Return to Business as Unusual: Workplace of the future

White paper

Part one in the *Business as Unusual* white paper series

Authors

Sampath Sowmyanarayan
Jay Venkat
Michael Coden
Val Elbert

BCG | verizon

Introduction: What will the future workplace look like?

It's a constant concern for business leaders around the globe. Every year, think tanks, businesses (including Verizon), academics and analysts give their view on the technology trends that they believe will most impact the future workplace—and how those technologies are shaping business technology investment.

Over the years, the pressures driving toward remote working have been building, but no one could have predicted the seismic shift caused by COVID-19. Entire functions of many global organizations are now working remotely, and this looks set to permanently alter the way people think about the world of work.

Remote working is no longer a benefit, luxury or convenience. It's also more than a current make-do for organizations looking to conduct business as usual. We argue that senior leaders will have to leverage this inflection point to drive sustainable competitive advantage for their organizations in the new normal.

We are creating a series of articles that will examine how business leaders need to think about enabling the workplace of the future, with remote working fully integrated into business practice. In this first article, we are focusing on the technology building blocks that CIOs need to consider while taking into account the underlying emerging set of new technologies.

Over the last 30 years, remote working in the U.S. has grown 7% yearly. Despite that growth, only 7% of U.S. civilians currently have access to a "flexible workplace" benefit.

The COVID-19 effect

Even before the coronavirus hit, remote working had been steadily increasing in many countries around the globe. For example, the St. Louis Federal Reserve Bank[1] found that over the last 30 years, remote working in the U.S. has grown 7% yearly. Despite that growth, only 7% of U.S. civilians currently have access to a "flexible workplace" benefit, according to the U.S. Bureau of Labor Statistics.[2]

Many organizations, therefore, have largely stayed true to the idea of the office workplace—that is, until COVID-19 hit. One reason for this could be that many established businesses have foundations that were built in the last century, and the corporate world is still primarily defined by the baby boomers—a group that entered the workforce before mobile phones, personal computers and the internet even existed. For them, the office is where work is done, and the very concept of remote working may raise concerns over productivity and motivation.

Which is why many organizations have not enabled remote working as part of their business as usual before now. Those organizations that were still largely built around an office-based model are the ones that have had to scramble the hardest in recent weeks in the drive to set up remote working capabilities.

The 4 waves of remote working

In our view, there are four waves of remote working, and right now, we're in the middle of the COVID-19-induced third wave. The COVID-19 crisis is hastening organizations' ambitions to embrace remote working as the new normal. What CIOs around the globe need to think about is how to make this happen.

What's interesting is that, over recent years, we've already seen "traditional" ways of working being pressured from various directions, including the impact of the sharing economy on lifestyle, the gradual decline in commute efficiency, the fight for millennial talent and the impact of the climate crisis on air travel. This is perhaps why many jobs were already starting to be enabled remotely, from contact centers to customer service, computer programming to sales, data entry to medical billing, coding to design.

What is becoming clear is that the post-COVID-19 new normal will be different. Boston Consulting Group's view is that "comfort with remote work will reshape our future workplace," where flexible work arrangements will increasingly be the norm.[3]

Comfort with remote work will reshape our future workplace.

In the post-COVID-19 fourth wave of remote working, organizations wishing to drive sustainable competitive advantage will have to resolve a set of challenges across both technologies and people, and piece together talent attraction and retention, employee engagement, and partner engagement effectiveness in a cohesive manner.

Underlying this wave will be the emerging deployment across key industries of a set of new technologies now taking shape, such as artificial intelligence (AI), machine learning (ML), and spatial sensing and mapping.

For example, remote workers will need access to experts, call center operators will need an environment where security and data privacy issues are well addressed, and teachers will need a way to monitor tests and exams. It's critical to start with the user's needs and create a user experience that threads back through the supporting technologies to create a user-friendly and highly functional working environment.

It's critical to start with user's needs and create a user experience through the supporting technologies.

The four waves of remote working

1

A decade ago

Mainly centered around cost savings

2

In recent years

Benefit to attract and retain talent, or tapping into the ecosystems of global partnerships and supply chains

3

Currently

Business continuity tool designed to enable organizations to stay functional in the light of COVID-19

4

The new normal

Competitive advantage within remote working; deployment at scale across key industry verticals, extension into next-generation technologies

The challenge for CIOs

The unique set of challenges presented by a remote workforce requires all senior leaders of an organization—CIOs, CHROs, CISOs—to work together to resolve them.

