The new BAU: Business as unusual

Insights on optimising today and planning for tomorrow

Eleven of our experts address the most common questions we've been asked by O2 Business customers during the recent rapid transition to working from home and while they plan for the future.

Inside you'll find immediate and longer-term considerations for your business covering four key areas:

O2 business

Introduction

Ant Morse
Head of Digital Solutions, O2 Business
in linkedin.com/in/antmorse

Dave Cornwell
Head of Solutions, O2 Business
in linkedin.com/in/dpcornwell

We're all coming to terms with the new BAU: 'Business as unusual'. And the question we're being asked a lot by customers is "What now?". Not just because of the uncertainty that COVID-19 has generated from a macro perspective. But also because the overnight shift to working from home has affected sectors, businesses and groups of people differently. So standard answers have been in short supply.

Yet there are ways to compartmentalise what has happened. Like framing questions about our choices into different phases. There was the initial rush to ensure people could carry on working. We have now entered a phase in which organisations are re-evaluating the choices made to either rectify issues or build on positive actions. And then there is the future.

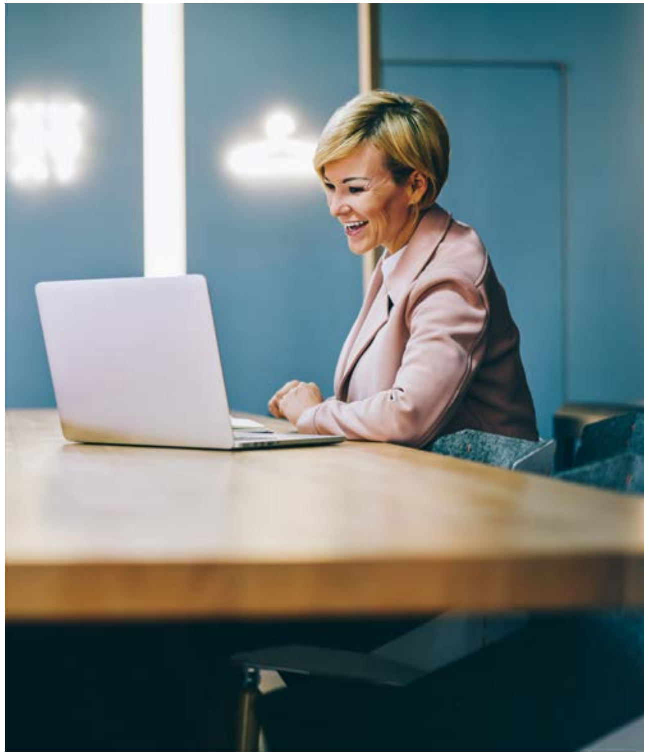
- **Will we all be living, working and learning remotely?** If so, do we actually have the right tools?

- **Have inflexible workplaces versus connectivity issues at home convinced us that a hybrid model for the office is the way to go?** Would we work better by splitting our time between a home office and a collaboration hub? (Especially if quality connectivity and telepresence technology at the hub made it easier to connect with people.)

- **How do we strike the right balance between enabling our people to do their jobs effectively and the need to keep our data secure?** Are we moving beyond only hardening the network perimeter and towards relying on application partners to provide suitable data security tools and controls?

- **How are we going to manage truly disparate teams of people?** Are we actually experiencing a shift from time-based to output-oriented work? And how will we monitor, and reward, this?

- **Even if we do return to the office, will there be more focus on planning for a similar future event?** Will companies that can continue working as normal in such an event have a sizeable competitive advantage?



Introduction

Ant Morse
linkedin.com/in/antmorse

Dave Cornwell
linkedin.com/in/dpcornwell

Rather than just focus on what might be, in this paper we've aimed to address each of the three phases (recent decisions, current planning and future strategies) in turn. And we've done so through the lens of four areas that our customers have asked us about the most:

- **The digital workplace –** "How can we move on from remote collaboration to a fully digital workplace?"
- **Collaboration –** "Now we've set up people to work remotely, did we miss anything?"
- **Security –** "Have we left ourselves open to cyber attacks?"
- **Connectivity –** "Should we all just make the shift to mobile connectivity?"

Of course, technology is only part of the solution. Factors like the impact on people and their wellbeing, the company culture, attitudes towards a remote workforce and even guidelines on the use of technology itself are all equally important. So they should be considered carefully.

And what about your longer-term plans? Will we all have an obligation to allow people to work remotely on a more permanent basis? Our own research told us that 67% of employees ranked flexible working in their five most important workplace benefits.

