, but is somewhat curtailed (except where clearly pulled by strong demand — this continues to drive new builds and investments). At this time, the management also is preparing investment projects for the third phase — the next "permanent" normal.

Phase 3: Adaptation

The third stage is the next normal: ***adaptation***. At this point, it is likely that a vaccine is (or several vaccines are) widely available for COVID-19, treatments have improved, or the virus has been contained by social measures to the point of routine manageability. However, the world has been alerted to the possibility (likelihood?) of another pandemic. Long-term changes will be planned and put in place, alongside the acceptance of other temporary changes that have proved effective.

In our July 2020 survey, we asked data center operators which steps/changes they are likely to adopt over the longer term – from 24 to 36 months. The results are shown in Figure 3 and are further discussed in **Adaptation: Post-pandemic data centers**.

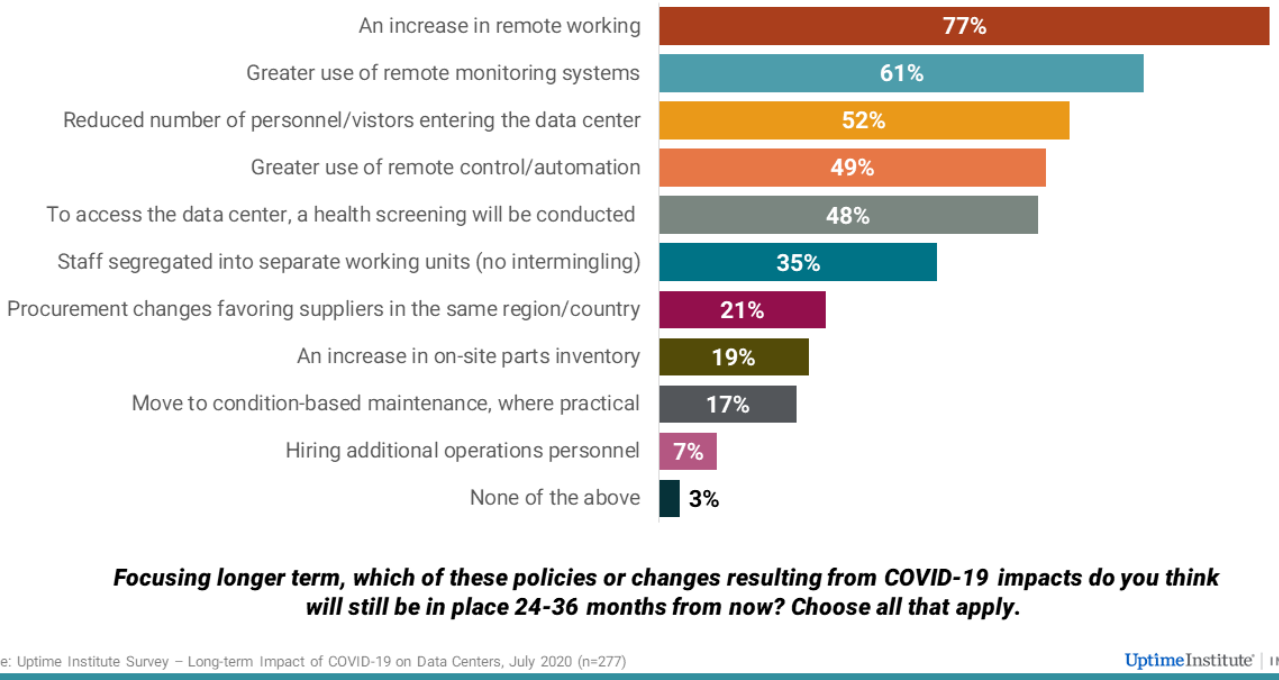


Figure 3. **Living with pandemics: Adaptation strategies that will endure**

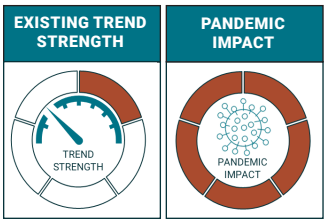
Adaptation: Post-pandemic data centers

In this section, 13 areas of possible or probable change in data center operations are discussed. The list may not prove exhaustive; the areas discussed are mostly concerned with operations, and other changes may occur with time.

These changes should be put in context: When asked to agree or disagree with the statement, "We expect minimal or no changes to our data center (as a result of COVID-19)," 68% agreed. But even though a single operator may perceive a change to be fairly minimal, when many operators undertake the same small modification, it may be considered an industry-wide change. Equally, 32% disagree with the statement; they are planning for and expecting major changes.

In the sections that follow, some of the trends and changes were pre-existing and likely to happen anyway — albeit possibly more slowly/weakly. The **EXISTING TREND STRENGTH** icon shows the strength of the trend independent of the pandemic. The **PANDEMIC IMPACT** icon shows the accelerating/reinforcing impact of COVID-19.

More — and better — pandemic planning



Data center managers, on both the facilities and the IT side, are known for their preparedness. Disaster recovery, business continuity, root-cause analysis, redundancy, fault tolerance — all these are established in the lexicon of day-to-day management. Even so, the pandemic caught most by surprise. Few had an effective pandemic plan in place.

Operators do not intend to be caught out again — and there is an expectation that another pandemic will occur. Pandemic awareness and planning have already been added to the business continuity playbook at many organizations, both as an extension to management and operations, and to disaster recovery planning. Virtually all (94%) of the respondents to the July 2020 Uptime Institute COVID-19 impact survey said they will improve their pandemic readiness and business continuity planning (see Figure 4).