The CIO needs to be a proactive participant in leading and driving change, describing the competitive advantage and clearly demonstrating the link between the technology agenda and the employee value proposition. Opening up the possibility of remote working to more employees demonstrates that it can work (and in days rather than months), so it can be a part of the new operational plan. But that means throwing away the old plan.

Opening up the possibility of remote working to more employees demonstrates that it can work, but that means throwing away the old plan.

They may have been working toward a PC refresh, a global software deployment or a new software-defined wide area network. Are those still the right priorities for the business?

Of course, it's not that CIOs don't plan for unprecedented events. It's that most business continuity plans contemplate regional pandemics, and focus on how other regions of the globe can pick up the workplace slack. The global nature of the COVID-19 pandemic is unprecedented and has caught many CIOs unaware.

Within this new wave, the CIO's role in managing the table-stakes agenda from the previous three waves remains the same. From the broadest goal of on-the-ground operations (such as ensuring that technological systems and procedures are aligned with business goals) to planning ahead for the future (like understanding digital technologies and how to cost-effectively utilize them), the CIO still plays an integral role. But now an additional focus needs to be put on the forward-looking "next wave" of technical building, beyond the table-stakes priorities. And early preparation is key.

We'll expand on the challenges CIOs and businesses are facing more in our next chapter, but the "new" considerations include:

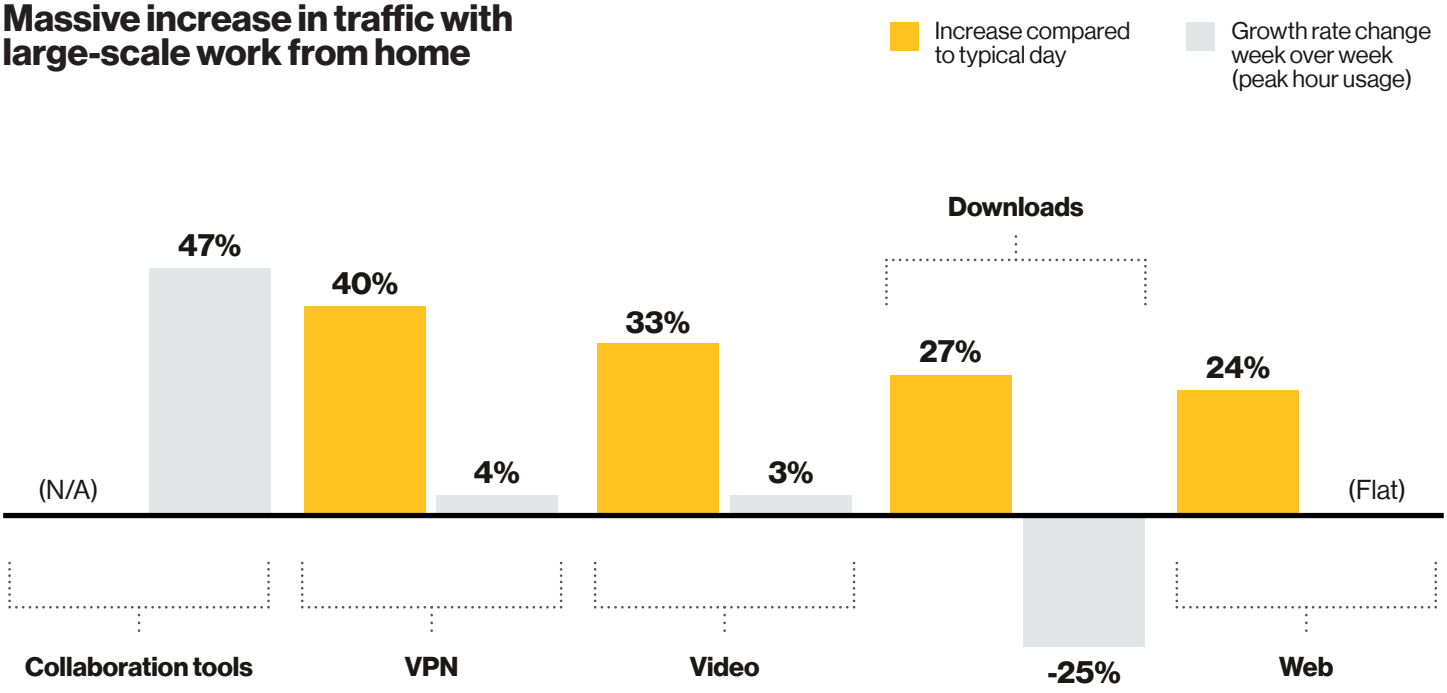
- Is remote-access infrastructure robust enough to handle most employees shifting to remote work?
- Are core business applications cloud ready? Or are you relying on bulky solutions that are not user friendly as a workaround?
- Can your collaboration solutions cope with a massive explosion in traffic volumes as users switch to virtual collaboration solutions (see figure below)?
- Is your dispersed office environment secure?