While none of us want it to happen, it is possible that we could face an enforced remote working policy again in the future. And this time it won't be acceptable to pull a quick solution together. Business leaders will expect IT leaders to be prepared with a prescriptive and predictable approach to send everybody home.

We can learn from recent months and then use that knowledge to inform future plans. On the pages that follow you'll find some of the most common questions we've been asked. As well as our experts' recommendations for the months and years ahead.

If you would like to discuss any of the points raised here, then please get in touch with us or our colleagues directly.

Digital workplace

Digital workplace experts Jonathan Undrell and Narinder Dhiliwal review the state of play for digital transformation and the impact on long-term workplace strategies.

Jonathan Undrell,
Head of Digital Workplace, O2 Business
linkedin.com/in/jundrell

Narinder Dhiliwal,
Digital Workplace Consultant, O2 Business
linkedin.com/in/narinder-dhiliwal-b709029

"How can we move on from remote collaboration to a fully digital workplace?"

We get asked this a lot. Especially since most of the organisations we've spoken to have had to make lots of workplace technology decisions on the fly. The good news is that many were already on some kind of digital transformation pathway.

Just imagine if something like COVID-19 had happened 15 years ago. The traditional castle-and-moat style corporate set-ups wouldn't have been able to cope. Today's organisations were already much more flexible. They were using some public cloud apps. Users were starting to work remotely. Mobile working was becoming a factor of daily life. Especially for knowledge workers. One of the biggest issues has come in the form of enabling all kinds of employees to work away from the office, the store or the factory.

Businesses have been forced into minimal viable solutions to shift everyone to working from home. While there are plenty that have adopted some form of hybrid cloud or mix of on-premises and cloud IT, there are still those with legacy infrastructure. Some may have had the tools in place but weren't using them to the full potential. Out of necessity they've had to focus on practical details. Like which cloud apps to sign up for. How many laptops were available. Remote access to corporate systems. And then how to solve all the end user IT issues as people quickly made the shift.

So now it's only natural that those in key positions are starting to ask what it means for the future of their organisations. If you were forced to equip people for mobile working, do you want them to stay mobile? Perhaps they worked in frontline customer service positions. Did they work more or less effectively away from the main office? If you're happy for people to work away from the office more often (or all the time), then how will you make sure there's still some in-person contact from time to time?

For example, headquarters could be reimagined as places for team huddles and customer meetings. Instead of rows and rows of fixed desks.

There is already – almost naturally – a kind of shift from reacting to a crisis towards long-term planning.

Digital workplace

Jonathan Undrell
linkedin.com/in/jundrell

Narinder Dhiliwal
linkedin.com/in/narinder-dhiliwal-b709029

Questions are now being asked about how we measure productivity too. Whilst there are cloud tools for tracking employee activity, by and large managers have had to trust teams to get the work done. So perhaps workplace productivity goals are being reset from time-based to output-based models.

Previously, there may have been conflicting views in the organisation about the pace of digital transformation and workplace mobility. Now, IT teams and business units might be closer aligned. Business units can see that IT teams are critical to profitability. And IT teams can understand the need for people to just get on with work. This closeness is one outcome. But what about the impact on your costs? Did you previously spend significant sums on travel despite the tools being in place to host video calls, webinars or training sessions? And what about the impact on your organisation's carbon footprint from all this reduced travel?

Plus, there's the impact on people. Those in HR, IT, Finance and senior management have been working together to maintain morale and support for employees working remotely. The transition may have been easier for people used to working from home. Particularly for those whose commute was stressful. But for retail store workers, contact centre staff and others it's been harder to do the job. This 'soft' metric could start to become much more central to digital workplace strategies than it might have been in the past. And recruitment practices may change as organisations are able to draw on a pool of talent unrestricted by geography.

We've also seen more people in IT come around to the idea that employees are consumers. It used to be that complete access to systems or better hardware was the privilege of senior management. But staff at all levels want (and need) specific devices, apps and, above all, positive digital workplace experiences. How can we make those experiences better? And better for everyone? Are people happier and more productive working from home? Or are they more frustrated? Will they still need spaces to meet with fellow team members (or customers)? And instead of a series of tiers based on seniority, should we be considering universal experiences?

> Those in HR, IT, Finance and senior management have been working together to maintain morale and support for employees working remotely.

Organisations have asked us multiple questions like these almost as individual issues. But when you start grouping them together, you actually start to form a strategic view again. There is already – almost naturally – a kind of shift from reacting to a crisis towards long-term planning. Previous digital workplace strategies may have been accelerated. Or even ripped up. But we are seeing that the importance of strategic thinking is greater right now perhaps more than ever.