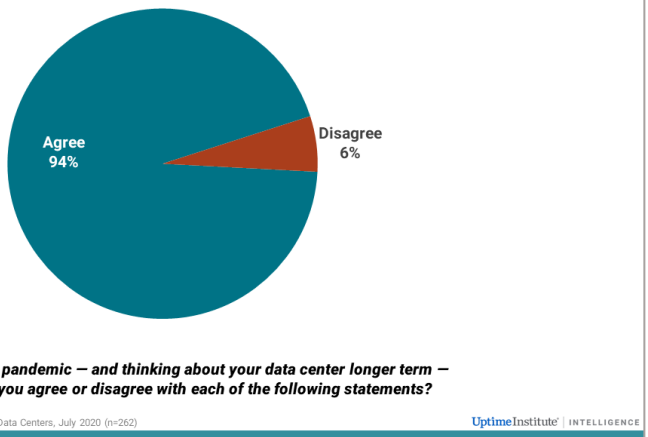


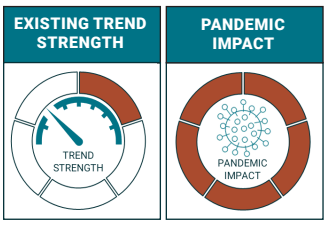
Figure 4. **Most will improve their pandemic readiness and disaster recovery plans as a result of COVID-19**

Some of the procedures and processes that managers expect to have in place in two to three years' time require changes in technology and strategy and may involve major investments. But more routinely, operators expect to clean more regularly, to separate workers into teams, to conduct health screening for visitors, to change air filters more often, and to store more spare parts. These are all part of pandemic awareness and amended processes. Some plan to add emergency accommodation and food storage on-site.

Operators will also enhance their rapid response plans, so they are ready to move to a high alert status at any moment. This will involve rapid implementation of staffing plans, organizing emergency fuel supplies, and changing maintenance processes, for example. To help, they may store personal protective equipment, pay for third-party services, buy reserve cloud capacity, and move to pre-agreed maintenance and management procedures. Operators will be routinely trained in pandemic control and response.

See our report **Pandemic planning and response: A guide for critical infrastructure** for detailed guidance on these topics and more.

More remote working



Data center managers, like their counterparts in other industries, faced some staffing challenges when the coronavirus that causes COVID-19 arrived in their locality. It became necessary to separate workers into two or more teams, for infection control. Staff who may have come into contact with the virus had to be isolated, while others may have fallen ill. In an Uptime survey in April 2020, at the height of COVID-19's first wave, many data center operators were operating on reduced staff. A third identified a reduced level of on-site staff as their biggest single risk.

To reduce risk, almost all data centers delayed maintenance, postponed major projects, and hoped to ride it through. Where possible, staff worked from home and connected to the facility using a combination of simple productivity tools and, where available, remote access and monitoring systems. On-site activities were limited to the strictly necessary.

Many of these changes are now not only well embedded for the duration of this pandemic but are also likely to be permanent. As in other industries, many found remote working to be efficient, practical and safe. As shown in Figure 5, a full 77% of operators surveyed expect an increase in remote working over the next two to three years' time.

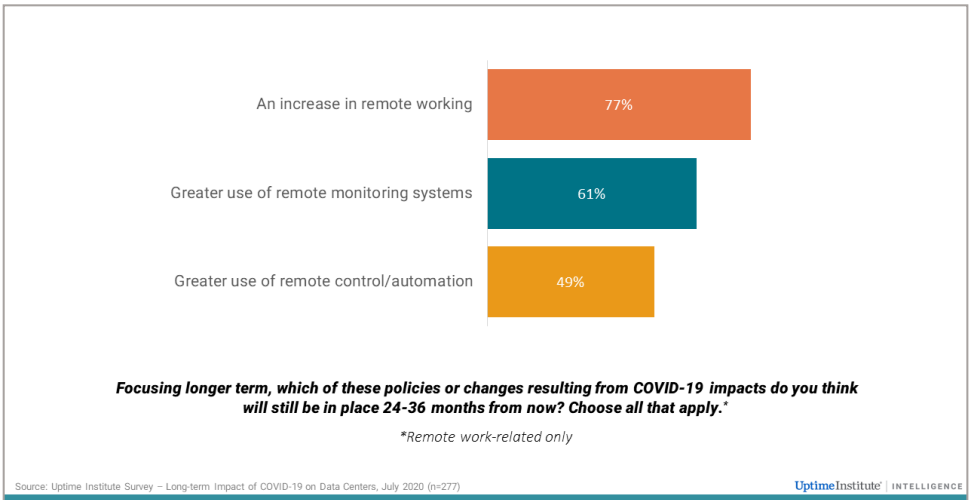


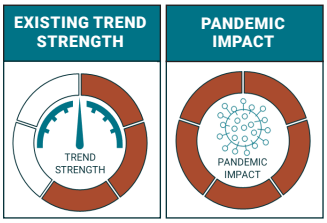
Figure 5. **Data center staff will spend more time off-site**

This has some significant implications for the data center industry, and for operations in particular:

- **Incident management.** Operating with fewer workers on-site during an incident, such as major equipment failure or power outage, will require more planning and testing, and possibly investment in systems and increased resiliency. There may be some increased risk.
- **Remote monitoring/data center infrastructure management (DCIM).** For those working remotely, good monitoring tools, planning resources, and business information will be necessary. This will require greater use of DCIM and other similar systems. If remote control/automation is involved, this will involve a review of systems, security and processes.

- **Remote workers/skills.** The increased use of remote workers has skills and workforce implications. Will this involve a separation of hands-on technicians and remote/software workers? Will there be a rotation system? Will this open the way for greater diversity of workers, who for various reasons cannot regularly attend the data center? Remote working may help managers to overcome skills shortages.
- **Third-party services.** As data centers instrument and prepare their data centers for more remote management, the opportunity for remote, third-party management by a service company increases. Services companies may offer remotely delivered monitoring, management and servicing, replacing on-site workers and sometimes offering to install their own monitoring technology. As a result, we expect the pandemic to trigger increased use of third-party management.

More automation and remote management



For many years, suppliers of DCIM software struggled to persuade data center operators of their product's key value. The price points, and the effort and discipline deployment required (along with some poor experiences), deterred many.

In recent years this has shifted, as larger and more progressive operators have begun to invest more. Now, the COVID-19 pandemic may persuade even the laggards to invest in remote management and automation. With fewer staff on-site and the possible need to reduce maintenance, it is critical to identify problems early, to react quickly, to see trends developing, and to monitor events during an incident. Remote monitoring looks as if it will become a necessity — as will the integration, intelligence, information sharing, and remote collaboration that DCIM helps enable.