Once you move the office perimeter to the user device, it's vital to establish secure trust environments to safeguard customer, financial or personal data. We've already seen a massive uptick in cybercrime looking to exploit COVID-19.

What's clear is that CIOs need to seize the opportunity to plan for the future right now. They need to look at how to put in place a network architecture that will enable them to quickly adapt to the new, flexible remote-working world. This series of articles will outline the technical building blocks that all organizations should consider deploying post-virus, to future-ready their business success.

Once you move the office perimeter to the user device, it's vital to establish secure trust environments.

Massive increase in traffic with large-scale work from home



A CIO's guide to driving remote flexibility: Challenges and resolutions

When most people talk about remote working today, they are really talking about working from home. And of course, that is what many people are currently doing.

What's interesting is that, even before we entered the pandemic situation, Gartner research suggested that "By 2030, the demand for remote work will increase by 30% due to Generation Z fully entering the workforce."[4] However, the model needs to be flexible—the ability to "work from wherever," rather than just home, is key. The challenge for CIOs is that most current workplace constructs cannot be fully scaled to support a flexible remote-working model.

The ability to "work from wherever," rather than just home is key. The challenge for CIOs is that most current workplace constructs cannot be fully scaled to support a flexible remote-working model.

We have already mentioned that buy-in from senior leadership is critical to ensuring that an effective remote-working model is created.

For the CIO specifically, six factors are required for an employee to be able to effectively work remotely:

1. A scalable network enabled by automation, such as software-defined networking (SDN) and virtualized network services (VNS), that can flex to support new usage patterns with work shifting outside of offices and enable application availability prioritization
2. Cloud-ready applications for collaboration, core operations and support
3. Strong and secure mobile connectivity to access those applications, as well as the corporate WAN (for those that are not cloud-enabled)
4. End-to-end monitoring of network performance to maintain control, usability and security
5. Zero-trust security implementation that strengthens the protection of sensitive information outside of physical offices
6. A resilient end-user support model and supply chain that can deal with spikes in teleworker demand, both in terms of calls for help and the need for laptops, tablets or other mobile devices

For many organizations, the COVID-19 pandemic has highlighted the gaps in their current model that prevent scalability.

Here are the future technological building-block investments CIOs should be focusing on now to enable them to redefine the new normal in the workplace of tomorrow:

A scalable network

One challenge many organizations will have to look at is the scalability of their enterprise network services (ENS), as both hardware and connections are usually restricted. The first priority is to look at core network provisioning and ensure that there is enough capacity, via either private or public internet, to enable scaling to support changing work patterns. The ability to quickly scale services is vital in a high-demand, high-usage situation. With a strong network foundation, SDN can come into its own.

The ability to quickly scale services is vital in a high-demand, high-usage situation.

SDN technologies give organizations the flexibility to scale at speed by enabling the network administrator to add or remove virtual machines (either on premises or in the cloud). Services, such as virtual private network (VPN) resources, can be orchestrated by a centralized policy engine to flex and scale as the business requires. And new services, like software-based firewall services to terminate VPN traffic in an emergency work-from-home environment, can be quickly initiated on demand.

SDN can also enable policy-driven automated workflows via application program interfaces (APIs) and dashboards, giving CIOs the benefit of network-wide visibility, analytics and control, and also allowing enterprises to more seamlessly take advantage of non-homogenous connection types.

Cloud-ready applications

A second challenge for organizations is that many applications are not ready for remote working. Most organizations use three types of applications on a daily basis:

1. Collaboration tools—e.g., cross-platform video conferencing or unified communications
2. Core operations—e.g., mainframe-based applications or contact center platforms
3. Support applications—e.g., integrated payment processing

The challenges with collaboration tools are that they are not yet universally adopted; they lack interoperability (for example, you can't use Cisco Webex to chat with someone on Microsoft Teams); and they are often only available for the most recent operating system updates (as many of us trying to support elderly relatives by getting them to download Hangouts have recently found out). In addition, it is often difficult to use them for real-time collaborative document sharing and editing. What's more, many require WAN access to enable employees to collaborate with partners (e.g., local deployment of Google apps).