Digital workplace

Jonathan Undrell
linkedin.com/in/jundrell

Narinder Dhiliwal
linkedin.com/in/narinder-dhiliwal-b709029

Things to think about right now

- Any organisation with legacy, on-premises services/apps should look to fast-track its migration to cloud services wherever possible.
- Ask whether it's more than just knowledge workers that can work from home – there may be other employees who want to make the shift too.
- Build a communications strategy that incorporates organisational social media for engaging, agile and quicker ways of keeping in touch.
- Avoid spending extra by looking at the technologies you already have and see if they can be used more effectively as you adopt new working practices. Especially as potentially sensitive data is being discussed with house mates or family members within earshot.

Pointers for longer-term planning

- Consider how your digital workplace strategy allows for rapid changes in working practices (such as home working) and the further steps you could take to improve it.
- If this were to happen again, how would you react or prepare differently? Should you have a contingency plan to enable remote working at a predictable rate?
- Look at recruitment strategies again now that geography may be less of a barrier to employee onboarding, and prepare your employer brand to compete for the best talent from anywhere.
- Reappraise the workplace in terms of how many desks are still needed versus providing huddle spaces for teams or state-of-the-art meeting spaces for customer meetings.
- Look at more flexible ways to introduce new technology infrastructure (like Opex rather than Capex investments) so your organisation is in a better place to respond to another major disruption.

Got a question about your digital workplace?

Connect with our experts on LinkedIn. Or talk to the O2 Business team on **0800 955 5590**.

Security

Security specialists Phil Ray and Dean Thomson take a look at some of the key considerations for keeping people secure while working from home.

Phil Ray
Security Solution Architect, O2 Business
linkedin.com/in/phil-ray-5354948

Dean Thomson
Head of Digital Cyber Security, O2 Business
linkedin.com/in/deanthomson

“Have we left ourselves open to cyber attacks?”

Security is a central topic in almost all the conversations we’re having about remote working since COVID-19. Concerns include maintaining vigilance against data loss. Preventing users accessing websites that host unproductive or malign content. And avoiding the problems of shadow IT or BYOD creeping back in. Another note of major concern is all the relentless and well-crafted phishing attacks. It’s clear the hackers have a new target and that’s the COVID-19 remote worker.

To put these concerns into some kind of perspective, most remote working projects would have taken three to six months to deliver. Yet organisations have been forced into either short-term fixes or ramping up existing systems. And typically within a week or so.

Previously, the IT Security team would have been heavily involved. And while this may have slowed down large-scale rollouts, IT Security always had a duty of care to ensure that remote working tools were robust and resilient. As we all know, speed (rather than security) suddenly became the driving force behind the workstyle and technology choices organisations had to make.

So it’s important to remember that no one is ‘behind the curve’ when it comes to current security considerations. If anything, the curve jumped. The things that IT Security teams were thinking about before everyone was forced to work from home? They’re still the same things people should be thinking about now (and into the future).

The main difference is that most businesses are having to query their security arrangements retrospectively. In a different and much larger context. For example:

- Which collaboration tool has the most user-friendly security settings?
- What’s the impact of remote working on our GDPR compliance policy?
- Can our users work on sensitive information away from the office or should they be restricted to certain data?
- Depending on the sensitivity of the information, should family members and/or housemates have to sign NDAs?

Our plans in the future will need to accommodate more than just technology or workplaces. They will need to include the impact of major disruption on people.

Security

Phil Ray
linkedin.com/in/phil-ray-5354948

Dean Thomson
linkedin.com/in/deanthomson

All of these questions now no longer apply to a handful of users but to the entire workforce.

The sheer scale of remote working, coupled with the speed at which it's been introduced, almost inevitably creates security concerns about data hacks or phishing attacks. Some of the people we've talked to say they felt fairly well covered by existing security protocols. Others were very concerned about the wholesale use of video conferencing apps that had been hijacked.

Perhaps the most common thread has been the fact that users are working outside the old confines of the 'corporate' network. Whichever camp they're in, we've tended to focus on the new fundamentals. Like asking, what if this happens again? What worked for you before? What didn't?

As organisations start to dive into the security implications of mass remote working, we're talking to them about things like their Virtual Private Networks (VPNs):

- Are traditional VPNs still fit for purpose when people have had to use their own devices?
- How do I know the user that looks like he is authenticating from home is really my employee?
- How do I get visibility on what my users are doing on company devices while at home?
- Can we still provide adequate protection and performance on legacy VPN technology that wasn't designed for so many users?
- Why am I backhauling all my user traffic into the network to allow access to cloud native applications?
- If I can't filter traffic swiftly to the apps people need to do their jobs, then will people just find workarounds?
- If so, can we improve or completely change our existing VPN by upgrading to cloud security platforms that securely allow users to go direct to Office 365, AWS and all the others?