Clearly this has been grasped by most operators. As Figure 6 shows, 90% say they will increase their use of remote monitoring/management. This points to a surge in business for suppliers — or at least, for those that remain. The expertise of the suppliers in managing remote access securely will be one of the key points on the tender documents.

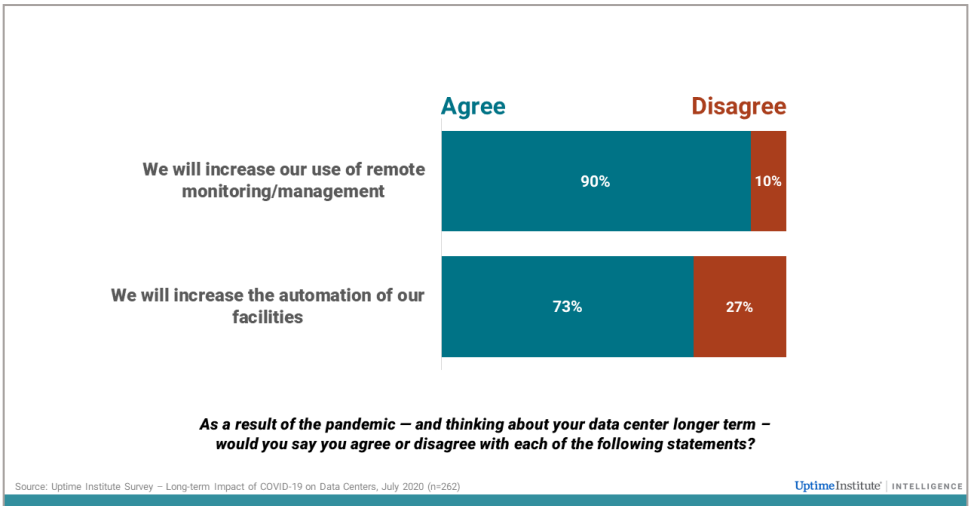


Figure 6. **Remote working will drive investment in monitoring/automation**

If that 90% figure seems high, the 73% saying they will increase the automation of their facilities is a yet more striking number. Automation — where data models and software drive the real-time switching of power, cooling or redundancy — has been viewed with great skepticism by most operators. In fact, most DCIM software suppliers have been asked at some time to prove that their software cannot be used for controlling and switching. (The use of automation in IT itself, moving and optimizing workloads or network routing, has never been considered controversial.)

The pandemic will now act as a catalyst, accelerating a very slow journey up the DCIM/automation stack described in our data center management maturity model (Figure 7). Most today are at levels 2 or 3 but are moving to levels 3 and 4.

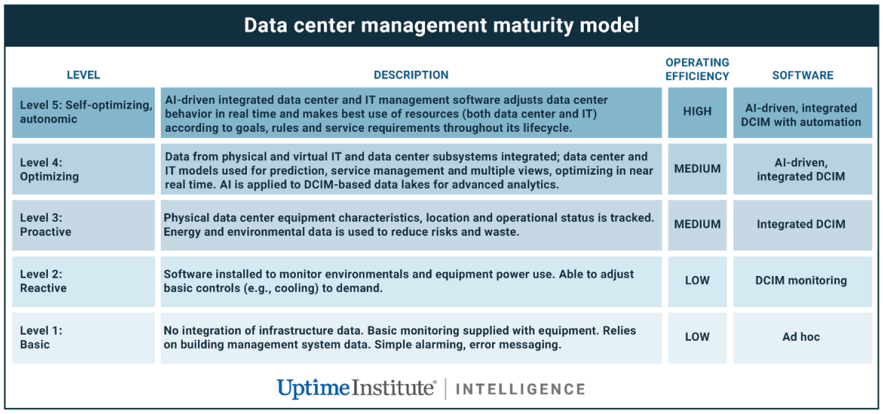


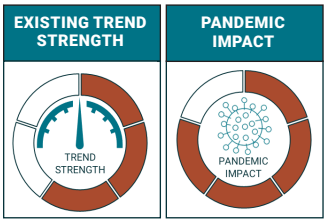
Figure 7. **Advanced data center management requires more use of artificial intelligence and automation**

DCIM and automation will now likely become a much-discussed topic among operators as they step up their investment and deployment. Many of those that do not need a full DCIM system, or that are not ready to deploy one, may benefit from the cloud based DCIM-lite services, or DMaaS (data center management as a service). In time, these simpler systems with basic monitoring will be developed into more complete cloud-based DCIM services (although some functions will need to be local and/or on-site). Equally, DCIM systems will be able to pool data so analytics can be carried out on very large data sets. Using artificial intelligence (AI), this can, for example, predict machine failure based on previously unseen patterns.

The accelerated adoption of more remote management and automation will bring with it increased use of machine learning and AI. This will likely enable more efficient energy use, maintenance and cooling, and better risk identification — with the promise of greater, dynamic load and power management to come.

Remote working may also highlight some of the shortcomings of today's data center management tools. Data center operators will likely want better critical incident management, more collaboration and messaging, tighter integration with service management tools, and insights into human resources and skill set management.

Increased local site resiliency



Having fewer workers on-site, whether in a planned way or because of governmental directives or unforeseen circumstances, raises the immediate question: What happens if there is a failure? Will there be enough workers available to diagnose and fix the issue quickly? As every operations manager knows, time to recovery is a critical metric. Equally, there are certain failures (such as in the power chain) where the clock is ticking before systems have to be taken down — leading to further, bigger problems. In some regions, including in some areas of the United States, the electricity grid has become less reliable, with failures taking longer to fix as a result of pandemic-related procedures and staff shortages.

Remote monitoring and preventive maintenance will help reduce the likelihood of an incident, but failures will always happen. Given this, an obvious step is to design the data center to better withstand failures, or to harden the existing design. In Uptime Institute's July 2020 survey, 64% of operators said they will increase infrastructure resiliency as a result of the pandemic (Figure 8).