The answer here is to ensure that collaboration tools are easily accessible both internally and externally, unified and integrated across different systems and devices. This might have to be user-case specific; for example, field staff who have to interact with multiple customers will need to have a tool that works for their clients as well.

The answer here is to ensure that collaboration tools are easily accessible both internally and externally, unified and integrated across different systems and devices.

Additionally, for many organizations, core applications are not cloud based, but require access to the WAN through a Citrix desktop. This means that organizations need to rethink how they make access to core operational tools available. And this will, of course, vary by industry and job function.

For example, payment processing and inventory management may have different starting points when it comes to cloud hosting. And payment processing may have different processes and requirements in different verticals, which may make moving all operations to the cloud even more complicated. But thinking about which applications can be moved to the (secure) cloud is a key component of enabling remote working.

Remote working capability will be limited to the capacity and resilience of network connectivity.

Strong and secure mobile connectivity

This is perhaps a fundamental challenge when it comes to enabling remote working. Many employees' remote working capability will be limited to the capacity and resilience of their network connectivity. Home broadband capabilities vary dramatically from country to country and city to city; even in well-served markets such as Europe, the European Commission reports that ~83% of EU households do not have access to next-gen high-speed internet access services.[5]

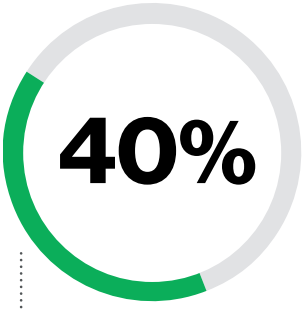
In addition, many home networks are still unsecured, exposing users to potential cyberattacks. This is particularly true when people use a "home tech" apparatus and utilize the same devices for home and work, and/or access free Wi-Fi on the go. (See figure below for findings from Verizon's 2019 Data Breach Investigations Report).[6] It could also manifest as security issues across work practices, such as capturing sensitive customer information on scraps of paper that may land in the wrong hands.

Employees can be internet enabled with hotspots, dongles or even just mobile phones, which can help them work remotely if their broadband connection is insufficient. But this is also where the VPN comes into its own, enabling the compartmentalization of work and personal information.

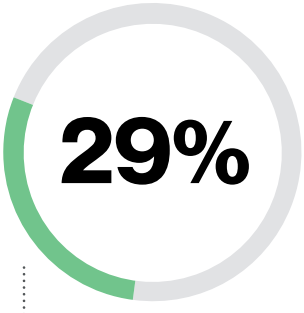
Supporting secure VPN access is a critical component to consider if remote working is to be successful.

However, many VPN solutions are not designed to handle the volume of traffic that a sudden increase in remote workers causes, and therefore may suffer loss of availability and downtime. What's more, traditional VPNs may not address the risk of malware being introduced to corporate systems as a result of insecure remote-worker systems and devices. Supporting secure VPN access is a critical component to consider if remote working is to be successful.