VPNs are just the thin end of the wedge. As we all know, security goes deeper than the surface layer of end users. Access to backend apps has been crucial for keeping businesses going. But those businesses are now starting to review security protocols, plug gaps and reassess remote working policies. We see that there's a real need for cyber awareness training in the new work/home environment.

Just a few months ago, not all businesses would have felt compelled to invest in remote working technology for all employees. The focus may have been on groups of knowledge workers. But what about retailers, contact centres, entertainment venues or construction companies? All these businesses typically rely on large numbers of people working in one place. As the economy reopens, will they invest in ways to help staff work from home if, and when, they need to?

Those organisations that are able to look ahead are looking deeper still. Not just by assessing the security of applications or corporate data. But by analysing the resilience of the organisation as a whole.

Some business continuity plans have proven to be too literal.

Few businesses will have cobbled along without any serious contingency plan. Especially when in recent years the focus has been on risk management, compliance and data privacy anyway. Yet some business continuity plans have proven to be too literal. They have been about 'business continuity' or business-as-usual. But what about when multiple issues hit at the same time and business cannot go back to 'usual'? Or when plans are just plans that are simply written down and left untested?

What we can all probably recognise – whether our business continuity plans helped us mitigate any security problems or not – is that the rapid shift to home working was unlikely to be included. Especially when you consider the degree to which the home has swiftly become an extension of the office. And that home working could very well become the new normal for some.

Having talked with some business leaders on this very subject, it's clear that business continuity plans will have to be broader in scope in the coming years. Our plans in the future will need to accommodate more than just technology or workplaces. They will need to include the impact of major disruption on people. They will need to include cultural factors. Like how to engage employees on the subject of data security. Most certainly, they will need to be more than just plans. They will need to be tested. And they will need to be ingrained within organisations so they can ride any future shocks and navigate out of them.

Security

Phil Ray
linkedin.com/in/phil-ray-5354948

Dean Thomson
linkedin.com/in/deanthomson

Things to think about right now

- Check individuals' security postures (which devices they're using, how they're connecting, etc.) before allowing BYOD access to the corporate network and assets.
- Extend considerations of the corporate security perimeter to include the potential risks from how people work from home.
- Offer remote cyber training, tips and tricks on how people can stay secure against bad actors looking to benefit in a crisis – especially as potentially sensitive data is being discussed with housemates or family members within earshot.

Pointers for longer-term planning

- Continue developing the secure remote working strategy to realise future cost savings from office spaces or productivity improvements from home working.
- Maintain regular security training events or communications to engage the workforce and stay ahead of the ever-evolving threat landscape.
- Prepare for a more mobile workforce returning to the office – from a 'wifi-first' approach to connectivity to re-embracing BYOD but with the tools (like advanced VPN) to ensure device compliance.

Collaboration

Collaboration experts Martyn Gill, Soumya Unni and Chris Hall respond to some of the most pressing concerns about new ways of working together.

Martyn Gill
Digital Solution Expert, O2 Business
linkedin.com/in/martyngillo2

Soumya Unni
Head of Collaboration Solutions, O2 Business
linkedin.com/in/soumyaunni

Chris Hall
Collaboration Solution Architect, O2 Business
linkedin.com/in/chris-hall-1a77862b

"Now we've set up people to work remotely, did we miss anything?"

As soon as people were asked to work from home, there was a huge surge in the use of collaboration tools. Our team was being asked to spin up applications like Microsoft Teams from, say, 100 users to 1000 users overnight. Previously, our Skype for Business contracts would have been balanced 80/20 between the office and home. Suddenly it was more like 10/90.

This shift has had a number of implications. The first couple are short-term, practical implications. Getting people collaborating in the cloud. And making sure they had the equipment to do so. Including the huge numbers of frontline employees, such as contact centre staff. Other implications may have a longer-term effect. Like the need for robust user authentication. The necessity of data loss prevention. Or the potential for AI and chatbots to support customer interactions while people work from home.

If we look at those shorter-term implications, we have to look at the effect on people. Did they have access to Microsoft Teams or Google Hangouts? If they used other tools like Zoom, were these corporate or personal accounts? Were there any security issues – like malware or phishing attacks? And given the shortage of some devices, did people even have the webcams or laptops to be able to work from home?