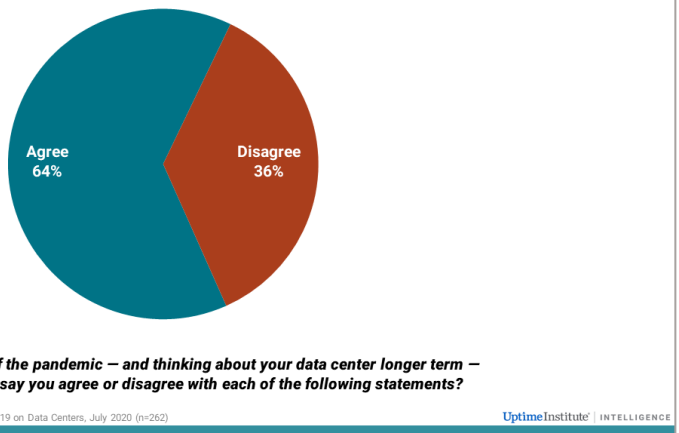


Figure 8. **Many will increase their infrastructure resiliency as a result of COVID-19**

There may be many ways to do this. For example, a data center may be upgraded from a Tier II to a Tier III site, which allows maintenance/repair without systems going offline; or from a Tier III to a Tier IV, which involves moving from having concurrently maintainable systems to full fault tolerance.

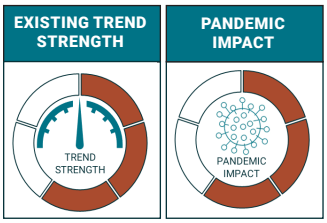
Such steps, of course, can be expensive and difficult, especially if done retroactively. But there may be other measures that can be taken — adding in extra redundancy can help, as can auditing existing data centers to reduce risks and identify points of failure.*

Because of the growing criticality of many IT services, there are signs that operators are designing for increasing resiliency in smaller, lightly staffed data centers. Edge data centers, for example, may be unmanned but can still play a critical role in delivering services. The COVID-19 pandemic,

* Uptime Institute's Data Center Risk Assessment is a low-cost service that identifies risks/single points of failure. Undertaking an Uptime Institute Tier certification also reveals unforeseen design errors in more than 90% of cases.

therefore, may be another factor supporting an existing trend. Separately, at least one major cloud service provider has asked all its colocation partners to ensure their data centers are N+2 redundancy. If they have only N+1, it has asked them to upgrade.

Increased distributed resiliency/ disaster recovery



While increasing the resiliency of a single site will help maintain a service during a period of pandemic, COVID-19 has brought a more frightening scenario into focus: What if an entire site is contaminated, or all operators are sick or isolated? What if, with a more serious virus, it is not safe for anyone to work on-site? Even during COVID-19, Uptime Institute is aware of certain sites that shut down for a period of time.

The traditional approach has been to use a backup disaster recovery site or service, but this has many issues and still risks hours of service loss in most cases. In the years ahead, we expect cloud-based services and distributed resiliency to play a bigger role.

The distributed resiliency approach is used by all of the internet giants and many others. Using the concept of availability zones, data centers are organized into three (or more) clusters, and data and processing distributed across all three. In the event of a failure of one site, the others (two or more) take up all the load synchronously (in a way similar to the synchronous, real-time replication used by, for example, financial services companies for transactions). Each of the sites is fully active — there is no disaster recovery. As long as there are at least three data centers sufficiently near each other to ensure low latency, but far enough away to avoid a localized event affecting more than one data center, the approach is considered initially expensive but highly effective.

As Figure 9 shows, the availability zone approach is spreading rapidly across enterprises, using their own data centers and/or with colocation partners. (Note that Figure 9 is based on findings from the 2020 Uptime Institute annual survey.) The costs and build-out risks are managed down, somewhat, by using racks at multiple colocation sites. In this way, the risk of a complete shutdown of a single data center may be somewhat mitigated.

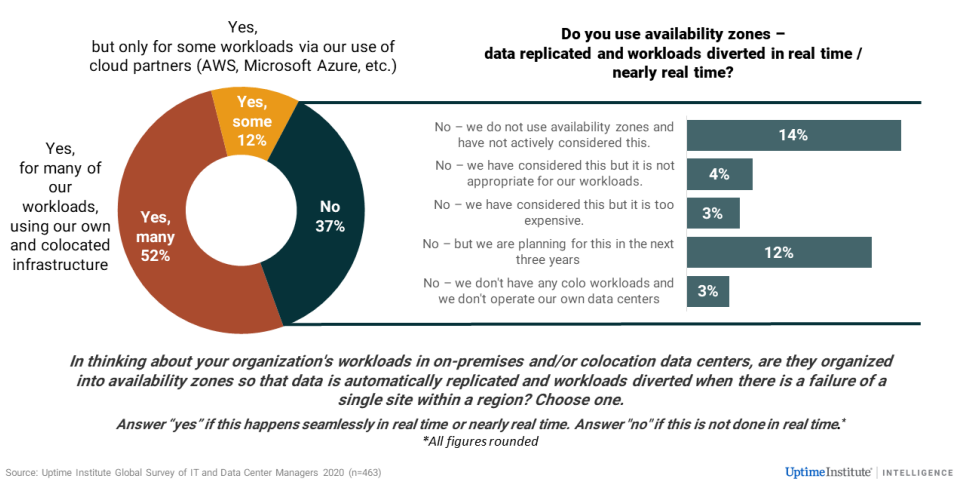
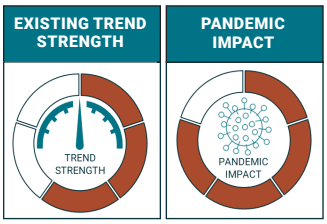


Figure 9. **Most use availability zones**

There are caveats. The approach is most effective for private cloud workloads that can move seamlessly between data centers, and many workloads are not designed this way. In addition, the approach adds considerable complexity in the software infrastructure, which introduces risk. The approach also adds to hardware and colocation costs. Even so, Uptime expects that the pandemic will encourage more operators to make more use of distributed resiliency.

More controlled access



One of the first steps taken by data center operators when the COVID-19 pandemic occurred was to reduce access to the data center — already a tightly controlled environment. Some workers were sent home; maintenance visits were reduced and nonessential visits, almost universally stopped.