Findings from Verizon's *2019 Data Breach Investigations Report*



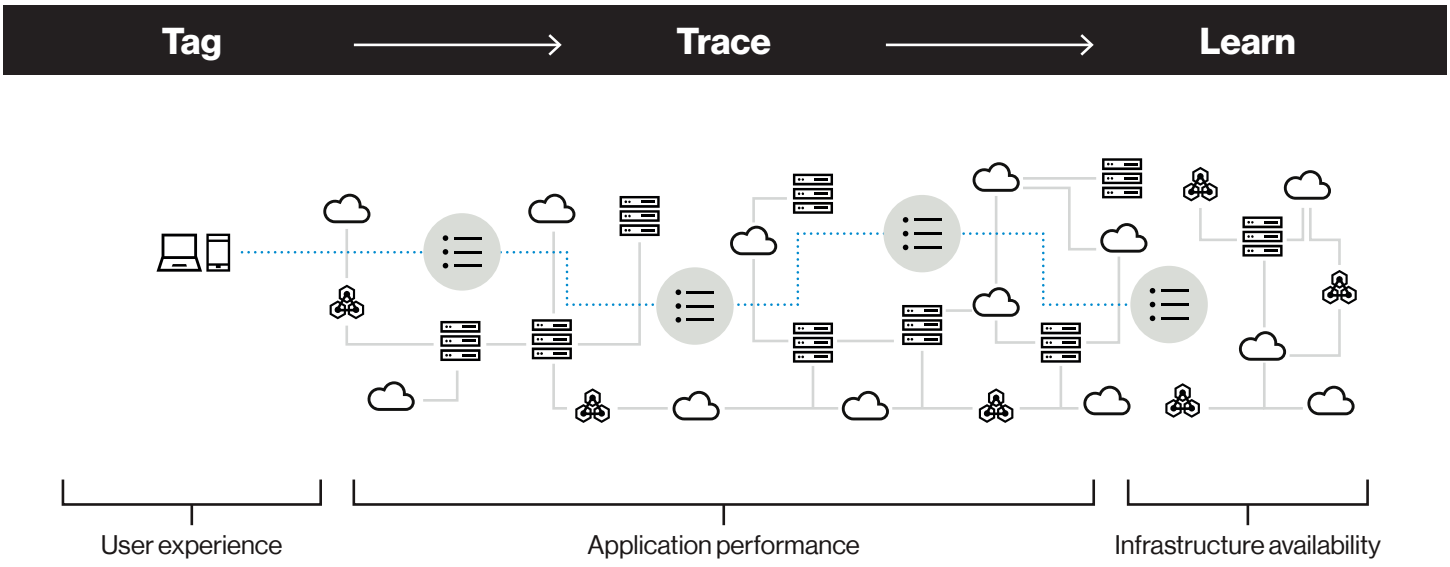
Forty percent of all breaches involved compromised and weak credentials.



Twenty-nine percent of all breaches involved use of stolen credentials.

End-to-end network monitoring

Another challenge for CIOs is getting an end-to-end view of how business processes are working across their network, especially as mobile endpoints proliferate in a remote working model (refer to figure on next page). The essence of the story is that, as work moves outside offices, monitoring needs to follow. CIOs basically need to look to measure end-user and device experiences across the now disaggregated infrastructure.



Implementing robust tracking and monitoring capabilities for data-exchange process flows and transactions is critical.

At the device level, this means setting up a more robust network-monitoring architecture and accounting for more variables in the supply chain to achieve high levels of efficacy and productivity within the work-from-home environment. At the user or transaction level, this means monitoring the experience across the supply chain, e.g., baselining the supply chain to identify improvement levers and where investments should be channeled.

For large organizations with managed services and differentiated service level agreements across multiple locations, implementing robust tracking and monitoring capabilities for data-exchange process flows and transactions is critical.

These must be complemented with the right toolsets to reduce errors. In addition, dynamic scenario planning should be considered, and constantly refreshed, to prepare for the worst and put in place preparatory measures.

Zero-trust security

Security of customer, financial and personal data is fundamental for all organizations, large and small. Many companies have historically restricted access to sensitive data to on-premises devices, so shifting to employee homes (as needed) may be largely unprecedented territory. Security issues also become more complex when data and applications are utilizing hybrid storage, i.e., a mix of on-premises and in-the-cloud storage. So the challenge is how to protect access to sensitive data, while also maintaining the availability of resources.

Organizations need to adopt robust protect, detect and respond mechanisms.

Protect

Establish a security architecture designed to support remote working, e.g., one that leverages strong identity management, multifactor authentication, VPN, trusted mobile endpoints, network segmentation and post-authentication access controls. The use of personal devices for work also has to be weighed, as this may pose challenges when it comes to corporate-wide malware propagation and data privacy issues.

Detect

Implement fully integrated risk monitoring and detection capabilities for work-from-home devices to identify potential security breaches. Organizations need to build deep, end-to-end, integrated data and analytics capabilities to detect breaches early, while also working to reduce the impact of phishing attacks.

Respond

How the organization deals with a security threat. This is obviously easier within an "internal" environment and more complicated in a remote work model with multiple mobile endpoints. Cyber-risk monitoring enables organizations to effectively manage their security posture. Organizations should also consider the retention of professional support to assist in the event of a security breach.