> One thing we've noticed is that businesses are starting to really focus on how they can help their employees work better. Not just work remotely.

Talking to some business leaders, it became clear the extent to which corporate devices were being left idle. People preferred to use their Apple iPads, iPhones or Samsung Galaxy devices rather than the often 'heavy-duty' corporate-issue device. Corporate laptops had been abandoned. Even for calls. It seems that people were favouring their personal devices because the camera quality was better or it connected to 4G as well as wifi. Simple things, like copying and pasting dial-in details from the corporate email system into a separate collaboration app became frustrating. Which all seems to point to Bring Your Own Device (BYOD) being back on the cards. Certainly, businesses will need to adjust to the fact that a whole host of devices are using corporate apps – not just the ones that the business issued.

Collaboration

Martyn Gill
linkedin.com/in/martyngillo2

Soumya Unni
linkedin.com/in/soumyaunni

Chris Hall
linkedin.com/in/chris-hall-1a77862b

A side effect of the sudden rush to provision hundreds or thousands of home workers was that the IT Service Desk was inundated. People not used to operating cloud apps, sharing screens or connecting remotely needed help. Yet the priority was always to get people up-and-running. Get them collaborating.

We've spoken with businesses that say after this initial flurry of activity, new things were coming to light. If they'd spun up Teams, they may have done so at the expense of usual security protocols. For users, reapplying these after the event is not too taxing. It could be as simple as getting everyone to reset their passwords and install multi-factor authentication. For IT teams, the implications are bigger. For example, how to ensure people actually follow the guidance. Or how to apply Unified Endpoint Management (UEM) to all users.

We were hearing about plenty of user frustration with Virtual Private Networks (VPNs). A VPN makes sense if you want to control access to apps and protect data on devices. But certain forms of VPN can be slow, sluggish and clunky to users who had been used to seamless collaboration from the office. In some cases, the VPN has made it harder to collaborate in real-time – either via a video conferencing app or after a call via shared document software.

So is the VPN dead? We don't think so. Especially as there are advanced VPNs that provide more flexibility and speed. However, there are plenty of people who would prefer direct access to collaboration apps. UEM could be one way to facilitate this, while enabling people to use their own devices at the same time.

One of the most common points that people have raised with us is the importance of educating and engaging employees. Some IT leaders have told us they've struggled to get information out to employees on some of the basics of collaboration. Things like how to set up a meeting in Microsoft Teams. Or advice on hosting a webinar. In the rush to simply get people collaborating, user support may have been overlooked. Our advice has been to set up some kind of central repository of how-to guides or videos. And then to think about how these could be used going forward.

If, for example, there are further periods where people are asked to work from home, what kind of training support might you post in advance? Could you then use this central 'knowledge base' as a portal for organisation-wide Learning & Development?

One thing we've noticed is that businesses are starting to really focus on how they can help their employees work better. Not just work remotely. Like thinking about the collaboration experience. Or the expectations for people joining calls or working together on shared documents. And this is influencing the way technology decisions are made. So yes, BYOD might very well be back on the cards for some businesses. For others, it's not about the technology necessarily. It's more about the user experience. This might even include reassessing workflows and procedures so they take into account how people work together from home.

Then there is the future of collaboration to consider:

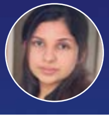
- Will we ever go back to an 'everyone in the office' culture or will the majority remain at home?
- Will organisations have a responsibility to ensure people have the option to remain at home and need to provide a universal experience for a hybrid workforce?
- What will this mean for meeting spaces and the ability to collaborate both in and outside of the room?

Depending on the make-up of the workforce, some of these considerations may be more or less important. But even the most reactive of decisions on collaboration can be re-evaluated. And then built upon to make sure the organisation is more resilient in the future.

A side effect of the sudden rush to provision hundreds or thousands of home workers was that the IT Service Desk was inundated.

Collaboration

Martyn Gill
linkedin.com/in/martyngillo2


Soumya Unni
linkedin.com/in/soumyaunni

Chris Hall
linkedin.com/in/chris-hall-1a77862b

Things to think about right now

- Rapid change has resulted in new headaches for Compliance, HR and IT teams. So choose the right enterprise collaboration tool by identifying which business areas will benefit, involving users in the process and checking compatibility with tools already in use.
- Organisations are now having to deal with the data management and security issues of lots of people working from home. Especially how they share, access and store information. Re-evaluate your security requirements. Like how to move data securely between users and cloud apps, ensure GDPR compliance away from a VPN, access sensitive documents or reduce the risk of a data breach.
- Lots of people working remotely may cause some organisations to panic unnecessarily about productivity. So implement new workflows that simplify business processes. Or even change the focus from hours spent to quality outcomes to help your employees flourish in a flexible working environment.
- The importance of internal communication and clear, concise key messages is critical now more than ever. Find the right platform (such as virtual broadcasts or town-hall meetings) to cascade information. Then look at how such media could be extended to communicate externally via virtual conferences or networking events.
- Businesses with contact centres need to retain their focus on customers. Providing technology that allows frontline employees to work from home and increasing self-service capabilities will help you cope with increased customer interactions.