It seems likely that this lockdown mentality will become the norm: Half of operators expect to be restricting access to their sites, even in three years' time (see Figure 10). And half expect to be conducting health screening tests. Data center tours, it seems, will become extremely rare. Some operators are looking at whether they can use building information modeling to give remote "access" or to conduct virtual reality tours.

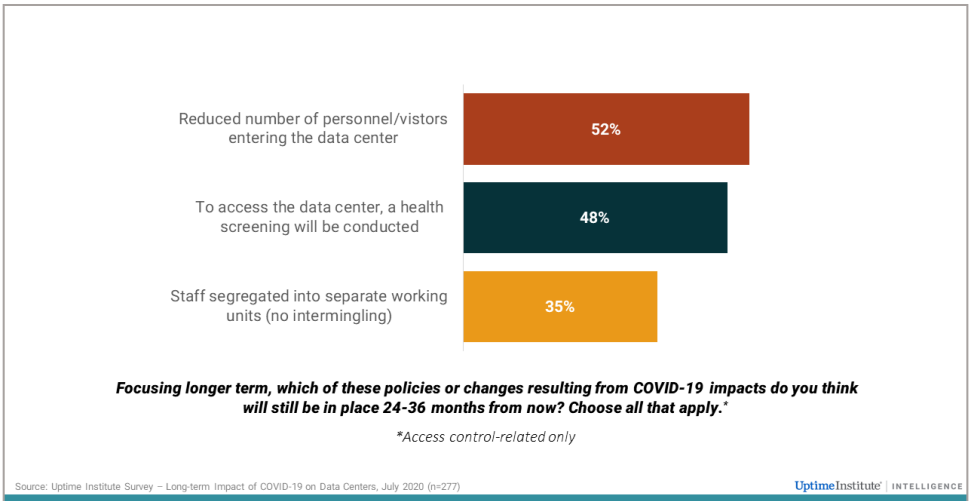
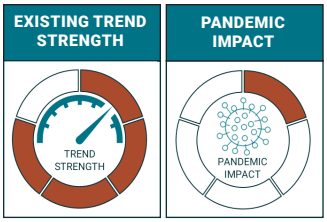


Figure 10. **Entry to data centers will be (even more) tightly controlled**

There are some implications (see **More remote working**). Reducing access may affect maintenance procedures and will possibly require colo operators to renegotiate agreements with their clients.

Greater move to prefab

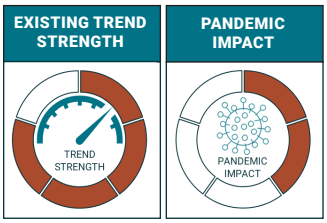


One of the clear findings of Uptime Institute research is that construction projects have been delayed by COVID-19. The primary reasons are threefold: lockdown of staff or other restrictions; supply chain difficulties; and the need to introduce new processes on-site, partly to allow for social distancing. Concerns over future demand, or business uncertainty, do not appear to be a factor. Demand for data centers shows no sign of weakening.

Several suppliers and observers have noted that the use of prefab designs, or pre-built skids, will reduce these delays. This is because a far greater proportion of the work can be done in a factory, under controlled conditions. Because the manufacturing is repeatable, safe processes can be established at the factory and repeated for all clients. Operators will therefore benefit from speedier and more reliable deployment. But there are some caveats: The manufacturing plant will need to be within the region, and it will need to mitigate against its own pandemic risks.

The trend toward increased use of prefab technology is strong (see our report **Ten data center industry trends for 2020**). At the small end of the market (50 kW – 1 MW), there is a strong trend toward micro data centers, containerized data centers and other forms of prefab data centers, delivered as products. For larger data centers, the adoption of lean construction techniques, using prefabricated blocks and complete skids, is speeding up builds and reducing risks (see our report **Best-in-class data center provisioning**). Overall, this is already a strong trend, and the pandemic will have a limited (or no) impact.

Workloads shift to the edge



As the COVID-19 lockdowns rolled across the world during the first half of 2020, a multitude of effects were seen on data center workloads and network traffic patterns. Overall data traffic went up 20% or more in some countries, driven by video conferencing and streaming; wired traffic shot up, as did voice calls over internet protocol, but mobile network voice calls fell sharply. Traffic peaks shifted from the evening (streaming) to the daytime.

Corporate data centers experienced changes in IT demand too. In investment banking, several reported to Uptime that they had hit new peaks, driven by increased trading, while others in heavily impacted sectors experienced dramatic falls. Some cloud services providers struggled to meet exceptional demand: Microsoft experienced near overwhelming demand for Azure and Teams in Europe, for example.

All of these effects were, with a few exceptions, successfully absorbed by the internet, by the exchanges, and by corporate and cloud/internet data centers. But there were some shifts in traffic patterns that are likely to prove enduring, and that will require a response.

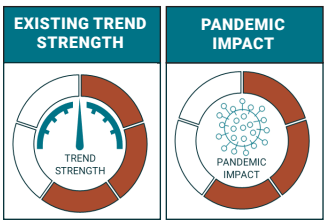
The biggest effect is that traffic shifted from the metro centers to the metro edges – effectively, from offices to houses. This put pressure on edge and last mile networks. This may be met by increasing network

capacity, but more caching, content distribution networks and local processing will also be required. These improvements will also help to build resiliency.

A second effect is that many corporate applications and networks were not designed to support the additional latency, security and traffic volumes caused by a sudden shift to remote working. In large, busy offices, most business takes place face-to-face or on the corporate local area network, not over a wide area network.

The sum effect of all this is difficult to gauge, given the strength of existing trends. It is widely expected that much more capacity will be built at the edge (see "The internet tilts toward the edge" in **Ten data center industry trends for 2020**), and that this will be supported by increased last mile network capacity and by more, small data centers. Equally, many bandwidth-heavy corporate applications (such as conferencing) are being moved off corporate networks in favor of public cloud services (such as Teams). The pandemic will be an accelerator for all these trends.

More oversight, permits and certifications



The COVID-19 pandemic caught governments and regulators by surprise in hundreds of different ways. One of the issues concerned how data centers are regulated and managed: Are data centers part of the critical national infrastructure (CNI)? Which data centers? Should workers be allowed to travel to the facility, to ensure continued operations? Does the government have a role in ensuring uptime and continued operations of services that are not deemed critical?