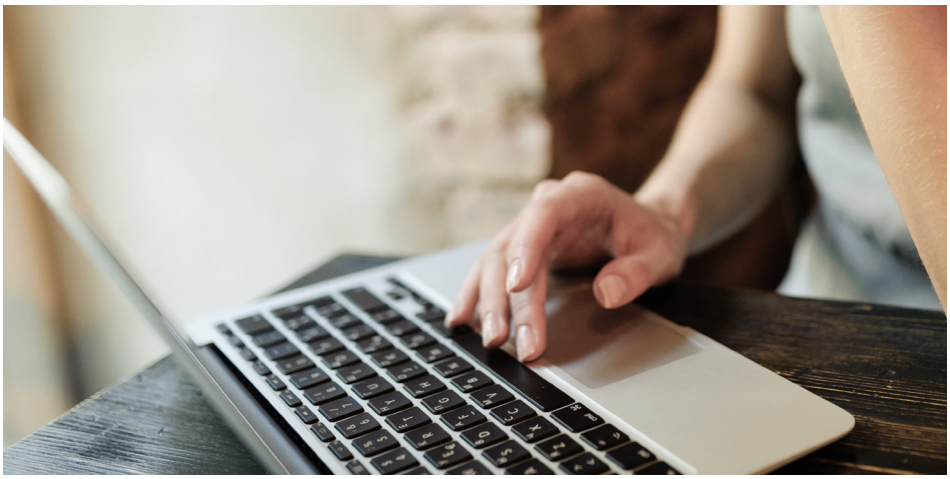
A resilient end-user support model

Finally, CIOs also need to review their technology supply chain to assess if they have an overdependence on specific suppliers. This may impact their ability to deliver equipment to employees or their customers, and reliance on a specific hardware vendor may also pose challenges for installation of any required customized features (for example, within SDN) to support remote working versus operating on a universal software layer. Diversification as a business-as-usual policy may be necessary to ensure that the organization is not anchored to a single brand or technology, so that issues such as stock depletion can be overcome.

What about 5G and mobile edge computing?

5G and mobile edge computing (MEC) have a lot to offer in remote working scenarios, but 5G capabilities, at least in the initial phases of rollout, will be more focused on urban areas, or deployed to support Industrial Internet of Things (IoT) or similar applications. In that sense, the other technical building blocks we've previously referenced should be considered alongside any 5G and MEC deployment strategy.

Of course, when 5G is available, it is expected to deliver faster download speeds, greater capacity and better quality communications, thus addressing stable connectivity issues in certain locations. But both are technology enhancers, not full enablers. It's more critical that companies act now—and act fast—to enable remote working.



Call to action: The time is now.

COVID-19 upended the world in an instant. It's critical to begin strategizing around and implementing the technical building blocks outlined above now, to allow you to rapidly scale and adapt and future proof your business for remote working.

And given pre-pandemic remote working trends, it's safe to say that we're well on our way to the fourth wave of remote working. Plan now to ensure you're capturing the true needs of your employees and customers to ensure alignment across your organization as we pivot toward the "New Normal."

Looking ahead, solving technical challenges is just the first step in planning for the future of remote working. Are organizations well set-up vis-a-vis these dimensions? How will you set up typically siloed functions for success in a remote working model?

What becomes of corporate culture when moving to a dispersed organization paradigm? And what are the mindsets required to emerge as remote leaders in a post-Covid world?

We will tackle these topics in the upcoming articles:

- Technology Transformation and Readiness Assessment
- Mastering Change Management to Lead In the Workplace of the Future

Authors

Sampath Sowmyanarayan, President, Global Enterprise, Verizon Business

Jay Venkat, Managing Director and Senior Partner, Lead of North America Technology Advantage Practice Area, Boston Consulting Group

Michael Coden, Managing Director, Global Leader of Cybersecurity Practice, Boston Consulting Group Platinion

Val Elbert, Managing Director and Partner, Boston Consulting Group

1 https://www.stlouisfed.org/publications/regional-economist/third-quarter-2019/working-home-more-americans-telecommuting
2 https://www.pewresearch.org/fact-tank/2020/03/20/before-the-coronavirus-telework-was-an-optional-benefit-mostly-for-the-affluent-few/
3 https://www.linkedin.com/pulse/covid-19-future-work-diana-dosik/
4 "With Coronavirus in Mind, Is Your Organization Ready for Remote Work?," Smarter with Gartner, March 2020. https://www.gartner.com/smarterwithgartner/with-coronavirus-in-mind-are-you-ready-for-remote-work/
5 https://op.europa.eu/webpub/eca/special-reports/broadband-12-2018/en/
6 *2019 Data Breach Investigations Report*