Pointers for longer-term planning

- Collaboration is more than just a single tool. It is an ecosystem of tools which allow people to communicate and collaborate. This ecosystem should be fully integrated, including security and compliance controls. It should also provide an enhanced experience to being in an office, not just a comparable one.
- The frontline employee is first with the customer, first with the product and first with the brand. So they will be key to how organisations successfully exit lockdown. Giving these people a voice in your digital transformation strategy (including future training, data management and technology requirements) could have a direct impact on driving loyalty from your customer base.
- As businesses look to see which functions can be delivered away from the office, any changes may depend on the extent to which you can provide on-demand training and education. In particular, using a collaboration platform that is intuitive to users and can respond to their needs – perhaps using AI.
- Businesses with a contact centre workforce will continue looking at ways to enhance customer experience. Integrating new contact centre tools (like speech recognition, AI chatbots and call recording for compliance) with your collaboration tools can help make your business more agile.
- Contact centres with rows of agents might be a thing of the past. Given the right tools, a remote contact centre workforce can be more reactive and agile. This may allow you to take advantage of the gig economy while driving significant cost savings for the business.

Looking for answers on remote collaboration?

Connect with our experts on LinkedIn. Or talk to the O2 Business team on **0800 955 5590**.

Connectivity

Connectivity leads Sakir Passwala and Taylor Franks take a look at the network implications of the huge shift to working from home.

Sakir Passwala
Solution Architect, O2 Business
linkedin.com/in/sakir-passwala-54907971

Taylor Franks
Connectivity Specialist, O2 Business
linkedin.com/in/taylorfrankso2

“Should we all just make the shift to mobile connectivity?”

Organisations are being run on conferencing services like Microsoft Teams or Google Hangouts. People are collaborating on messaging platforms like WhatsApp. And everyone and their cat seems to be video calling on Houseparty. Every single one of these apps depends on connectivity. And the blurring of boundaries between home life and work life highlights the twin aspects of connectivity: the end user and the network.

If you’ve been on a video call (whether for work or personal reasons), you’ll have noticed the ‘bad connection’ alert for some users. It might be that they live in a rural location with a poorer broadband connection. Or that other members of their household have hijacked the internet and are streaming YouTube or PlayStation games.

The competition for connectivity at home is actually a huge challenge for businesses. Trying to keep people productive as they work from home is not just about their corporate set-up. It’s about what else is going on around them. As with most issues with technology there are quick fixes and long-term improvements.

> What is clear from the conversations we’re having is that connectivity – both at home and at the corporate level – has become critical to future workplace strategies.

Quick fixes in this case might involve using a wired connection for corporate devices to improve performance. But if you live in a household with teenagers who have their own phones and gaming devices then this is probably just patching over the cracks.

We’re advising businesses to ask employees about their experiences.

- How are they finding video calls?
- Have they been frustrated or surprised by the connection quality?
- What’s it been like using the corporate Virtual Private Network (VPN) or Virtual Desktop Infrastructure (VDI)?
- Are they using their own workarounds?

The answers to questions like these, coupled with hard data about app usage, can inform the business approach to connectivity while everyone is working from home.