In a flurry of activity across the world, from February to June, governments began to sort out some of these issues. But there is little consistency: In the US, much of Europe, and parts of the Middle East, data center workers were granted either key worker or CNI status, enabling them to travel to maintain services. In China, South Korea, and some other countries, there were informal exemptions. Other countries did not address the issue at all.

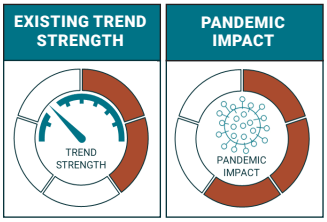
As the lessons from the pandemic are learned, stricter and greater clarification of status and the role of workers is likely. There may even be some international agreements.

Like it or not, more data centers may find themselves classed as part of the CNI. (In most countries, at the moment, only some are — such as telecommunications services.) This can offer advantages in terms of priority access to power and water; but it can mean greater oversight, including for resiliency. One European government official has said that his government intends to review which data centers should be included — noting that unregulated services such as Netflix, Skype, Zoom and Facebook can play a critical role during lockdowns, for example.

Greater government oversight, however, resolves only part of the problem. Few governments are able to monitor this directly, so it will likely depend on a combination of self-regulation and certification in areas such as resiliency, and perhaps sustainability.

It is not only governments that are concerned. Service providers and big IT clients, especially in regulated industries, must also be assured that standards are met, even though site visits will be discouraged. This may also drive up the need for certification and inspections.

Move from scheduled to predictive maintenance

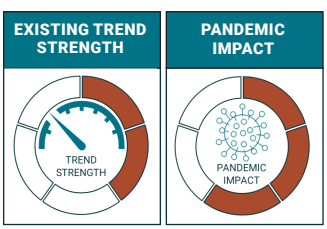


Data centers are operated with strict maintenance schedules. Critical equipment (e.g., generators and the fuel that runs them, transfer switches, uninterruptible power supplies, cooling systems and batteries) requires regular servicing; much of the equipment will fail prematurely, and unpredictably, without it. But in the pandemic, site visits became an infection risk, and there were fewer technicians available to carry out the work. In the early weeks of the pandemic, 42% of operators and data center managers identified reduced scheduled maintenance as one of their top three risk factors. Over time, over a third have adopted this mode as an ongoing strategy, trading off one risk for another.

One approach that is gaining traction gradually, especially if there is much improved monitoring, is to move to condition-based maintenance or predictive maintenance. The former involves less formal scheduled maintenance and more maintenance based on regular monitoring. Early identification of issues triggers a service/parts replacement when needed, rather than according to a schedule. Predictive maintenance takes this a step further, using statistical models and, sometimes, AI to predict when a problem is more likely to occur. Improved problem identification is one of the key benefits.

Changing maintenance approaches can be difficult for data centers, because of warranties and permits, service level agreements and long-established maintenance agreements and plans. In addition, not all suppliers want to change their schedules or reduce their on-site time — for commercial and other reasons. But 17% of the operators surveyed by Uptime Institute do expect to do more condition-based or predictive maintenance as a pandemic-related strategy.

Changes to procurement and supply chain policies



The digital infrastructure supply chain is global, interconnected, and sometimes fragile. It can take just one interruption (e.g., in the manufacture of a component, in regional labor supply or in moving goods from one country to another) to disrupt the global delivery of a critical product — perhaps for an uninterruptible power supply, a transfer switch or a cooling system.

During the first months of the COVID-19 lockdown, supply chain shortages were highlighted in the media, but Uptime's COVID survey results showed that most did not consider this a major problem (although some reported difficulties getting parts). Big suppliers worked hard to ensure parts arrived on time, and they were supported in this by governments that did not want to see key industries damaged.

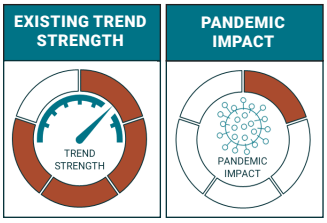
Even so, data center managers now alert to the risks are taking a number of steps to mitigate against supply chain breakdowns. A possible

strategic first step is to reduce the urgency of any failure through increased on-site redundancy or load switching (see **Increased local site resiliency**).

A second step is to build up critical inventory (possibly, even fuel) on-site; just under a fifth said they will be doing this in three years' time. This will require planning and management, especially if maintenance patterns are also changing.

A third step is to review the supply chain. About a fifth plan to favor suppliers based in their own region — a move that will likely favor the bigger suppliers and encourage smaller ones to develop a stronger local presence. This applies to services companies, whose experts may not be able to cross borders. Although it is not often easy because of the lack of standardization, there may also be a move among bigger operators to seek more secondary sources for key components.

A move to the cloud



As the COVID-19 pandemic has unfolded, many observers and stakeholders — especially cloud and colocation executives — have asserted that the pandemic (and fear of future pandemics) strengthens the business case for enterprises to move more of their workloads to the cloud.

There are many arguments for this, but they may be summed in one sentiment: Data centers were difficult enough to run even before the pandemic, and the costs, risks and complexity have all now increased. With the threat of new pandemics in future, it will be easier, even if not cheaper, to move to the cloud.

There is some evidence that many enterprise operators are thinking along these lines. In our July 2020 survey, a fifth (19%) said they are likely to accelerate their move to a public cloud, or use public cloud services more, as a result of the pandemic. Just one in twenty thought the pandemic would slow their move to a public cloud. (Three-quarters said it would make no difference or that they did not know; see Figure 11.)