Connectivity

Sakir Passwala
linkedin.com/in/sakir-passwala-54907971

Taylor Franks
linkedin.com/in/taylorfrankso2

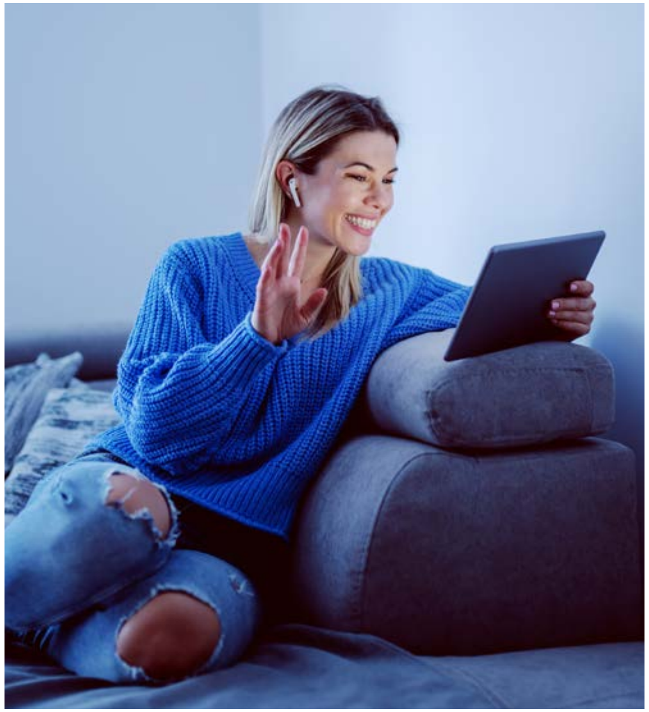
A longer-term improvement for home workers might involve shifting from traditional ADSL connections to modern FTTC or FTTP connections. But there are some obvious dependencies here. For FTTC installations, engineer availability is limited. Orders or upgrades are currently on hold. And with superfast FTTP installations, the rollout is very limited in the UK and roads need to be dug up.

A medium-term option could be to blend the sources of connectivity. In other words, a form of load balancing whereby your employees switch to a mobile connection when they need to. Or they use 4G for certain devices and broadband for others to split the load. The 4G network in the UK is strong – even serving those rural areas where ADSL lines deliver slower broadband speeds.

Instead of simply reviewing office estates, businesses are starting to explore reviewing home office estates too.

Some businesses have asked us about how 5G will help the current situation. We're exploring lots of new use cases for 5G – from remote monitoring of equipment to creative collaboration. As our investment in the UK's 5G infrastructure continues, we'll be demonstrating how 5G mobile connectivity can also support home workers, businesses and the Government in similar situations in the future.

Whether via wifi or 5G, home connections are likely to play a much more significant role in future connectivity strategies. But that's on top of, rather than at the expense of, central business considerations too.



For example, we're being asked about how to manage the increase in data usage. Particularly by businesses that pay for mobile data and even provide broadband to the homes of employees. Again, there are ways of managing data for individual users and restricting access to data-hungry sites. Doing this can reduce 'bill shock'. And ensure connectivity doesn't become a major drain on financial resources when earnings are under pressure.

As we move out of the initial period of adjusting to working from home, there are more strategic factors to consider. A big shift in focus is about to begin. Instead of simply reviewing office estates, businesses are starting to explore reviewing home office estates too.

This might mean re-evaluating committed or proposed investments in a Wide Area Network (WAN). Perhaps a future-proofed option would be to consider investing in people's home broadband set-ups. Especially where the data shows that there are poor quality connections or low speeds that prevent people doing their jobs. Having the infrastructure in place to scale bandwidth up or down is likely to become more important. Especially when you consider that large groups of people may be asked to work from home again in the future.

And if network infrastructure does need refreshing, how do you build in this adaptability? One option might be more granular load balancing via software-defined networking (or SD-WAN). This will involve assessing whether it's right for the business. Then the best way to deploy it for users.

The disruptive change we have seen is also an opportunity to review voice infrastructure. BT is switching off its analogue network in a few years. So we're already talking to businesses about the transition from ISDN or PTSN calls to SIP Trunking.

And finally, should mobile connectivity be the lynchpin of working from home or a back-up to home and office broadband? The answer to this question really depends on the effect of extended periods of working from home on employees. In particular, the amount of data being transferred, the availability of mobile connections and the strength of home broadband.

What is clear from the conversations we're having though is that connectivity – both at home and at the corporate level – has become critical to future workplace strategies. And mobile connectivity, in particular, will have a much bigger role to play. Especially as businesses aim to build more flexibility and resilience into everything they do.

Connectivity

Sakir Passwala
linkedin.com/in/sakir-passwala-54907971

Taylor Franks
linkedin.com/in/taylorfrankso2

Things to think about right now

- Consider advising colleagues to use Ethernet or whole-home wifi systems to improve coverage in temporary home offices that have poor connections.
- Start looking at shifting users to better connectivity at home through 4G or even an uplift from ADSL to FTTC or FTTP, so you can give them a predictable (and better) experience.
- Ensure the datacentre serving home users for VPN or VDI access has sufficient bandwidth to support all users and ask the supplier if it can be scaled up when required. Any immediate connectivity concerns have probably been overcome by now.