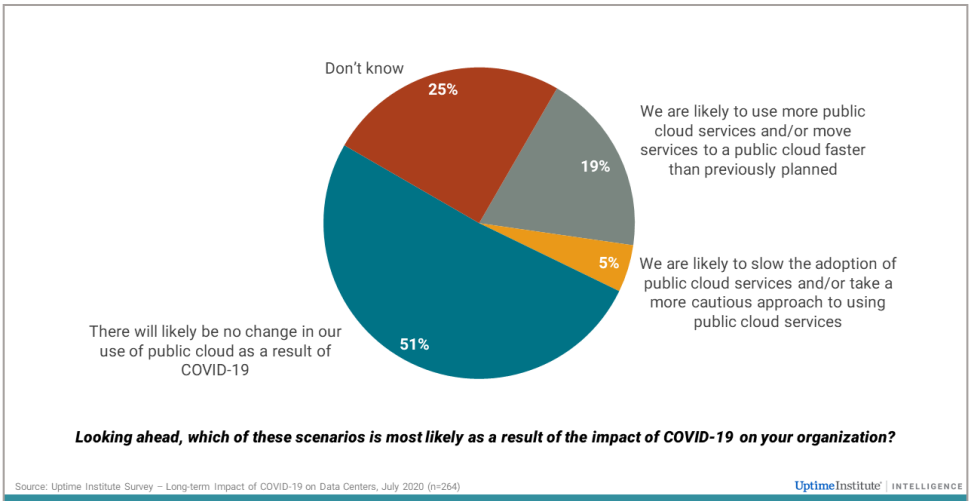


Figure 11. **Pandemic encourages some to move more to a public cloud**

Drilling a little deeper, there are some strong reasons why the use of cloud services has or will increase (further) as a result of COVID-19. First, during the pandemic, many enterprises found they do not have the network infrastructure, or necessarily the applications, to support all of their remotely situated staff, and all their customer interactions, on their networks. As a result, they have rapidly adopted or stepped up their use of cloud and other third-party services. Enterprise dependency on cloud platform providers (Amazon Web Services, Microsoft Azure, Google Cloud Platform) and on software as a service (Salesforce, Zoom, Teams) has significantly increased in the space of a few months.

Second, many operators foresee that the loss of an entire site due to staffing issues is now a possibility (see **Increased distributed resiliency/ disaster recovery**). This will drive up the use of distributed, active-active-active availability zone approaches. Building and managing the IT infrastructure for this is always challenging and expensive; one of the "easier" ways, for many applications and services, is to make use of existing infrastructure — run by cloud providers, their software infrastructure partners, and some colocation companies.

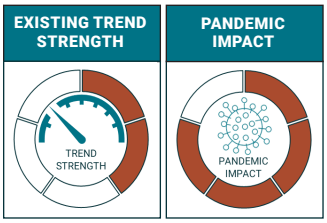
In spite of all this, it would be simplistic to state that the pandemic will trigger a significantly accelerated decline in enterprise data centers or increase in the migration of existing workloads. One of the reasons for cloud adoption, and certainly for the use of software as a service, is to enable use of new services, such as teleconferencing. Few organizations have, in recent years, contemplated hosting such services in their own data centers.

There is already a strong disposition among business and organizational leaders to make more use of the cloud. But migration can be a difficult process, involving re-platforming or rewriting applications, changing security and compliance processes, and foregoing corporate control for limited transparency. Uptime Institute's research shows the balance of workloads shifting gradually, over time, in a cautious fashion.

A further issue: Chief Information Officers are facing cost constraints, with a global slowdown (if not recession) already underway. Cloud adoption usually involves a short-term spending increase, even if costs fall over time (which, depending on scale, they may not).

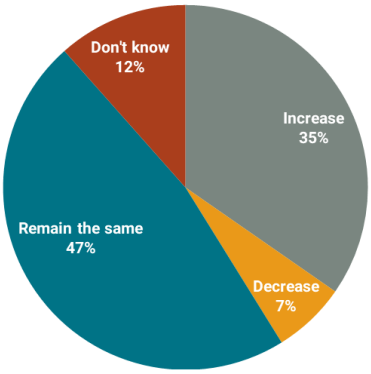
The verdict? Public cloud adoption by enterprise is a strong trend with multiple adoption drivers. The pandemic will add to the rationale but will not make a decisive difference.

Increased automation and resiliency, driving up costs



Will data centers after the COVID-19 pandemic be more expensive to run — or perhaps, with fewer on-site staff, could they even cost less to run?

In our July 2020 survey, Uptime asked operators if they expect their data center operations to cost more, less or about the same in two to three years' time due to pandemic-related policies and changes. The results are shown in Figure 12. While about half think it will be the same, more than a third expect a cost increase, and only 7% expect a decrease.

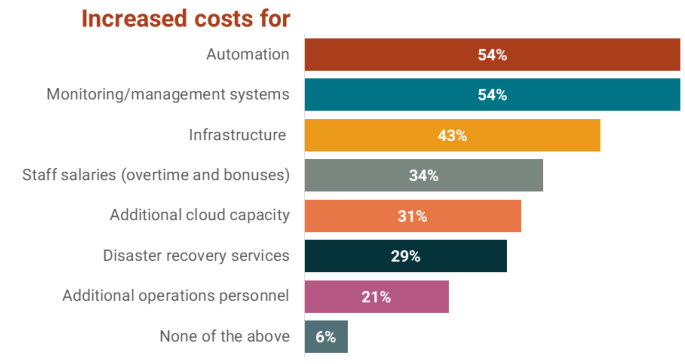


Looking ahead 24-36 months, do you think the cost of your monthly data center operations will increase, decrease, or remain the same due to your organization's COVID-19 policies and changes?

Source: Uptime Institute Survey – Long-term Impact of COVID-19 on Data Centers, July 2020 (n=277)

Figure 12. **About a third think operational costs will increase as a result of COVID-19**

For those expecting an increase, the biggest reasons cited were increases in automation and remote management and in upgrading infrastructure (see Figure 13). These investments are in line with changes identified in earlier sections of this report, and again suggest that the pandemic will lead to a surge in business for DCIM, monitoring and automation vendors. Extra staff, more third-party services and staff working longer hours are also expected to drive up costs for many.



Looking ahead 24-36 months, which of these do you think will contribute to the data center operations cost increase due to your COVID-19 policies and changes? Choose all that apply.*

**Among those who anticipated increased costs*

Source: Uptime Institute Survey – Long-term Impact of COVID-19 on Data Centers, July 2020 (n=96)

Figure 13. **Many expect increased costs associated with post-pandemic policies and changes**

We also asked how big these spending increases are likely to be. The overwhelming majority expected the increases to be below 20% per

month — even so, a significant boost for operational managers who may have been struggling to secure management support/investment. Of the small percentage expecting a decrease, about two-thirds anticipated cuts of up to 20%, with the remainder expecting larger cuts.