Pointers for longer-term planning

- Often, connectivity can be the part of your infrastructure which is least flexible. So consider your ability to flex in a changing environment. Particularly, how you can enhance user connectivity as part of your planning for another similar event.
- Look at the fast deployment of connectivity solutions based on 4G or 5G to people's homes that's managed centrally but without the lead times associated with traditional forms of connectivity.
- Decide whether 'suitable home connectivity' might be a basic requirement for employees in the future – much like a 'full clean driving licence' is today.
- Check that future workspaces (in homes or in an office) can support the likely mass shift from desktop computers with LAN connections to mobile devices that need wifi or WAN infrastructure.

Rethinking your connectivity requirements?

Connect with our experts on LinkedIn. Or talk to the O2 Business team on **0800 955 5590**.

What comes next?

Ant Morse
Head of Digital Solutions, O2 Business
linkedin.com/in/antmorse

Dave Cornwell
Head of Solutions, O2 Business
linkedin.com/in/dpcornwell

What we've seen is a remarkable reaction to the Government lockdown. Many roles have continued as normal but from a new location. People in roles that everyone thought would be too hard to send home have done just that. And many of the perceived barriers in technology, policy or compliance have been overcome with comparative ease.

The technology we all use today is much better and more able to support a remote workforce than it was 10 years ago. Likewise our public and private technology infrastructure, although more complex than ever, has been able to meet the demands placed upon it without missing a beat. This has all led to a very different lockdown experience than we would've had just a few years ago.

But there is still more to do.

Many users have been pressed into using technologies, such as collaboration tools. Not because they wanted to, but because it offers a better experience than simply being in the same room. This meant adoption rates rose sharply. But we now have to shift the balance towards users seeking to use technology not because they have to but because it offers a better experience. This goes beyond better devices and video tools. It's about an integrated ecosystem of tools and physical spaces.

And what comes next? Are we facing a new normal – business as unusual – in our working lives? We think so. And we're also predicting a change in the way we plan and build technology solutions. How we manage and recruit people. And how we plan for similar events in the future.

To rely on an old phrase: "Work is something you do, not somewhere you go."This means recruitment policies can change. You're no longer limiting your talent pool to those who happen to live within 30 miles of your office. You attract the best talent, not the best talent local to you. This could have knock-on effects for certain social considerations. Like whether childcare needs will change. Or whether less of a pull towards cities and industrial centres drives a change in property prices.

What comes next?

Ant Morse
linkedin.com/in/antmorse

Dave Cornwell
linkedin.com/in/dpcornwell

In a world in which we've experienced a pandemic in recent memory, will it be socially acceptable to increase risk by traveling in packed trains or planes?

We already knew that remote workers were more productive and took fewer sick days. But they also reported workplace loneliness as a growing factor in their lives. As we become more comfortable with – or even demand – a remote workforce in the knowledge that it is more efficient, we must also consider digital inclusion for our remote workers.

Finally, our plans must be better. Having experienced the events of early 2020 first-hand, it's entirely reasonable to think we may face something similar again in our working lives. Not having a plan will be unacceptable.

So future plans must be clear enough to be put in place quickly and predictably enough. That way stakeholders will know how quickly each business function can be back up and running. In data centre and application architecture we talk about a Recovery Time Objective (RTO) – the point in time when a service will return in an outage. Forward-thinking IT teams will be developing RTOs for job functions and departments.

We all hope that we will not see another pandemic of this magnitude. But if we do then technology leaders will need to be proactively executing plans rather than reactively deploying technologies.

More on how we're helping

We're closely following Government advice so we can make the right decisions for everyone who relies on our network.

We understand the importance of keeping Britain moving at a time like this. And we don't underestimate the role we have to play.

Here are some of the ways we've been helping:

- We've been supporting the Government using our text messaging platform to deliver over 34 million texts following the announcement from No 10.
- We've been providing devices to the NHS Nightingale Project.

We're also providing plenty of practical tools to support everyday operations for organisations across the UK:

- Flexible SaaS security to protect remote workers without adding strain to VPNs.
- Business SMS for group texts to employees or customers without fixed contracts.
- Mobile Voice and SMS recording for maintaining audit trails or best practice despite remote working.
- Data management with Moda to reduces the risk of 'bill shock' by proactively controlling data usage.
- Wellbeing app from Evermind to enable employees to take part in activities that build resilience and reduce stress.

If you want to talk through anything you've read here please get in touch with our team or call us on **0800 955 5590**.

You can also keep up to speed with everything we're doing right here:
o2.co.uk/business/why-o2/our-approach/covid-19

Published in May 2020. All information is correct at time of going to print.
Telefónica UK Limited Registered in England no. 1743099. Registered Office 260 Bath Road Slough SL1 4DX