One aspect of this is puzzling: DCIM and automation vendors usually argue — quite strongly — that organizations using their products will cut costs, not increase them. This is not the expectation of managers: they expect to be adding functions and paying more, not cutting back on other resources. They may also be accounting for the fact that, by upgrading infrastructure, they will likely be increasing their support and power costs — a price worth paying if the risk of an outage is reduced.

Conclusions

One of the clear lessons of the pandemic is that critical infrastructure is just that: critical. Without remotely delivered services, the overall impact of the pandemic to most businesses would have been far worse. As the world emerges from one pandemic but goes on to yellow alert for another, those operating critical infrastructure are now in the front line, having to plan for and incorporate the necessary capabilities, capacities and resiliency to ride through forthcoming emergencies — even if they never occur.

Few of these changes seem revolutionary but taken together they represent a new phase in the maturity of the data center sector. In keeping with long-term trends, data centers are becoming more automated, more resilient, more remotely operated, and more likely to be subject to watchful oversight.

Figure 14 demonstrates most of the points made above and throughout this report: Operators strongly agree they will plan for future pandemics; they will operate their data centers more remotely, with increased automation, and they will step up their resiliency.

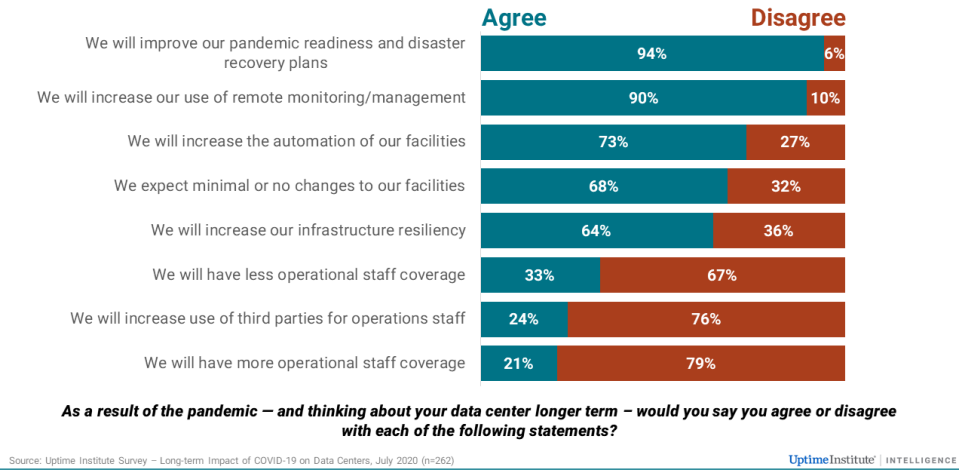


Figure 14. **Operators agree: We will plan for a remotely controlled and resilient future**

Appendix

In our most recent (July 2020) global survey, The long-term impact of COVID-19 on data centers, Uptime Institute questioned more than 300 professionals familiar with the operation of their organization's critical IT infrastructure and data center facilities. We asked them more than a dozen questions about the immediate, short-term and anticipated long-term impacts of COVID-19. The respondent demographics are shown in Figure A1.

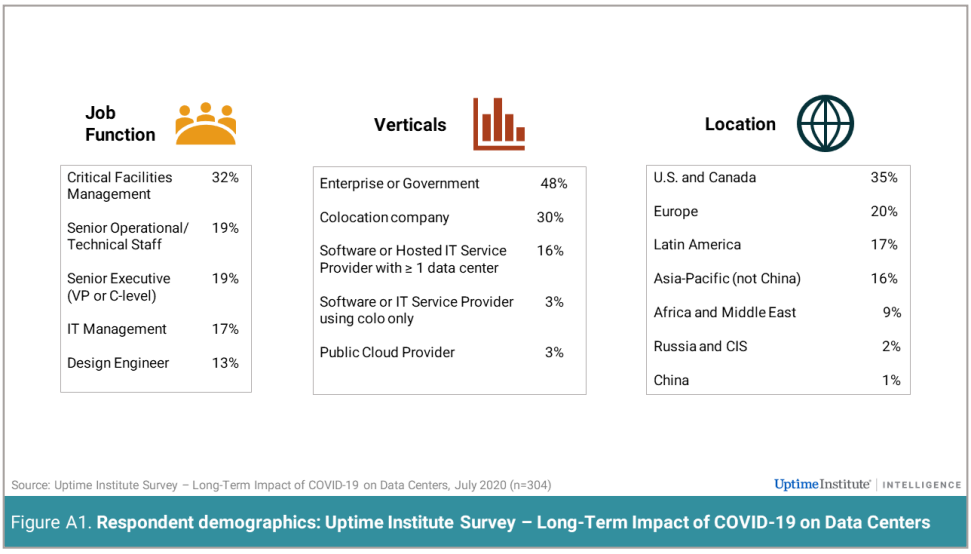
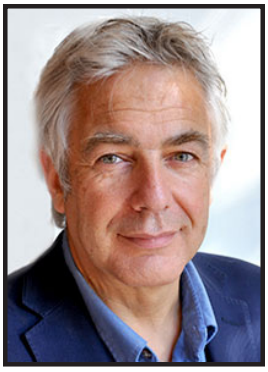


Figure A1. **Respondent demographics: Uptime Institute Survey – Long-Term Impact of COVID-19 on Data Centers**

Uptime Institute has a robust collection of COVID-19 resources — reports, Bulletins, webinars and more — to help operators of critical infrastructure facilities prepare for and respond to the impacts of pandemics and other emergencies. Resources are available in multiple languages and may be accessed here.

Uptime Institute® | INTELLIGENCE

ABOUT THE AUTHOR



Andy Lawrence is Uptime Institute's Executive Director of Research. Mr. Lawrence has built his career focusing on innovative new solutions, emerging technologies, and opportunities found at the intersection of IT and infrastructure. Contact: alawrence@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

